

AURORA Supporting Document : Examples with Internal Values

October 24, 2008

AURORA Examples (Intermediate Values)

This document describes example vectors of the hash function family AURORA. We give two examples for the message M_1 and M_2 below for each hash size.

Let the message M_1 be the 24-bit ASCII string “abc”, which is equivalent to the following binary string:

01100001 01100010 01100011.

Let the message M_2 be the 448-bit ASCII string

“abcbcdcedefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq”.

AURORA-256 (M_1 : 1 block message)

MSF_L								
input	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000
con		5107ed2a		94a13089		12d49830		9eed0b1f
after con	61626380	5107ed2a	00000000	94a13089	00000000	12d49830	00000000	9eed0b1f
R 1	input	51ed9889	00000000	94070b30	00000000	12a1ed1f	00000000	9ed4302a 61626380
	F	F_0		F_1		F_0		F_1
	input	51ed9889		94070b30		12a1ed1f		9ed4302a
	after S	e04593e1		80ebc211		37364504		a93b111a
	after M	6f9a5e1e		a4c205ba		dded79c9		8fc40420
	con	853fd5fe		c3f464df		2a004c08		36435c4b
	after con	6f9a5e1e	a4c205ba	c3f464df	dded79c9	2a004c08	8fc40420	57213fcb
	output	6f9a5e1e	6f9a5e1e	6f9a5e1e	6f9a5e1e	6f9a5e1e	6f9a5e1e	6f9a5e1e
R 2	input	eae53565	a4c205ba	67a53bc1	dded79c9	f7368beb	8fc40420	d8ed61e0 6f9a5e1e
	F	F_0		F_1		F_0		F_1
	input	eae53565		67a53bc1		f7368beb		d8ed61e0
	after S	6f328f98		a3faa49b		f9c6fcb9		9e452172
	after M	bdad2ca8		f3e653be		5d5c2dd8		ec190047
	con	85bd57fe		7e118162		a8004c8a		fd38e1ae
	after con	bdad2ca8	217f5244	f3e653be	a3fcb8ab	5d5c2dd8	27c448aa	ec190047 92a2bfb0
	output	bdad2ca8	9cd27eec	f3e653be	501aab15	5d5c2dd8	7a986572	ec190047 7ebbbff7
R 3	input	9cbb6515	f3e653be	50d2bf72	5d5c2dd8	7a1a7ef7	ec190047	7e98abec bdad2ca8
	F	F_0		F_1		F_0		F_1
	input	9cbb6515		50d2bf72		7a1a7ef7		7e98abec
	after S	d0ef98d8		33ddc889		6c0f53f9		539381c1
	after M	4d04a215		d819f11a		c4f473ca		e94ca2dd
	con	87b55fffc		b958c8a5		a0024e82		6eb726e6
	after con	4d04a215	74530c42	d819f11a	e404e57d	c4f473ca	4c1b4ec5	e94ca2dd d31a0a4e
	output	4d04a215	3957ae57	d819f11a	3c1d1467	c4f473ca	88ef3d0f	e94ca2dd 3a56a893
R 4	input	39563d67	d819f11a	3c57a80f	c4f473ca	881dae93	e94ca2dd	3aef1457 4d04a215
	F	F_0		F_1		F_0		F_1
	input	39563d67		3c57a80f		881dae93		3aef1457
	after S	fdf38ea3		cd82a06d		30ce17a8		4be91982
	after M	f9b53c36		41abf8d2		7afb7576		dc559f18
	con	8f957ff4		c88b1ad5		800a46a2		ca555735
	after con	f9b53c36	578c8eee	41abf8d2	0c7f691f	7afb7576	6946e47f	dc559f18 8751f520
	output	f9b53c36	ae39b2d8	41abf8d2	4dd491cd	7afb7576	13bd9109	dc559f18 5b046a38
R 5	input	ae0491cd	41abf8d2	4d396a09	7afb7576	13d4b238	dc559f18	5bbd91d8 f9b53c36
	F	F_0		F_1		F_0		F_1
	input	ae0491cd		4d396a09		13d4b238		5bbd91d8
	after S	17bdab2e		8bfd7f24		4e3bbf58		9027ab9e
	after M	49950587		2ed27264		b53cde68		4a5760bd
	con	af15ff4d		00e7761d		002a6622		13c59f59
	after con	49950587	eebe0706	2ed27264	7a1c036b	b53cde68	dc7ff93a	4a5760bd ea70a36f
	output	49950587	a72b0281	2ed27264	54ce710f	b53cde68	69432752	4a5760bd a027c3d2
R 6	input	a727270f	2ed27264	542bc352	b53cde68	69ce02d2	4a5760bd	a0437181 49950587
	F	F_0		F_1		F_0		F_1
	input	a727270f		542bc352		69ce02d2		a0437181
	after S	b123236d		a1bb3cac		4c77d3dd		7a6b2df4
	after M	0677e537		ae7deb90		63bf73c5		9b9008dc
	con	2d15ff56		9acd5d86		00a8e422		44f00573
	after con	0677e537	03c78d32	ae7deb90	2ff183ee	63bf73c5	4aff849f	9b9008dc 0d6500f4
	output	0677e537	05b06805	ae7deb90	818c687e	63bf73c5	2940f75a	9b9008dc 96f50828
R 7	input	05f5f77e	ae7deb90	81b0085a	63bf73c5	298c6828	9b9008dc	96406805 0677e537
	F	F_0		F_1		F_0		F_1
	input	05f5f77e		81b0085a		298c6828		96406805
	after S	007ef953		f4fe0244		5ced91b5		09ad9100
	after M	e031ddbf		5e1787ff		60417464		2ef49810
	con	75779c0f		285fcf34		63f1bc40		6194b7e0
	after con	e031ddbf	db0a779f	5e1787ff	4be0bcf1	60417464	f861b49c	2ef49810 67e352d7
	output	e031ddbf	3b3baa20	5e1787ff	15f73b0e	60417464	9820c0f8	2ef49810 4917cac7
R 8	input	3b17c00e	5e1787ff	153bcdf8	60417464	98f7aac7	2ef49810	49203b20 e031ddbf
	F	F_0		F_1		F_0		F_1
	input	3b17c00e		153bcdf8		98f7aac7		49203b20
	after S	a462deb7		d8a4ee22		93f95a60		5fd1a4d1
	after M	05475e59		5856eb54		6e23b75a		61480389
	con	05475e59		5856eb54		6e23b75a		61480389
	after con	05475e59	5b50d9a6	5856eb54	38179f30	6e23b75a	40d72f4a	61480389 8179de36
	output	05475e59	5b50d9a6	5856eb54	38179f30	6e23b75a	40d72f4a	61480389 8179de36

MSF_R								
	input	00000000	00000000	00000000	00000000	00000000	00000000	00000001
	con	cb4c7695		7c4e2a3b		896a7901		ab89dba1
	after con	00000000		cb4c7695		00000000		ab89dba0
R 1	input	cb89793b	00000000	7c4cdb01	00000000	894e76a0	00000000	ab6a2a95
	F	F_2		F_3		F_2		F_3
	input	cb89793b		7c4cdb01		894e76a0		ab6a2a95
	after S	a5e151a4		ae3d4fdc		e10e0a7a		817f1a2b
	after M	e46bdf29		78cd79cc		d635a167		e11e797a
	con	a1506aff		f6a4c0b1		9500131d		7e9c514b
	after con	e46bdf29	a1506aff	78cd79cc	f6a4c0b1	d635a167	9500131d	e11e797a
	output	e46bdf29	453bb5d6	78cd79cc	8e69b97d	d635a167	4335b27a	e11e797a
R 2	input	4582b27d	78cd79cc	8e3b287a	d635a167	4369b531	e11e797a	9f35b9d6
	F	F_2		F_3		F_2		F_3
	input	4582b27d		8e3b287a		4369b531		9f35b9d6
	after S	2806bdfb		47a4b56c		6b4c3e46		aa8f14ca
	after M	b6485d37		c3b5f49b		01b04a45		278ab2bc
	con	a1112bff		41187c06		d400135c		87f366f7
	after con	b6485d37	d9dc5233	c3b5f49b	972ddd61	01b04a45	351e6a26	278ab2bc
	output	b6485d37	6f940f04	c3b5f49b	549829fa	01b04a45	34ae2063	278ab2bc
R 3	input	6f1220fa	c3b5f49b	54940b63	01b04a45	34980f62	278ab2bc	44ae2904
	F	F_2		F_3		F_2		F_3
	input	6f1220fa		54940b63		34980f62		44ae2904
	after S	1c37d105		a180c23f		67936df8		f7175cbd
	after M	a0ba3bc4		27b88024		0be6bc93		b932ae28
	con	a0152ffe		f9f1153e		d0011258		d582de1e
	after con	a0ba3bc4	63a0db65	27b88024	f8415f7b	0be6bc93	f78ba0e4	b932ae28
	output	a0ba3bc4	c31ae0a1	27b88024	dff9df5f	0be6bc93	fc6d1c77	b932ae28
R 4	input	c3f81c5f	27b88024	df1a2d77	0be6bc93	fcf9e001	b932ae28	da6ddfa1
	F	F_2		F_3		F_2		F_3
	input	c3f81c5f		df1a2d77		fcf9e001		da6ddfa1
	after S	3c22ec07		7d0f4954		cb6672dc		15ea7d36
	after M	abfc14b2		ab89ce71		67f60b9c		a3f67eae
	con	a4053ffa		9dc7235a		c0051648		b94aba28
	after con	abfc14b2	83bdfbde	ab89ce71	96219fc9	67f60b9c	7937b860	a3f67eae
	output	abfc14b2	2841ab6c	ab89ce71	3da851b8	67f60b9c	1ec1b3fc	a3f67eae
R 5	input	2806b3b8	ab89ce71	3d41fffc	67f60b9c	1ea8ab42	a3f67eae	bac1516c
	F	F_2		F_3		F_2		F_3
	input	2806b3b8		3d41fffc		1ea8ab42		bac1516c
	after S	b54dc410		8e635bcb		94a081c9		f19be097
	after M	3a42ac8c		41bca70d		97c03996		e8f2c05b
	con	b4457fea		84caaec3		80150608		2278a325
	after con	3a42ac8c	1fccb19b	41bca70d	e33ca55f	97c03996	23e378a6	e8f2c05b
	output	3a42ac8c	258e1d17	41bca70d	a2800252	97c03996	b4234130	e8f2c05b
R 6	input	25764152	41bca70d	a28e7730	97c03996	b4801dcc	e8f2c05b	61230217
	F	F_2		F_3		F_2		F_3
	input	25764152		a28e7730		b4801dcc		61230217
	after S	870a63ac		2a475411		f2a6ce31		21fbd362
	after M	1d2b08ba		4b1778f7		4ea2d071		800b587a
	con	f5457fab		dd83e79a		80544708		30ca7a6c
	after con	1d2b08ba	b4f9d8a6	4b1778f7	4a43de0c	4ea2d071	68a68753	800b587a
	output	1d2b08ba	a9d2d01c	4b1778f7	0154a6fb	4ea2d071	26045722	800b587a
R 7	input	a98357fb	4b1778f7	01d28e22	4ea2d071	2654d09a	800b587a	8a04a61c
	F	F_2		F_3		F_2		F_3
	input	a98357fb		01d28e22		2654d09a		8a04a61c
	after S	68da82d2		dcdd4774		12a1ffc5		35bde8ec
	after M	c29830b5		b6c27a7f		e3b2a2fa		0654b064
	con	8d6cd653		a1ddb9e6		29ac3f21		0c328632
	after con	c29830b5	c67baea4	b6c27a7f	ef7f6997	e3b2a2fa	a9a7675b	0654b064
	output	c29830b5	04e39e11	b6c27a7f	59bd13e8	e3b2a2fa	4a15c5a1	0654b064
R 8	input	044dc5e8	b6c27a7f	59e33ea1	e3b2a2fa	4abd9eec	0654b064	17151311
	F	F_2		F_3		F_2		F_3
	input	044dc5e8		59e33ea1		4abd9eec		17151311
	after S	bd8bd7b4		75849936		6127a9c1		62d84e40
	after M	9143bac2		7688bebb		549bad3e		11429543
	con	9143bac2		7688bebb		549bad3e		11429543
	after con	9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543
	output	9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543
	output	9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543

CPF										
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000		
con		2883f695		ca509844		096a4c18		cf76858f		
mask									01010101	
after con		00000000	2883f695	00000000	ca509844	00000000	096a4c18	00000000	ce77848e	
T		61626380	a20fda55	00000000	29426112	00000000	12d49830	00000000	9eed0b1f	
output		61626380	8a8c2cc0	00000000	e312f956	00000000	1bbed428	00000000	509a8f91	
R 1	input	8a9ad456	00000000	e38c8f28	00000000	1b122c91	00000000	50bef9c0	61626380	
	F	F_1		F_0		F_1		F_0		
	input	8a9ad456		e38c8f28		1b122c91		50bef9c0		
	after S	35c53bf3		84edd5b5		7c3742ab		33e566de		
	after M	a3ec0549		30ba9b03		a577369f		57db93c3		
	con	9698ed2b			f89c5476			12d4f203		
	mask									01010101
	after con	a3ec0549	9698ed2b	30ba9b03	f89c5476	a577369f	12d4f203	57db93c3	3770d5c2	
	T	00000000	e5a63b4a	00000000	be27151d	00000000	896a7901	00000000	ab89dba0	
output	a3ec0549	d0d2d328	30ba9b03	7601da68	a577369f	3ec9bd9d	57db93c3	cb229da1		
R 2	input	d022bd68	30ba9b03	76d29d9d	a577369f	3e01d3a1	57db93c3	cbc9da28	a3ec0549	
	F	F_1		F_0		F_1		F_0		
	input	d022bd68		76d29d9d		3e01d3a1		cbc9da28		
	after S	ff742791		0adddfdf		99dc2536		a57915b5		
	after M	c6a73d66		74c31210		388096bd		b9d6be29		
	con	429feaff			e1fa326f			15002604		
	mask									9b21ae25
	after con	c6a73d66	722571fc	74c31210	448d04f0	388096bd	42dbb5c7	b9d6be29	39ccaa6d	
	T	6f9a5e1e	d54b17c0	a4c205ba	ce6cc2cb	dded79c9	f7ed35c1	8fc40420	d8e53beb	
output	a93d6378	61c95b5a	d00117aa	fe22d42b	e56def74	8db616bb	3612ba09	58ff2faf		
R 3	input	61ff162b	d00117aa	fec92fbb	e56def74	8d225baf	3612ba09	58b6d45a	a93d6378	
	F	F_1		F_0		F_1		F_0		
	input	61ff162b		fec92fbb		8d225baf		58b6d45a		
	after S	215b64bb		cf7985ef		bc7490c7		834a3b44		
	after M	80f5765b		06e74e0c		e6384bd4		ad2a7080		
	con	42a0d5ff			ed498163			2a00263b		
	mask									fd38a296
	after con	80f5765b	92a1c255	06e74e0c	08246e17	e6384bd4	1c129c32	ad2a7080	5504c0ef	
	T	e46bdf29	a29ddaeb	78cd79cc	4734dcbe	d635a167	4335b27a	e11e797a	9f822831	
output	649ea972	b0c96ee5	7e2a37c0	49f7fca5	300deab3	b91f659c	4c3409fa	67ac985e		
R 4	input	b0ac65a5	7e2a37c0	49c9989c	300deab3	b9f76e5e	4c3409fa	671ffce5	649ea972	
	F	F_1		F_0		F_1		F_0		
	input	b0ac65a5		49c9989c		b9f76e5e		671ffce5		
	after S	fe4898fa		5f7993d0		14f901f0		a304cb32		
	after M	16439395		fb1e1d32		c7165e03		7013fe21		
	con	42deabff			3f08c0b1			54002645		
	mask									7e9c70d7
	after con	16439395	3cf49c3f	fb1e1d32	0f052a02	c7165e03	18342fbf	7013fe21	1b03d8a4	
	T	bdad2ca8	39a4fdd8	f3e653be	a035562b	5d5c2dd8	7a986572	ec190047	7ebbbff7	
output	abeebf3d	1313f272	08f84e8c	542e611b	9a4a73db	a5ba14ce	9c0afe66	15ab9972		
R 5	input	13ab141b	08f84e8c	541399ce	9a4a73db	a52ef272	9c0afe66	15ba6172	abeebf3d	
	F	F_1		F_0		F_1		F_0		
	input	13ab141b		541399ce		a52ef272		15ba6172		
	after S	4e81197c		a14ed477		fa186e89		d8f12189		
	after M	55865595		17ebb1d5		feacd4bf		e3c98bb8		
	con	422257ff			8230f80c			a80026b9		
	mask									0fe6cdef
	after con	55865595	4ada1973	17ebb1d5	187a8bd7	feacd4bf	340ad8df	e3c98bb8	a50973d3	
	T	b6485d37	37ca0782	c3b5f49b	2a4c14fd	01b04a45	34ae2063	278ab2bc	44120b62	
output	e3ce08a2	28964b64	d45e454e	25dd2eff	ff1c9efa	fe082c03	c4433904	02d2f309		
R 6	input	28d22cff	d45e454e	2596f303	ff1c9efa	fedd4b09	c4433904	02082e64	e3ce08a2	
	F	F_1		F_0		F_1		F_0		
	input	28d22cff		2596f303		fedd4b09		02082e64		
	after S	b5dd425b		87095e69		cf167324		d30218a2		
	after M	ddd5fdfe		92f5828c		4699a5e6		1a03fc33		
	con	43daaffe			dcac6452			50012741		
	mask									375b9373
	after con	ddd5fdfe	9784eab0	92f5828c	23b0faa8	4699a5e6	94421e45	1a03fc33	d5949ad0	
	T	4d04a215	72af5cae	d819f11a	783a28ce	c4f473ca	88ef3d0f	e94ca2dd	3a56a893	
output	90d15feb	38fe4be0	4aec7396	c97f50ea	826dd62c	5a3486ac	f34f5eee	f5c1ce70		
R 7	input	38c186ea	4aec7396	c9feceac	826dd62c	5a7f4b70	f34f5eee	f53450e0	90d15feb	
	F	F_1		F_0		F_1		F_0		
	input	38c186ea		c9feceac		5a7f4b70		f53450e0		
	after S	589b1d6f		79cf7748		4459731e		7e673372		
	after M	1930bf2a		ca3a5fa6		00109385		40678215		
	con	402a5ffd			f3e22a7d			a00224b1		
	mask									ab05bc3d
	after con	1930bf2a	0ac62c6b	ca3a5fa6	718ffc51	00109385	534d7a5f	40678215	3ad5e2d7	
	T	a0ba3bc4	e18d7050	27b88024	effcefaf	0be6bc93	fc6d1c77	b932ae28	daf82d01	
output	b98a84ee	f27be311	ed82df82	54494c58	0bf62f16	af30f5ad	f9552c3d	0a4a4dc3		

R 8	input	f24af558	ed82df82	547b4dad	0bf62f16	af49e3c3	f9552c3d	a0304c11	b98a84ee
	F	F_1		F_0		F_1		F_0	
	input	f24af558		547b4dad		af49e3c3		a0304c11	
	after S	6e617e83		a1438b08		c75f843c		7a113d40	
	after M	f3d6c625		32a60751		2a04d045		e2657ad1	
	con	47cabffa				e4458d6a		40052351	
	mask	e52aab9a							
	after con	01010101							
	T	f3d6c625	aa486078	32a60751	efb3a27c	2a04d045	b9500f6c	e2657ad1	5da12e75
	output	f9b53c36	5c7365b0	41abf8d2	9ba9239b	7afb7576	13bd9109	dc559f18	5b046a38
	output	0a63fa13	05edc3ed	730dff83	46bc86b6	50ffa533	80e94e20	3e30e5c9	e4c03e9c
R 9	input	05c04eb6	730dff83	46ed3e20	50ffa533	80bcc39c	3e30e5c9	e4e986ed	0a63fa13
	F	F_1		F_0		F_1		F_0	
	input	05c04eb6		46ed3e20		80bcc39c		e4e986ed	
	after S	00de0e4a		9f4599d1		a6a73cd0		f6381d45	
	after M	169c0efc		546fcace		19a2f81e		738928e5	
	con	480a7ff5				3b8e46b5		800a2c91	
	mask	72957451							
	after con	01010101							
	T	169c0efc	3b078076	546fcace	6b71e386	19a2f81e	be3ac958	738928e5	79f78f43
	output	abfc14b2	1420d5b6	ab89ce71	1ed428dc	67f60b9c	1ec1b3fc	a3f67eae	ba06ff42
	output	bd601a4e	39bb5b3c	ffe604bf	21ca0194	7e54f382	b95982ba	d07f564b	b07858e4
R 10	input	39788294	ffe604bf	21bb58ba	7e54f382	b9ca5be4	d07f564b	b059013c	bd601a4e
	F	F_1		F_0		F_1		F_0	
	input	39788294		21bb58ba		b9ca5be4		b059013c	
	after S	fd0c0680		8aef83f1		14ee90f6		fe75dccc	
	after M	fe959ad4		5a8e5fa5		5d7af584		fb4e25bf	
	con	578affea				8073bb0e		00153311	
	mask	89e2cfac							
	after con	01010101							
	T	fe959ad4	a86cfb55	5a8e5fa5	fe27488c	5d7af584	d06a655a	fb4e25bf	3583d4e3
	output	49950587	4e560502	2ed27264	a99ce21f	b53cde68	69432752	4a5760bd	a027c3d2
	output	b7009f53	18af6483	745c2dc1	0d35f536	e8462bec	e453b78c	b1194502	6eea328e
R 11	input	18eab736	745c2dc1	0daf328c	e8462bec	e435648e	b1194502	6e53f583	b7009f53
	F	F_1		F_0		F_1		F_0	
	input	18eab736		0daf328c		e435648e		6e53f583	
	after S	9d6f0bc6		5dc70ded		f68fa247		01267eda	
	after M	2b1ef3e6		fefb24d5		1097df0e		c476b916	
	con	688affd5				09955d87		002a0c11	
	mask	44f1464a							
	after con	01010101							
	T	2b1ef3e6	1cd6d214	fefb24d5	e1d3766b	1097df0e	b1334913	c476b916	f2f0d818
	output	3a42ac8c	12c70e8b	41bca70d	d1400129	97c03996	b4234130	e8f2c05b	617677cc
	output	115c5f6a	250f2f79	bf4783d8	ce685397	8757e698	1587d72d	2c84794d	57f016c2
R 12	input	25f0d797	bf4783d8	ce0f162d	8757e698	15682fc2	2c84794d	57875379	115c5f6a
	F	F_1		F_0		F_1		F_0	
	input	25f0d797		ce0f162d		15682fc2		57875379	
	after S	87ba52b0		776d6449		d891858d		82292651	
	after M	ebafe48c		beaeafd1		d60d259e		6f5ae076	
	con	168affab				4d66aec3		00547211	
	mask	a27802b9							
	after con	01010101							
	T	ebafe48c	a9cd7c73	beaeafd1	ca31485b	d60d259e	2cd00b5c	6f5ae076	b2255cd2
	output	0677e537	0b60d00b	ae7deb90	0318d0fc	63bf73c5	2940f75a	9b9008dc	96f50828
	output	edd801bb	490248f4	10d34441	77873776	b5b2565b	d39dd998	f4cae8aa	4b8ab48c
R 13	input	498ad976	10d34441	7702b498	b5b2565b	d387488c	f4cae8aa	4b9d37f4	edd801bb
	F	F_1		F_0		F_1		F_0	
	input	498ad976		7702b498		d387488c		4b9d37f4	
	after S	5f352c0a		54d3f293		25292fed		73df50be	
	after M	8e33b438		b8ed098b		71a8163e		af8dab0d	
	con	ea8aff57				bb07cf35		00a88e11	
	mask	6194f4d8							
	after con	01010101							
	T	8e33b438	fa59bb16	b8ed098b	0eb5996e	71a8163e	f46266bb	af8dab0d	8d4df462
	output	1d2b08ba	d4e9680e	4b1778f7	00aa537d	4ea2d071	26045722	800b587a	8a838e9a
	output	9318bc82	a0836720	f3fa717c	b6f2c398	3f0ac64f	a3ce27a7	2f86f377	a843d1f5
R 14	input	a0432798	f3fa717c	b683d1a7	3f0ac64f	a3f267f5	2f86f377	a8cec320	9318bc82
	F	F_1		F_0		F_1		F_0	
	input	a0432798		b683d1a7		a3f267f5		a8cec320	
	after S	7a6b2393		4ada95b1		d66ea37e		a0773cd1	
	after M	25a14fa7		1c4c0d2e		3ae38abc		5e4d4720	
	con	babbce07				142fe79a		31f8de20	
	mask	30ca5bf0							
	after con	01010101							
	T	25a14fa7	4941bf7b	1c4c0d2e	2b2521d5	3ae38abc	1e7e2d57	5e4d4720	a2d3ce73
	output	e031ddbf	76775440	5e1787ff	2bee761c	60417464	9820c0f8	2ef49810	4917cac7
	output	c5909218	1a97a49c	425b8ad1	1c875ae7	5aa2fed8	cbcd6713	70b9df30	b5896b94

R 15	input	1a8967e7	425b8ad1	1c976b13	5aa2fed8	bc87a494	70b9df30	b5bd5a9c	c5909218
	F	F_1		F_0		F_1		F_0	
	input	1a8967e7		1c976b13		bc87a494		b5bd5a9c	
	after S	0fe1a303		ecb0924e		a729b280		3e2744d0	
	after M	16000835		7a3c065b		ad918253		9356ea2e	
	con	1ad9aca7		43bb73cd		53587e42		18650c64	
	mask	01010101							
	after con	16000835	58822676	7a3c065b	19198d15	ad918253	23e1a172	9356ea2e	dcf49f7d
R 16	T	c29830b5	0271cf08	b6c27a7f	acde89f4	e3b2a2fa	4a15c5a1	0654b064	174d3eec
	output	d4983880	4cf3e14b	ccfe7c24	cffb02ba	4e2320a9	c465e680	95025a4a	58ef4bbf
	input	4cefe6ba	ccfe7c24	cff34b80	4e2320a9	c4fbe1bf	95025a4a	5865024b	d4983880
	F	F_1		F_0		F_1		F_0	
	input	4cefe6ba		cff34b80		c4fbe1bf		5865024b	
	after S	3de986f1		415e73a6		56d23ac8		8398d373	
	after M	d863ac61		ea2c440d		ccf88599		805d9b2b	
	con	f22c594f		6871b9e6		a6b096b7		8c3227ae	
R 17	mask	01010101							
	after con	d863ac61	3ed2256b	ea2c440d	2652994f	ccf88599	33b2ccfd	805d9b2b	59ab1e2f
	T	05475e59	b6a1b34c	5856eb54	702f3e60	6e23b75a	40d72f4a	61480389	8179de36
	output	dd24f238	50103a46	b27aaf59	bc51e322	a2db32c3	bf9d662e	e11598a2	588f5b32
	input	508f6622	b27aaf59	bc105b2e	a2db32c3	bf513a32	e11598a2	589de346	dd24f238
	F	F_1		F_0		F_1		F_0	
	input	508f6622		bc105b2e		bf513a32		589de346	
	after S	33d59a74		a7f59018		c8e04b0d		83df849f	
	after M	af4f8b03		450cf117		caa2a45c		8f77c6b0	
	T	9143bac2	93c0e05e	7688bebb	ca9d0e20	549bad3e	52cf1d5a	11429543	d3daa5f6
	output	3e0c31c1	8ef5c404	33844fac	2d4acdf4	9e390962	797821a4	9e3553f3	8189917e
	output	3e0c31c1	8ef5c404	33844fac	2d4acdf4	9e390962	797821a4	9e3553f3	8189917e

AURORA-224 (M_1 : 1 block message)

MSF_L								
input	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	51ed9889	00000000	94070b30	00000000	12a1ed1f	00000000	9ed4302a 61626380
R 2	input	eae53565	a4c205ba	67a53bc1	dded79c9	f7368beb	8fc40420	d8ed61e0 6f9a5e1e
R 3	input	9cbb6515	f3e653be	50d2bf72	5d5c2dd8	7a1a7ef7	ec190047	7e98abec bdad2ca8
R 4	input	39563d67	d819f11a	3c57a80f	c4f473ca	881dae93	e94ca2dd	3aef1457 4d04a215
R 5	input	ae0491cd	41abf8d2	4d396a09	7afb7576	13d4b238	dc559f18	5bbd91d8 f9b53c36
R 6	input	a727270f	2ed27264	542bc352	b53cde68	69ce02d2	4a5760bd	a0437181 49950587
R 7	input	05f5f77e	ae7deb90	81b0085a	63bf73c5	298c6828	9b9008dc	96406805 0677e537
R 8	input	3b17c00e	5e1787ff	153bcacf	60417464	98f7aac7	2ef49810	49203b20 e031ddbfb
output		05475e59	5b50d9a6	5856eb54	38179f30	6e23b75a	40d72f4a	61480389 8179de36
MSF_R								
input	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cb89793b	00000000	7c4cbb01	00000000	894e76a0	00000000	ab6a2a95 00000000
R 2	input	4582b27d	78cd79cc	8e3b287a	d635a167	4369b531	e11e797a	9f35b9d6 e46bdf29
R 3	input	6f1220fa	c3b5f49b	54940b63	01b04a45	34980f62	278ab2bc	44ae2904 b6485d37
R 4	input	c3f81c5f	27b88024	df1a2d77	0be6bc93	fcf9e001	b932ae28	da6ddfa1 a0ba3bc4
R 5	input	2806b3b8	ab89ce71	3d41ffff	67f60b9c	1ea8ab42	a3f67eae	bac1516c abfc14b2
R 6	input	25764152	41bca70d	a28e7730	97c03996	b4801dcc	e8f2c05b	61230217 3a42ac8c
R 7	input	a98357fb	4b17787f	01d28e22	4ea2d071	2654d09a	800b587a	8a04a61c 1d2b08ba
R 8	input	044dc5e8	b6c27a7f	59e33ea1	e3b2a2fa	4abd9eec	0654b064	17151311 c29830b5
output		9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543 d3daa5f6
CPF								
input	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
mask								01010101
T		61626380	a20fda55	00000000	29426112	00000000	12d49830	00000000 9eed0b1f
R 1	input	75652ba9	ffffff	1c7370d7	ffffff	e4edd36e	ffffff	af41063f 9e9d9c7f
T		00000000	e5a63b4a	00000000	be27151d	00000000	896a7901	00000000 ab89dba0
R 2	input	12932c55	548e32c1	eda0b2aa	42645857	26ca5e06	ba95439b	d9258c52 9e6177cc
T		6f9a5e1e	d54b17c0	a4c205ba	ce6cc2cb	dded79c9	f7ed35c1	8fc40420 d8e53beb
R 3	input	d2d5420d	9ea60a44	575287b5	c66f6b22	439619ce	98b560ed	cbfaa71c 7e9288fc
T		e46bdf29	a29ddaeb	78cd79cc	4734dcbe	d635a167	4335b27a	e11e797a 9f822831
R 4	input	ee628ee6	a9d2dcd5	bd312f9a	dec7db51	f90d0125	18555505	e47293e2 74c1db9b
T		bdad2ca8	39a4fdd8	f3e653be	a035562b	5d5c2dd8	7a986572	ec190047 7ebbbff7
R 5	input	65d25258	1d49c32d	af8e3c87	4167696d	2a5533dc	d52c2921	4cf6dd66 0a8b953c
T		b6485d37	37ca0782	c3b5f49b	2a4c14fd	01b04a45	34ae2063	278ab2bc 44120b62
R 6	input	021a3de2	707337e5	5ae671f8	113b5846	59dd152a	c3ee9126	a409465f dc0fdb38
T		4d04a215	72af5cae	d819f11a	783a28ce	c4f473ca	88ef3d0f	e94ca2dd 3a56a893
R 7	input	5ac1a610	b74d81d0	da48634c	6b3e5eee	b4f99753	3f8e2057	06ca646d 564af1cd
T		a0ba3bc4	e18d7050	27b88024	effcefaf	0be6bc93	fc6d1c77	b932ae28 daf82d01
R 8	input	d51f6134	55ac9e2c	0556bfcf	0dd9c5c9	653475ba	499b7062	d6de8574 6306e0cd
T		f9b53c36	5c7365b0	41abf8d2	9ba9239b	7afb7576	13bd9109	dc559f18 5b046a38
R 9	input	de3b2c23	c3826fc9	f0689080	de1b9bcc	be1cba6f	37472f19	37c3fc86 69c8c2d6
T		abfc14b2	1420d5b6	ab89ce71	1ed428dc	67f60b9c	1ec1b3fc	a3f67eae ba06ff42
R 10	input	d121a30e	42019eda	12e25dd8	2d3b1830	e3c95547	218d6b2d	2241a599 e5b684a1
T		49950587	4e560502	2ed27264	a99ce21f	b53cde68	69432752	4a5760bd a027c3d2
R 11	input	40d167cd	13921988	396b8d06	af2fc600	5294e631	70f46452	f7c82a5d 522387e8
T		3a42ac8c	12c70e8b	41bca70d	d1400129	97c03996	b4234130	e8f2c05b 617677cc
R 12	input	a4ae2ce2	37cbcd41	0187bf8b	c63c3c6e	958d81d3	1bf9c8e7	8501f0a2 f71ac5f8
T		0677e537	0b60d00b	ae7deb90	0318d0fc	63bf73c5	2940f75a	9b9008dc 96f50828
R 13	input	3af9471f	b44318de	922baf17	4668797e	177c68c4	51ff6970	083ab127 167d6ff1
T		1d2b08ba	d4e9680e	4b1778f7	00aa537d	4ea2d071	26045722	800b587a 8a838e9a
R 14	input	838cb4e8	d9b22e29	6fb5fd7c	ad05d44e	94605099	9decbb15	e1f4b3f5 14bed7c8
T		e031ddbfb	76775440	5e1787ff	2bee761c	60417464	9820c0f8	2ef49810 4917cac7
R 15	input	35fd097c	4ad7794b	86f1d2ca	899cd227	dd0498c4	626b0d2a	20e9bbe6 c0bef137
T		c29830b5	0271cf08	b6c27a7f	acde89f4	e3b2a2fa	4a15c5a1	0654b064 174d3eec
R 16	input	1d151bc1	54359ba0	8466cb49	00e20f7a	960e7edb	f3d6b901	3b76c94f 8d81541e
T		05475e59	b6a1b34c	5856eb54	702f3e60	6e23b75a	40d72f4a	61480389 8179de36
R 17	input	d8f2d7a7	251e9a0f	6b40aee	c839604a	b3f4fb50	0e71015e	eeabf9c8 cdbfd432
T		9143bac2	93c0e05e	7688bebb	ca9d0e20	549bad3e	52cf1d5a	11429543 d3daa5f6
output		af0223e3	889fe370	d33fe33d	a71333ec	95efc89b	9dca79a1	f258b491 fd7f5016
output		50fddc1c	77601c8f	2cc01cc2	58ecc13	6a103764	6235865e	0da74b6e 0280afe9

AURORA-512 (M_1 : 1 block message)

$MS_{L,0}$								
input		61626380	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	d06c99c9	00000000	85b16108	00000000	1ce9e324	00000000	16a3f45c
R 2	input	587e39b0	40502cd6	6a73c3c5	bdd1dac3	ae288de8	072f6edd	530949e9
R 3	input	2f43b0aa	a7ad5f65	5bba6871	c29c2534	48e1ac7	406aac69	4f7304b0
R 4	input	2d56841b	3ef26a90	0f58c082	db32b10b	6e3bb3d6	f51d2516	46fa07bc
R 5	input	88d78b78	ec9b92a0	a84517db	84bbbecc	654e0783	cd238a2d	9d8dd96a
R 6	input	51ed60ec	f36afc3d	279fc6a2	3cdf7dcb	a1034f74	ff24f444	73518c25
R 7	input	65963589	aaa23cc4	5d348706	e3d21b75	3f523ba5	739eda91	88167213
R 8	input	4be55ff9	2f8a5dc5	c9259fb9	1a319a70	24b9e8f7	cb5965ea	c98bba4d
output		b3657bed	9cef2628	49042202	5335b872	acbc4c3	67e5d129	832ae0de
$MS_{R,0}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cd991fb3	00000000	60a599cb	00000000	0e357107	00000000	9a51b2ae
R 2	input	99e09a92	de175c14	0b164a1a	da1fecce	4bd0c990	9b126664	65a79c85
R 3	input	717d5404	7abadec1	788127c0	031e483f	461e3244	4139a10e	7bb80eb1
R 4	input	77e71c40	51a68c42	bc9f4c1d	c17af6b4	625af1a9	12009496	20c6a1be
R 5	input	25098541	6c025baf	a4872a66	f041cabf	e800d5c1	55aee88f	c054d2a5
R 6	input	26554ea2	7cbbb6de	1c46a563	997bbe01	e464ba1b	792d60cb	c883e59c
R 7	input	d969560d	1a6c957c	20d99453	a203acd4	52f6817e	59b07836	ea8a4d28
R 8	input	bf6d27a9	961993de	443c6b27	9a7157ea	7d2ec78d	72942327	7707fceb
output		3f5d49f9	a944da27	2ad57a20	b0a42dca	cd8681f4	bf12a2d3	ce73702b
$CP_{L,0}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626380	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000
R 1	input	c95a55f7	00000000	c93b518c	00000000	122737b6	00000000	1df21317
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000
R 2	input	37b73248	dd352477	2ddb7706	dfd0125b	cd44f561	287fbfeb	e62398b5
	T	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd
R 3	input	e48fd135	e8f6a16b	b66b646d	0876fc03	3a1a86e7	130480b7	973d3e20
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664
R 4	input	12fb90fb	d1cb08a8	296defe4	5dd08b2e	fccdc33c	6dc7b479	c01c6768
	T	ddcbf259	5f755960	a7ad5f65	b7c20954	c29c2534	4873b071	406aac69
R 5	input	5f89835d	fc9dccc4	916e5596	9785df66	36eceed8	a89bbe62	1b4dc1e6
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e
R 6	input	2d920d0b	159261b9	f5bc62f0	7ec95a5a	2ed4f3f9	8c0c53cb	6c9c1f50
	T	5aace684	5ab16778	3ef26a90	1e760e36	db32b10b	6efa8482	f51d2516
R 7	input	31633c33	2b53f390	8cceccf0	53fb1642	10b4991e	840119a7	3fee6900
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496
R 8	input	371a055f	e5f08a84	6481c70b	e77b614a	0544b958	ee98ccae	7bcc8a26
	T	ef0f862e	108a0ed5	ec9b92a0	509db2f1	84bbbecc	658d8bdb	cd238a2d
R 9	input	a523091c	20cd356e	b431d427	3d40789e	b8434b26	b0994e84	65fb893f
	T	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f
R 10	input	8e813417	017913b2	90a16f9d	10ab835e	accc324e	8a28713c	8e0ca747
	T	63f972d7	a33e9e4a	f36afc3d	4e0719d8	3cdf7dcb	a15160a2	ff24f444
R 11	input	5521d484	1d9a8431	183790dc	f3b4732b	cc359759	05e6d20c	eb448595
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb
R 12	input	75d2ae43	ed1f74e0	4d238c09	ba9ebdbd	921f616c	b8ac25f4	6a2cf0f8
	T	05d01b31	ca687626	aaa23cc4	baa4e512	e3d21b75	3f163506	739eda91
R 13	input	e45d3184	6156822c	ae497782	1147571e	e4593797	81761c1c	d8df7f5b
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203acd4	528a5653	59b07836
R 14	input	1d315813	11ae0216	4d79a341	bc8d1a43	de3c26df	24fdb490	fe3b2a6d
	T	b7666652	964bd09b	2f8a5dc5	937375f2	1a319a70	248b5fb9	cb5965ea
R 15	input	8580c138	142cb368	963501d5	98b5b120	a4a891bd	464cc2f8	3a607f27
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327
R 16	input	fb67310f	c6847de3	8a4eadb4	a45a9276	7856b87e	d92b0b4e	f3ec46d7
	T	b3657bed	39de4c50	49042202	a66b70e5	acbc4c3	67e5d129	832ae0de
R 17	input	9f458bac	7dbaad9e	3311d7a4	9a99c841	43b2a18d	97883f13	425b5ea8
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b
output		547269d8	4237e0ac	b2dd7506	dac3d182	c1cc02ca	24d01efe	3c03f932
output		547269d8	4237e0ac	b2dd7506	dac3d182	c1cc02ca	24d01efe	3c03f932

$CP_{R,0}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626380	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000
R 1	input	e3ddfdb5	00000000	1ca4e528	00000000	6e744bb4	00000000	4f2d3aca
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000
R 2	input	1a03e75c	884d5f33	bb4bfdcd	632904b6	880cf0d8	35619736	6769ad1c
	T	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd
R 3	input	c03dd7a8	d89f7f30	86099ac8	5bdc2fe0	3257111f	666d5fd9	c00651bc
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664
R 4	input	35978bbe	9850106e	c490a0a5	0c0dcfe1	e00f56bf	21d7c709	905f259a
	T	ddcbf259	5f755960	a7ad5f65	b7c20954	c29c2534	4873b071	406aac69
R 5	input	f1d716a8	86cf1c49	9cd2b108	85c9aa26	19db63eb	98ee6ee6	b7f2810b
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e
R 6	input	66818902	240f5c5a	ec42203a	3219529e	04c0801f	5ef6ae77	3916ef41
	T	5aace684	5ab16778	3ef26a90	1e760e36	db32b10b	6efa8482	f51d2516
R 7	input	a5402b7b	806c59bc	5fba2af0	8132d78d	bca47bee	827f4f4f	db864d27
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496
R 8	input	3c1eb3ec	f2d5ef5d	922abf42	d779acda	de4aad51	9574958b	3feeb730
	T	ef0f862e	108a0ed5	ec9b92a0	509db2f1	84bbbecc	658d8bdb	cd238a2d
R 9	input	82deae56	bb77af93	afc7ab45	6a0d4edd	4e97a7e5	50b7b31c	a6e3c8ac
	T	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f
R 10	input	df6c2e3b	17e6bec9	54db6f9c	685966a9	816eccdd	b608c678	dea63702
	T	63f972d7	a33e9e4a	f36afc3d	4e0719d8	3cdf7dcb	a15160a2	ff24f444
R 11	input	9aa11f68	c745cf51	519fe56d	4e92996d	273af7de	9a0afc31	80a274d5
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb
R 12	input	e6f6bc6b	46789e30	733b40d7	a4903e56	c68ab3d7	df480711	9f035fd2
	T	05d01b31	ca687626	aaa23cc4	baa4e512	e3d21b75	3f163506	739eda91
R 13	input	27af6482	a02ea319	381d9c9e	943e2520	1804acea	50cc939b	d2318a92
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203dcd4	528a5653	59b07836
R 14	input	3fb70328	ce0c60f8	6e01a8d4	a195be00	9b3356e2	8a6dc642	e89e911e
	T	b7666652	964bd09b	2f8a5dc5	937375f2	1a319a70	248b5fb9	cb5965ea
R 15	input	7ef10162	dd213c71	d7f0c265	be907f8f	3ecafcd	db522dfd	a8d75b1a
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327
R 16	input	c6817e63	f0ce4c51	797841bd	4b94ac36	9b1b239c	feb77809	bad0e43a
	T	b3657bed	39de4c50	49042202	a66b70e5	acbc4c3	67e5d129	832ae0de
R 17	input	f85e342d	3e9f1ae4	b3ab9614	db3e43f9	b38d47e3	15a9b6e0	75517953
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b
output		b5eecac3	e08ef4cd	dce5f2c4	f55cddf8	baf1a7bd	ddcc327a	7f765da4
output		b5eecac3	e08ef4cd	dce5f2c4	f55cddf8	baf1a7bd	ddcc327a	7f765da4

AURORA-512 final mixing (M_1 : 1 block message)

MS _{L,9}									
input		547269d8	4237e0ac	b2dd7506	dac3d182	c1cc02ca	24d01efe	3c03f932	1975b525
R 1	input	9219874b	b2dd7506	5f86d4f6	c1cc02ca	382a0301	3c03f932	0f7325f0	547269d8
R 2	input	7b3a4e00	ca92f9ac	21ada6d7	c18354e3	ee268964	c07b0109	a1589ec2	63cf10e3
R 3	input	c11a7927	1fe733c8	9f88a924	881783b5	c5f977b7	2f301c04	b1ace648	b93bfcdb
R 4	input	8d45d877	b26d4b7d	c9e3826a	aeba5d8e	742f1223	dfef6961	08288076	425d2be3
R 5	input	dc1de06f	82b7e932	b3adab04	8f379964	44ea8d47	c218fb8e	8ae24e77	37782dde
R 6	input	ff1d5e33	f12f484a	2e6f315b	e5c43291	77ca96c3	eca3a803	b8711fbe	a325d0de
R 7	input	d6a882bb	6d4ff3ac	439b497c	c578f048	0aa479c3	0f7cb6fe	343bf21e	b43aed4b
R 8	input	8c8fe39f	65bb9e9e	a58271b8	ce914a1e	8c22f631	fed97d56	4fc99246	b72cb731
output		aaa56e4d	cf1ef0d3	bd87d050	73169a4e	8f94f10f	734d8c59	094589a3	be693e92
MS _{R,9}									
input		b5eecac3	e08ef4cd	dce5f2c4	f55cddf8	baf1a7bd	ddcc327a	7f765da4	ce8450c9
R 1	input	2d1d2d4b	dce5f2c4	952bc9b1	baf1a7bd	d36985cf	7f765da4	549d6f63	b5eecac3
R 2	input	19d73043	d1957d78	be2bcbfe	51641b8e	bfa3a173	4ecb2d44	05aa1a4a	6174bdc9
R 3	input	83e108b0	5988bb35	d0394187	8bae5f58	1b5748a7	997d5de6	ffd19c3c	fa59940f
R 4	input	6c8e31a8	72a01acd	174544b4	213327f5	5aec0549	7353c797	bccb20fc	ac0423b3
R 5	input	4944522f	0b943980	236071e4	b36e4e3c	cadfbabb	d20b2243	7f286149	32e1d16e
R 6	input	85fedc7e	5c266481	7f163741	4060e6ef	bad64fb4	0f670f77	f13db354	4401217d
R 7	input	56834ca8	036a1837	e0fc537e	0b58a945	8deb8340	b79c28ef	c09b9801	32f811db
R 8	input	2c4ff201	2a7355e7	51117182	8828d296	811f6c66	fc0ee9ba	56724fd3	f5eeb5dd
output		a264dcd7	88178930	1c0445f8	942c976e	1947c37c	e5492ac6	2b7a1d15	de94a8c8
CP _{L,9}									
input		547269d8	4237e0ac	b2dd7506	dac3d182	c1cc02ca	24d01efe	3c03f932	1975b525
	mask								09090909
	T	547269d8	250c07e0	b2dd7506	be544a97	c1cc02ca	387387f6	3c03f932	0f19d401
R 1	input	0f535571	00000000	a663588c	00000000	126316bf	00000000	14f261e2	00000000
	T	b5eecac3	9695c2b1	dce5f2c4	cab4b7a5	baf1a7bd	d39d2db1	7f765da4	541dc9cf
R 2	input	b7d62d05	7b253a02	ad2ca576	89f998ec	fc1f253d	75870a52	62371a42	0f1dce6d
	T	63cf10e3	f75b1384	ca92f9ac	424d3c00	c18354e3	ee584ed7	c07b0109	a13aa664
R 3	input	a663b1d4	b733c127	a3501b31	4129d0d4	122941c9	c6af9c9a	3b99ae37	9cbe8e41
	T	6174bdc9	8c95d0a5	d1957d78	5f518d21	51641b8e	bfaa30fe	4ecb2d44	05d7cb73
R 4	input	f32934eb	53b36f6b	37cb9616	72e26e55	79d15e5b	8766aeed	a4f3ce7f	e06c2ebb
	T	b93bfcdb	8310ee91	1fe733c8	3ff3cc4f	881783b5	c5ac7924	2f301c04	b11aa9b7
R 5	input	f8429812	a068a646	d2a50477	70dab1e7	fc509aae	24ff4407	2de7f79b	482d5ea5
	T	fa59940f	419ca41e	5988bb35	682bce58	8bae5f58	1bd10887	997d5de6	ffe141a7
R 6	input	88586a6e	f6c71af3	0676463e	b6008cd1	bfc8e32c	f1314ed1	d9e8a61b	c23037db
	T	425d2be3	1bc624ed	b26d4b7d	925f00ef	aeba5d8e	7428d86a	dfef6961	08458223
R 7	input	c5cf07cc	7ebc79d0	11df38e1	c9488024	98244449	cf0de615	643a1a1b	82afd4c8
	T	ac0423b3	362282fe	72a01acd	0bf61054	213327f5	5acb31b4	7353c797	bc8e4449
R 8	input	4a704fa3	36d93165	5b26c37a	91232861	e003ec8e	dd03b233	f2dc71dd	9d2f0eb5
	T	37782dde	b95b1aef	82b7e932	67d49cdf	8f379964	44e2e004	c218fb8e	8a1dab47
R 9	input	e937fde0	faae0005	41327bbb	4c04bee8	d01d9e00	1f3811e0	c6c7a02d	7d14ed93
	T	32e1d16e	a4b05f24	0b943980	91efb097	b36e4e3c	ca2852e4	d20b2243	7f4471bb
R 10	input	2946823d	de7f6e76	1a7d3e14	480c39b2	3af03bb3	b1826947	6a59a73c	57c05ea7
	T	a325d0de	fedf2d7c	f12f484a	5d943e67	e5c43291	77715e5b	eca3a803	b81d31c3
R 11	input	4b3bf7c1	51fe8b50	1df16d2f	db673900	d0206873	4caff912	7706a366	a70a2c1b
	T	4401217d	428b27aa	5c266481	3feb59bf	4060e6ef	ba3ddc41	0f670f77	f1fe37b4
R 12	input	a4251368	be07d9d1	27a5476f	f9cce109	1f906b34	c34e89be	0b92eebd	66d74969
	T	b43aed4b	ad36f23c	6d4ff3ac	8749e577	c578f048	0a3b827c	0f7cb6fe	34a849c3
R 13	input	28da06a7	4f22fdb6	395588c3	45e49052	d87fb2ea	2ca8a046	b419933a	46991a93
	T	32f811db	2b7e4180	036a1837	f075cc54	0b58a945	8d9b4c7e	b79c28ef	c0835340
R 14	input	f8cbd0b7	078d8f67	f637683c	09dc41d8	b0b46341	bb78b5d0	e5fe0790	ded622cb
	T	b72cb731	1905ec8d	65bb9e9e	4a45253f	ce914a1e	8cc9e3b8	fed97d56	4f8f7131
R 15	input	cb297946	90333e1b	3475743a	0f336ae0	d0e12562	dd162351	ba813afa	c9a1284c
	T	f5eeb5dd	9608b669	2a7355e7	a88fa780	8828d296	8172f282	fc0ee9ba	564f7166
R 16	input	5ef4acb1	64075470	0974fd36	5449be84	fdad1d3fe	6776e5668	c389ab19	188a6cc5
	T	aaa56e4d	9e3de1a6	bd87d050	e62d349d	8f94f10f	734d8c59	094589a3	be693e92
R 17	input	b08f68bd	8207fd57	88d4fce2	4ec36e9d	1ed940f1	5899d957	66c494ee	69d6af3a
	T	a264dcd7	440bc498	1c0445f8	4a164bb7	1947c37c	e5492ac6	2b7a1d15	de94a8c8
output		3e3e9f09	5a567a11	5a1455d3	42c53501	0d5c63a5	a9cb5348	85894385	19b15962
output		6a4cf6d1	18619abd	e8c920d5	9806e483	cc90616f	8d1b4db6	b98abab7	00c4ec47

CP _{R,9}									
input		b5eecac3	e08ef4cd	dce5f2c4	f55cddf8	baf1a7bd	ddcc327a	7f765da4	ce8450c9
	mask								09090909
	T	547269d8	250c07e0	b2dd7506	be544a97	c1cc02ca	387387f6	3c03f932	0f19d401
R 1	input	8725d149	6e3887c2	5c4509ac	7b3da577	97af7e51	4375a496	9131445e	e19ca31b
	T	b5eecac3	9695c2b1	dce5f2c4	cab4b7a5	baf1a7bd	d39d2db1	7f765da4	541dc9cf
R 2	input	ee9a7937	190fa017	7796c0d0	1390abfa	dc38176d	d1fd6e7d	bb986b95	798282c9
	T	63cf10e3	f75b1384	ca92f9ac	424d3c00	c18354e3	ee584ed7	c07b0109	a13aa664
R 3	input	d9d16199	7d1ac557	4f95694b	775e991a	c6b486e0	10d47f99	d51b3e1a	fef195f4
	T	6174bdc9	8c95d0a5	d1957d78	5f518d21	51641b8e	bfaa30fe	4ecb2d44	05d7cb73
R 4	input	00a42016	a974ba38	0cfe75f7	cdfe1957	28920054	fa62c0d1	a963db2d	dbab4c6c
	T	b93bfcdb	8310ee91	1fe733c8	3ff3cc4f	881783b5	c5ac7924	2f301c04	b11aa9b7
R 5	input	38627527	c9b39bc6	22a34ff9	29f7a1db	a92f5ac2	a47c2a57	1f2d7928	63793aa4
	T	fa59940f	419ca41e	5988bb35	682bce58	8bae5f58	1bd10887	997d5de6	ffe141a7
R 6	input	4de85961	e9d6af6a	7ac1b656	a1e28d63	7e31057a	0f8e8116	7da6bb29	b0edba44
	T	425d2be3	1bc624ed	b26d4b7d	925f00ef	aeba5d8e	7428d86a	df6e6961	08458223
R 7	input	b87893a8	f4b493a6	b8ad7fae	35bef0df	36312d3a	3c277950	e8287704	4984a417
	T	ac0423b3	362282fe	72a01acd	0bf61054	213327f5	5acb31b4	7353c797	bc8e4449
R 8	input	b5c0e0de	d6efd646	745bd794	5c9235fb	332140f5	c8d18426	1f197f2c	4750a56e
	T	37782dde	b95b1aef	82b7e932	67d49cdf	8f379964	44e2e004	c218fb8e	8a1dab47
R 9	input	b3ac5288	9c8273d0	5ac6223e	91b4ef7c	e2ec5b90	cc913296	e31cd8fd	8de915db
	T	32e1d16e	a4b05f24	0b943980	91fef097	b36e4e3c	ca2852e4	d20b2243	7f4471bb
R 10	input	012cf454	8aceb79f	363dc3c8	1bd26e76	0f86f7e7	1334887d	2e5824b2	99f95488
	T	a325d0de	fedf2d7c	f12f484a	5d943e67	e5c43291	77715e5b	eca3a803	b81d31c3
R 11	input	11db7463	82d9f64d	76721cbb	9268cd1d	51fb1031	f78f0809	bc5fd6c3	bdb0e7b5
	T	4401217d	428b27aa	5c266481	3feb59bf	4060e6ef	ba3ddc41	0f670f77	f1fe37b4
R 12	input	55275d71	cd9bb96b	3591611e	4b3fe16b	c3d7e5b6	0d892d15	808cd5b7	79f76fb1
	T	b43aed4b	ad36f23c	6d4ff3ac	8749e577	c578f048	0a3b827c	0f7cb6fe	34a849c3
R 13	input	39aa2720	3dbe4c8b	b0eaf27f	c5ac1082	883b7925	af44d42e	87e57577	a346af15
	T	32f811db	2b7e4180	036a1837	f075cc54	0b58a945	8d9b4c7e	b79c28ef	c0835340
R 14	input	dd1951cb	1be0ca20	136f853e	d936c4e3	6a45cbcd	75acf57d	99ff6956	7b78b235
	T	b72cb731	1905ec8d	65bb9e9e	4a45253f	ce914a1e	8cc9e3b8	fc9d97d6	4f8f7131
R 15	input	e8a250ce	72522ba8	93dd6c01	98cb71bb	9b1ddc49	a5365fa2	79afa50b	069286fa
	T	f5eeb5dd	9608b669	2a7355e7	a88fa780	8828d296	8172f282	fc0ee9ba	564f7166
R 16	input	82d931c2	49364c29	50238ece	a9d6c1c3	e94ae89a	b89b09cc	96daf5c5	3acbd344
	T	aaa56e4d	9e3de1a6	bd87d050	e62d349d	8f94f10f	734d8c59	094589a3	be693e92
R 17	input	f582198f	735ee599	a80b339e	8cb7070a	95cba4be	4ea3e41e	0f745dde	c44cc560
	T	a264dcd7	440bc498	1c0445f8	4a164bb7	1947c37c	e5492ac6	2b7a1d15	de94a8c8
output		30046cfa	a535912c	8e3abbc5	549fb280	26a9d8b4	9404d510	dfde8a7a	ee7cfac7
output		85eaa639	45bb65e1	52df4901	a1c36f78	9c587f09	49c8e76a	a0a8d7de	20f8aa0e

AURORA-384 (M_1 : 1 block message)

$MS_{L,0}$								
input		61626380	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	d06c99c9	00000000	85b16108	00000000	1ce9e324	00000000	16a3f45c
R 2	input	587e39b0	40502cd6	6a73c3c5	bdd1dac3	ae288de8	072f6edd	530949e9
R 3	input	2f43b0aa	a7ad5f65	5bba6871	c29c2534	48e1ac7	406aac69	4f7304b0
R 4	input	2d56841b	3ef26a90	0f58c082	db32b10b	6e3bb3d6	f51d2516	46fa07bc
R 5	input	88d78b78	ec9b92a0	a84517db	84bbbecc	654e0783	cd238a2d	9d8dd96a
R 6	input	51ed60ec	f36afc3d	279fc6a2	3cdf7dcf	a1034f74	ff24f444	73518c25
R 7	input	65963589	aaa23cc4	5d348706	e3d21b75	3f523ba5	739eda91	88167213
R 8	input	4be55ff9	2f8a5dc5	c9259fb9	1a319a70	24b9e8f7	cb5965ea	c98bba4d
output		b3657bed	9cef2628	49042202	5335b872	acbc4c3	67e5d129	832ae0de
$MS_{R,0}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cd991fb3	00000000	60a599cb	00000000	0e357107	00000000	9a51b2ae
R 2	input	99e09a92	de175c14	0b164a1a	da1fecce	4bd0c990	9b126664	65a79c85
R 3	input	717d5404	7abadec1	788127c0	031e483f	461e3244	4139a10e	7bb80eb1
R 4	input	77e71c40	51a68c42	bc9f4c1d	c17af6b4	625af1a9	12009496	20c6a1be
R 5	input	25098541	6c025baf	a4872a66	f041cabf	e800d5c1	55aee88f	c054d2a5
R 6	input	26554ea2	7cbbb6de	1c46a563	997bbe01	e464ba1b	792d60cb	c883e59c
R 7	input	d969560d	1a6c957c	20d99453	a203acd4	52f6817e	59b07836	ea8a4d28
R 8	input	bf6d27a9	961993de	443c6b27	9a7157ea	7d2ec78d	72942327	7707fceb
output		3f5d49f9	a944da27	2ad57a20	b0a42dca	cd8681f4	bf12a2d3	ce73702b
$CP_{L,0}$								
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask							00000000
	T	61626380	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000
R 1	input	36a5aa08	ffffff	36c4ae73	ffffff	edd8c849	ffffff	e20dece8
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000
R 2	input	8c0455fb	0f5b083b	00dd9430	efbd8a92	02d577d5	9f3aa3a0	aeb14bf0
	T	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd
R 3	input	b49b324e	9d0f1dd9	f3c95f59	7f44037c	328e4fda	cfe9c630	0f4a1a73
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664
R 4	input	9958320a	e3688626	a4e3dc80	acb06fcd	d15c200e	61a86254	4e911675
	T	ddcbf259	5f755960	a7ad5f65	b7c20954	c29c2534	4873b071	406aac69
R 5	input	505d03e2	24600498	b89da52c	9aa189f1	3771651d	74381108	3906fdae
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e
R 6	input	22155636	e63efa13	0b1a4e92	96c4ae52	1a5c71c8	82db7a3c	5f32d25b
	T	5aace684	5ab16778	3ef26a90	1e760e36	db32b10b	6efa8482	f51d2516
R 7	input	88baa664	b13f69cf	fee555c4	19aca581	54d56f00	e283daee	8e6e07c7
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496
R 8	input	c7c078d3	ddaf10cb	16d35428	ccacdff20	484cc0c7	3ac5325c	e599a3e5
	T	ef0f862e	108a0ed5	ec9b92a0	509db2f1	84bbbecc	658d8bdb	cd238a2d
R 9	input	59f6ad77	5f3ae56f	e0fc4251	4f07221a	1e633397	ad723ba9	12e1e738
	T	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f
R 10	input	82404647	210deb66	c2d787b5	3887845b	99f8caf2	f87b7bc8	38cb052b
	T	63f972d7	a33e9e4a	f36afc3d	4e0719d8	3cdf7dcf	a15160a2	ff24f444
R 11	input	7642ff6d	ca9a5edd	e786b7a4	c94152a7	84190926	2004dd1e	bde258ce
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb
R 12	input	e777d362	9ecae34d	04b2013c	dcd8cf9a	d13f648d	2ccce9a	fd8846b2
	T	05d01b31	ca687626	aaa23cc4	baa4e512	e3d21b75	3f163506	739eda91
R 13	input	a50a6bfd	9de3da72	346859cf	308ae63d	51aa4844	2fb0ed69	3372554a
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203acd4	528a5653	59b07836
R 14	input	738db173	6d3c0455	10f1ca9a	139902ed	df63e771	5fb53b82	b7e99d08
	T	b7666652	964bd09b	2f8a5dc5	937375f2	1a319a70	248b5fb9	cb5965ea
R 15	input	232c3d51	3e6e12af	1335ba4a	a78dcccad	e0fe5d8a	13dde0f4	fd10c677
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327
R 16	input	ff4aff4f	877fb62e	f43cf241	19267e8f	909516b3	bf949e90	4f01f0c4
	T	b3657bed	39de4c50	49042202	a66b70e5	acbc4c3	67e5d129	832ae0de
R 17	input	e9e5a4fe	0f0aa135	fcf25801	0835723a	b77ee382	ae18bfc8	5548be78
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b
output		c9bcd052	ad49558d	5f436533	a5f17bcc	77c6ef75	ab4a739a	b6ab2190
output		36432fad	52b6aa72	a0bc9acc	5a0e8433	8839108a	54b58c65	4954de6f

$CP_{R,0}$									
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask								00000000
	T	61626380	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000	166c6124
R 1	input	1c22024a	ffffff	e35b1ad7	ffffff	918bb44b	ffffff	b0d2c535	9e9d9c7f
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000	9a999907
R 2	input	ccd402c7	bd136b57	71b53e8b	faa21e0f	eead1371	7449ab60	d91d6683	0fcf4e47
	T	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd	537ec3e8
R 3	input	1f5ad190	c33246b1	04a20721	5175155f	7971688a	3d0bde2c	b2877276	4a65c9a3
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664	65e04a90
R 4	input	3b245eda	eaecc5b5	bccff1b4	582e9b05	ef1a8386	7591db9e	2e1aca82	c2746249
	T	ddcbf259	5f755960	a7ad5f65	b7c20954	c29c2534	4873b071	406aac69	4f4368f7
R 5	input	1f62413f	9c72bb3a	d2379e0e	48e7e1b7	80455e36	aca9ada2	969a7227	bfe0f855
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e	7b7d2744
R 6	input	6b9e53fe	6a378837	6fc1e79a	9c1e4b7a	9ed66f65	d0b081fa	2b567032	474a9604
	T	5aace684	5ab16778	3ef26a90	1e760e36	db32b10b	6efa8482	f51d2516	4656c0d6
R 7	input	8c7b05d0	16eebff3	6705b72a	aadad6da	1921a6da	f67a9a7b	b828b23f	a74b8683
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496	20e74ca9
R 8	input	3888303f	8dc4d6d9	c621233a	9b74fa96	e6b3ab1c	cc6500b3	01e68f1e	1d75899e
	T	ef0f862e	108a0ed5	ec9b92a0	509db2f1	84bbbecc	658d8bdb	cd238a2d	9dd71783
R 9	input	9617129a	9270c313	cae3367c	323467dc	4f9d6968	b6f7cef0	d2cbf298	824198eb
	T	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f	c0092ac1
R 10	input	32f941df	11d3702c	0ac8671c	01c174c5	0e62c764	6da83971	6e7ed04a	dd6c9c6e
	T	63f972d7	a33e9e4a	f36afc3d	4e0719d8	3cdf7dcf	a15160a2	ff24f444	73edc674
R 11	input	4151b599	fe1a94cc	01965567	403ccc6e	f2fdbb82	88ee2ba5	56ac3dff	eb749a05
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb	c855a51b
R 12	input	fdb2906b	8abd9a33	b1411a2f	679cc53a	17e1eb4b	8e30df42	13eb0e00	388aee84
	T	05d01b31	ca687626	aaa23cc4	baa4e512	e3d21b75	3f163506	739eda91	889687a5
R 13	input	348a7209	5cf582fe	07e73859	6575ebb4	b8d3f48d	c4cc34b3	640250cd	3fd97397
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203dcd4	528a5653	59b07836	ea69947e
R 14	input	e50bfdfa	6516c3be	3483d3f9	2a29e705	8462fcc1	4deee13d	f022fcf7	4af51a83
	T	b7666652	964bd09b	2f8a5dc5	937375f2	1a319a70	248b5fb9	cb5965ea	c9e59ff7
R 15	input	d672dcfb	dad835ed	5b1b39e3	f7da8576	b08fea0b	0e885d25	5b1e0b81	c9a6549b
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327	776d6b8d
R 16	input	03fef40b	b348c8c0	73150e6c	468d563f	43d7e754	2139821c	66139ab8	d0ca3193
	T	b3657bed	39de4c50	49042202	a66b70e5	acbc4c3	67e5d129	832ae0de	344c868c
R 17	input	2c51c887	9a87ae47	1a9afa02	cc6145fa	7b8cd864	c9321779	6b803708	59808509
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b	b1b6e385
output		14461998	e53e9335	492729da	77c100e5	f05ee464	4bf8d03a	61e9ea48	47acfcef
output		ebb9e667	1ac16cca	b6d8d625	883eff1a	0fa11b9b	b4072fc5	9e1615b7	b8530310

AURORA-384 final mixing (M_1 : 1 block message)

MS _{L,9}									
input		36432fad	52b6aa72	a0bc9acc	5a0e8433	8839108a	54b58c65	4954de6f	5b3a1b65
R 1	input	825615fa	a0bc9acc	df077a6d	8839108a	48e74941	4954de6f	4d16702e	36432fad
R 2	input	559dff2d	b3732e3e	115b53b3	320ac2da	6832a626	08edb23e	0b865b6c	5f58d087
R 3	input	8da6ab29	b5be85ff	c6a4cab4	764ae212	f3290129	551bbffe	f767c649	8cf65d48
R 4	input	eff71a7a	c33287d7	4671cb39	a1a53c27	012df6c2	ac818113	4e1c2dce	8a96796c
R 5	input	3006c844	cf5253b0	f195d1ce	827759dc	3a1062a6	c0c8d3e0	40dd955e	aa1f0e5d
R 6	input	4cb5e55d	669a2d9c	b4f0b438	7208a19c	e23f9696	616c0ed5	a86dba13	5d5f6af1
R 7	input	3a491800	22a9871a	9b4cb338	4c92ccda	0e8ebe59	bfe7f64b	7a1e157c	cf584fff
R 8	input	d0995a2c	f7189abf	be42c1a9	77beb3ba	856b7669	e4ad6fba	2c7daa8c	a40a434d
output		02c242d8	f5dad867	0102103f	76bca385	8796cf9d	633ba027	89b1894c	2dbbca01
MS _{R,9}									
input		ebb9e667	1ac16cca	b6d8d625	883eff1a	0fa11b9b	b4072fc5	9e1615b7	b8530310
R 1	input	d7ca30a9	b6d8d625	e8649a0e	0fa11b9b	ba0b1d16	9e1615b7	22564d64	ebb9e667
R 2	input	f84828cf	d452b6d2	0e2ea126	85a24b45	8a340089	55036b1a	400c6dd6	ea4c380f
R 3	input	c66a24eb	216849a5	7ca53beb	48c3356a	c3718853	51cea2d4	bc743e57	ba029fce
R 4	input	f4f8bda0	b2baf7f7	14ad3c1f	4573546c	f69ba23f	257eb420	aa38a7a8	4c0c7677
R 5	input	fa72333b	9313820d	df491647	b99a5c28	9618b236	e835100a	a5f1a927	41d2303a
R 6	input	6ee227b1	7663e35a	5f38e8fb	74862f1c	b467e1d3	1e483144	93e526bd	37a83419
R 7	input	9c6c128a	45a409e6	920158bc	9071c9b4	07c3f258	55da3693	519d402a	d240e72b
R 8	input	67c6baf2	9e1337e5	7e7579b9	dbfa84d1	30562a39	8f3f1715	c5e64d0b	f844e2d4
output		57ff38eb	c9ec0f0e	cba067a4	105ae375	15d70cc4	9ae81bd1	57456ec4	af018c10
CP _{L,9}									
input		36432fad	52b6aa72	a0bc9acc	5a0e8433	8839108a	54b58c65	4954de6f	5b3a1b65
	mask								09090909
	T	36432fad	040e925d	a0bc9acc	bfccee1f5	8839108a	4816156d	4954de6f	4d567a41
R 1	input	3e5355a2	00000000	27e0588c	00000000	1234c9bf	00000000	14f29f81	00000000
	T	ebb9e667	ebb20eb2	b6d8d625	7405a6d4	0fa11b9b	ba56300e	9e1615b7	22ca9a16
R 2	input	30099d63	401344f4	42c07805	1fbf8906	b6a51aed	13efcc48	93ea5148	ab8111c0
	T	5f58d087	aab74cd8	b3732e3e	2264b7a4	320ac2da	6886fffb3	08edb23e	0b9d5326
R 3	input	2a85412b	c5f5d204	5eeae815	a058c1b7	e0616334	d4e4f6bf	efd7f0f8	4a494d40
	T	ea4c380f	fc170036	d452b6d2	871a36e7	85a24b45	8a0c2826	55036b1a	4048a189
R 4	input	39b5ba67	faeeec3e8	a2257d0d	1cf0c278	e471fab3	115aaa80	baca2371	a3feccc3
	T	8cf65d48	1b480293	b5be85ff	8c538c53	764ae212	f367abb4	551bbffe	f7a6ca29
R 5	input	d5f27cc7	c0502295	c516ac47	d5f4e2ad	07839b4e	f94acefb	8f6329ed	61569ec1
	T	ba029fce	e352c42b	216849a5	be389f75	48c3356a	c37424eb	51cea2d4	bc6a3b53
R 6	input	9f8d3e0f	0134d265	fac9c992	ba2314df	75e613e5	8da784ba	07b69eb6	57222851
	T	8a96796c	dee3ed9c	c33287d7	8c5a5af5	a1a53c27	011c1a39	ac818113	4ef7cbc2
R 7	input	462dabca	8935fc68	8536cfe4	263445b0	71d412a5	4430afe0	4ffb91d5	fb5bd16e
	T	4c0c7677	7a56d154	b2baf7f7	0a4dd3d0	4573546c	f638bd1f	257eb420	aaf83c3f
R 8	input	51ba9d49	de81e0a5	9d869109	be314cd5	8c86c2c0	3366ee1a	25404b2f	dd7aa391
	T	aa1f0e5d	612ac4bd	cf5253b0	e2212a88	827759dc	3addc8ce	c0c8d3e0	4006d1a6
R 9	input	7f91c269	0b3032ed	5767d8bb	820235b3	8381efef	740048a4	25dbfab7	460fb018
	T	41d2303a	fd24d913	9313820d	ef8c549d	b99a5c28	96f13347	e835100a	a5721636
R 10	input	f6231d0d	4ac4b09a	a61a9856	ad888c03	e2a98d3e	e6f4c785	e6c8ad85	539ebd95
	T	5d5f6af1	99e12c27	669a2d9c	687f74ba	7208a19c	e26de538	616c0ed5	a8b5b496
R 11	input	20da0b3f	a3769914	a8ac0b89	dc97430a	8272a6a6	ab775f76	09502b97	c1a88772
	T	37a83419	b71c70de	7663e35a	afb39358	74862f1c	b4e527fb	1e483144	93e2e8d3
R 12	input	5afbdea2	e1967b2d	c5826844	a344b80f	98ec3ebb	fa01ec0c	27fc7b61	ec464ce1
	T	cf584fff	74997cf9	22a9871a	371c2a00	4c92ccda	0e1e1838	bfe7f64b	7a49b359
R 13	input	3b14392a	c2015cfc	11e260fc	0e2c6c09	27674c6f	f48df764	1851d058	a8726a7c
	T	d240e72b	4e00f915	45a409e6	4961a045	9071c9b4	079d12bc	55da3693	516c5858
R 14	input	938f1ab1	82a51ffa	c7e67682	9ffae277	ef8e8dea	687ecf0f	abd21699	bde223ed
	T	a40a434d	a084ed19	f7189abf	7cd75459	77beb3ba	857d5aa9	e4ad6fba	2c99c169
R 15	input	7dfad9c5	9e26cd70	087029b7	5ec0f1f8	e2e38ddb	6b93dd7a	14ef1fc9	502be50a
	T	f844e2d4	33ba9505	9e1337e5	bf2b26f9	dbfa84d1	30e6bab9	8f3f1715	c5c67939
R 16	input	13af9590	05a55b32	9a156355	9c6367b0	6134babb	dc07f39b	fe60dc4d	f3e6829f
	T	02c242d8	ebb5b0ce	0102103f	ed79470b	8796cf9d	633ba027	89b1894c	2dbbca01
R 17	input	55ef0680	2f2d10a7	5a767b38	e39ab758	100891c2	24b34442	e28013f8	30390c93
	T	57ff38eb	e4f60787	cba067a4	082d71ba	15d70cc4	9ae81bd1	57456ec4	af018c10
output		fd391ca2	611d3369	f55002a5	d547a3e3	c2f7491c	697b1a4b	81b66395	49cb8dd2
output		cb7a330f	33ab991b	55ec9869	8f4927d0	4ace5996	3dce962e	c8e2bd4a	12f196b7

CP _{R,9}									
input		ebb9e667	1ac16cca	b6d8d625	883eff1a	0fa11b9b	b4072fc5	9e1615b7	b8530310
	mask								09090909
	T	36432fad	040e925d	a0bc9acc	bfcce1f5	8839108a	4816156d	4954de6f	4d567a41
R 1	input	5cbd5ec9	16644ce9	2008f488	87980b11	8e5773c8	d742cbd8	a59fcde4	ddfac9ca
	T	ebb9e667	ebb20eb2	b6d8d625	7405a6d4	0fa11b9b	ba56300e	9e1615b7	22ca9a16
R 2	input	ec73e011	dbb982c7	9d73ee29	e2c0fcd4	65a7aa54	8ac5315f	4b64d29c	204b144c
	T	5f58d087	aab74cd8	b3732e3e	2264b7a4	320ac2da	6886ffb3	08edb23e	0b9d5326
R 3	input	1c6d60aa	43ad267c	999b6190	a5a6e0be	3a9bdf51	2590a7d8	db8cd648	9832714e
	T	ea4c380f	fc170036	d452b6d2	871a36e7	85a24b45	8a0c2826	55036b1a	4048a189
R 4	input	d6779384	d995db62	73da23af	d1703a5d	e00754f1	b8255e6a	d3c9b38f	c882aeb0
	T	8cf65d48	1b480293	b5be85ff	8c538c53	764ae212	f367abb4	551bbffe	f7a6ca29
R 5	input	bf0f3893	939d0c53	7d99c2f4	b77cc15a	bd7646f3	61af85de	f5773b7f	39370a38
	T	ba029fce	e352c42b	216849a5	be389f75	48c3356a	c37424eb	51cea2d4	bc6a3b53
R 6	input	24c8e522	e5486515	4695daff	b1f0d81d	b0d7c68c	66d858ba	c5afb287	6102858b
	T	8a96796c	dee3ed9c	c33287d7	8c5a5af5	a1a53c27	011c1a39	ac818113	4ef7c9c2
R 7	input	73f6bc19	cec990d9	fd2ccac1	db61a5e6	cb043f79	3e8b524f	0e8ab742	8375e7d0
	T	4c0c7677	7a56d154	b2baf7f7	0a4dd3d0	4573546c	f638bd1f	257eb420	aaf83c3f
R 8	input	c46d45de	44225cc1	c9d864f2	462f44b0	e392807e	4dd67fab	10bb8ea8	a0d260fb
	T	aa1f0e5d	612ac4bd	cf5253b0	e2212a88	827759dc	3addc8ce	c0c8d3e0	4006d1a6
R 9	input	9d7b7fc5	59671503	4d4c09f9	898cd144	2ca42cb9	fe0f8ea5	fe5cc377	74b81507
	T	41d2303a	fd24d913	9313820d	ef8c549d	b99a5c28	96f13347	e835100a	a5721636
R 10	input	8950086a	acbf1ff1e	ce51bd71	59575d4b	29255be5	6111a367	456e0d09	fed7f983
	T	5d5f6af1	99e12c27	669a2d9c	687f74ba	7208a19c	e26de538	616c0ed5	a8b5b496
R 11	input	c637e211	0b325c09	1f0305b1	fce35863	4fcb5d99	ea2a9f29	5b216046	d5fa59c5
	T	37a83419	b71c70de	7663e35a	afb39358	74862f1c	b4e527fb	1e483144	93e2e8d3
R 12	input	1192904e	ff3c4f16	d31928e8	e0d289f4	4fe632d1	2d453b56	bbfafb07	32aa5055
	T	cf584fff	74997cf9	22a9871a	371c2a00	4c92ccda	0e1e1838	bfe7f64b	7a49b359
R 13	input	f1fb1114	7b79d5e1	a2061c23	c5e9964b	25a2c9f7	e232bf37	7fa33fc0	fbcc0c5ae
	T	d240e72b	4e00f915	45a409e6	4961a045	9071c9b4	079d12bc	55da3693	516c5858
R 14	input	7d2bb261	58261383	af3ec31a	ef0672ed	001cbf75	f1b1cc3a	36964b29	18281145
	T	a40a434d	a084ed19	f7189abf	7cd75459	77beb3ba	857d5aa9	e4ad6fba	2c99c169
R 15	input	a44ca417	5a1f6d38	2985110e	a100fc46	96519f43	e2ea236c	26e22061	a3abe9db
	T	f844e2d4	33ba9505	9e1337e5	bf2b26f9	dbfa84d1	30e6bab9	8f3f1715	c5c67939
R 16	input	afc64066	f716080b	74e69236	8874d289	6d6515ac	39058c2b	52e2dfd8	975b1cac
	T	02c242d8	ebb5b0ce	0102103f	ed79470b	8796cf9d	633ba027	89b1894c	2dbbca01
R 17	input	23b281b9	a21f591c	efb8c94b	820b08d4	02f97c61	c0252555	3f224104	71302465
	T	57ff38eb	e4f60787	cba067a4	082d71ba	15d70cc4	9ae81bd1	57456ec4	af018c10
output		1362c49b	0274a2eb	efc6760a	ae4068c0	b20e0da2	fd143fe2	a5e5a029	2c916698
output		f8db22fc	18b5ce21	591ea02f	267e97da	bdaf1639	49131027	3bf3b59e	94c26588

AURORA-256M (M_1 : 1 block message)

$MS_{L,0}^M$								
input		61626380	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	1395bab4	00000000	995db9b6	00000000	dcf52307	00000000	3e786087
R 2	input	64104673	2f020ca3	d20f62c9	d36967d2	a2e76192	3f2fdc05	408a7c2c
R 3	input	540bc035	db0f9d2f	ecd96797	21bcf3fd	1b864056	909b4c75	6abe8e5c
R 4	input	e76745bc	3da52426	56a0f574	09258fdd	2e890aa3	3f0a29ed	f7fbd2a5
R 5	input	482ee12b	fee931fb	d6f91f3f	0ed0e8c6	4fc1207f	7e52c1b1	a03827bf
R 6	input	f15e39f8	9b098080	0683de6a	64bde32a	800275d2	397ce87f	a7372647
R 7	input	0c901825	f4ae98a0	13168a97	44a00488	7754b053	1040087c	f5eaa8fb
R 8	input	d759f0a2	c5b13668	ee20f3f0	80f6e2ce	b840f7d3	cfb479c3	726ef64c
output		a9b8d5b1	6c09e3d9	f1a27ac9	71549807	d73e7f54	188a0697	ee3b886e
$MS_{R,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	e6860c3c	00000000	b78efff4	00000000	ee8511b8	00000000	bf3c20c3
R 2	input	1965be14	3c0b1724	07499ef2	5be32bc8	7b0cecf9	31fa6dc2	8a4635c1
R 3	input	03f34c0a	a5d11471	c67d8dd9	2858d31b	03159cee	b4634e6e	a860bdfc
R 4	input	38a99268	c8af06f5	6dd1364d	d37a9afa	241ed6db	b4571deb	f5ef192e
R 5	input	59feb000	92deccf1	c18ddbc4	b726ec8a	bc3ef880	66b56d70	d60069d8
R 6	input	baf60d2a	28dcae77	4304d31c	7890bc3b	d33651d5	1e5b7986	0849ab05
R 7	input	4f5ce121	5838946f	dec9e98f	d851b396	437790ab	dbbf702f	4e1152b6
R 8	input	ab5d889b	7b17fbaf	8afada61	6bf3a4c0	24172bb3	1b16ffff	ab20bc30
output		2abebf6a	51a944c5	9dc1026a	f632a6aa	ae5b0319	b54dfce2	bd3cbf1c
$CP_{L,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626380	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000
R 1	input	afdfef732	00000000	7f1465ed	00000000	b210d684	00000000	a14471cc
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000
R 2	input	6e7cdb11	8f538b76	3bd14236	624bce2b	509b9e94	ca9521df	6b0f5b0c
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05
R 3	input	05248d41	627ea547	f4164a17	430b1d5e	400b9585	9fbfaff3	bf8c27fe
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2
R 4	input	a5eb9bda	2eb0794a	a42c0dd2	ff778b6f	0138d581	34976c22	12262dea
	T	3d5fb62d	a9b280b9	db0f9d2f	d90d1c6a	21bcf3fd	1bbec097	909b4c75
R 5	input	20450aa0	2b9bd8ee	a4394154	5b43a2ab	d79eb143	a09c838b	8240e867
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e
R 6	input	416fd3d2	c87e4deb	2555e71d	ea0f2b54	54a90e21	7eea4747	2e2e20b5
	T	1398df30	cf40154a	3da52426	ad13a579	09258fdd	2efb4574	3f0a29ed
R 7	input	a982c89d	28558b25	f713c924	36b786a4	01a42c7e	ecff9cbb	a22123da
	T	31a37e56	1c68eb17	c8af06f5	038f0cb4	d37a9afa	24ef924d	b4571deb
R 8	input	c950f504	6dd691ec	8b69b28a	0e52ec34	9292e73f	43641db3	65d48471
	T	fca38584	91f2417f	fee931fb	ad824e56	0ed0e8c6	4f38e13f	7e52c1b1
R 9	input	57611470	a0b5d36f	6d9a403b	7a6d107b	470a4ecb	385f1ffc	15908cd2
	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70
R 10	input	6b1e7afa	5f2ca9e7	d6552d01	1ac0baf8	5734cd47	9866d1b1	b85b3f00
	T	bd70219b	e306ea8e	9b098080	0c044df1	64bde32a	8037396a	397ce87f
R 11	input	e54c3c03	619edb45	a5d7e72e	0e243a27	bfbec18	5c4bd59c	f9a40baa
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986
R 12	input	0ce5f94b	58ad8421	6662113f	6adc252b	0757c74a	76680e32	059796c6
	T	ca94c5b2	182d61f6	f4ae98a0	26a9504a	44a00488	77ea1897	1040087c
R 13	input	013257ad	245ddabb	5de6e404	61913f19	21259bb5	f6e1c990	7da8deba
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f
R 14	input	9e8c610c	cbc2d781	60bc1a26	f5b5ad90	99eef5c0	b370afb8	152221a8
	T	9027b8cb	ae41ee99	c5b13668	dc81ed45	80f6e2ce	b86ef0f0	cfb479c3
R 15	input	35892f95	2e8dd809	fe82e4a9	37789f0e	aca0b0c0	0be79fa5	b5fc4c83
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16ffff
R 16	input	7b8520e7	f77c524f	a80c6ab6	32812aaf	5ebba8c6	a74a5797	236d01ca
	T	a9b8d5b1	d813c7b2	f1a27ac9	e2a9300e	d73e7f54	188a0697	ee3b886e
R 17	input	1e9d89f8	1a8b1932	8ff8a1ac	07cbdeac	0e3f0ee1	50a35bdd	7e2d0ddc
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c
output		4729fb66	5fc8ff5c	b87b738d	d968fc1e	e065d931	abd07d17	f1e94c2b
output		4729fb66	5fc8ff5c	b87b738d	d968fc1e	e065d931	abd07d17	f1e94c2b

$CP_{R,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626380	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000 3e95b907
R 1	input	6bc350ba	00000000	54ce5d6d	00000000	ad3fc91b	00000000	c49a4313 61626380
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000 bf86fffb
R 2	input	36840cfa	05a0b72f	a6c6a9ae	4657cf14	4b307460	750fcec3	53ab2478 2d6060a7
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05 40106292
R 3	input	732c45b3	7e006ba1	457d1d4f	2b3a2efa	e80ead97	1904b7fb	325a9317 71fe0f23
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2 8a659ef9
R 4	input	a2de595c	2ed5b80b	0acfb18c	a1f328ef	9210d209	ed407eaa	9e0bb8b7 426f894a
	T	3d5fb62d	a9b280b9	db0f9d2f	d90d1c6a	21bcf3fd	1bbec097	909b4c75 6a0b6756
R 5	input	35c9b6b3	4ed5c63a	7ec6134f	d3824633	10a54a5b	8489a17e	6577bc4f 95ed2f99
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e a8f38dee
R 6	input	72c77764	76807890	e1b2c98c	e3996931	e0a1fa88	30252426	1007df97 9d7bcfe7
	T	1398df30	cf40154a	3da52426	ad13a579	09258fdd	2efb4574	3f0a29ed f767f5a3
R 7	input	39042d54	ffb353a7	a6069854	afabd8a9	65dca2c2	51db22e4	d046ae63 2f833261
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb f5a936db
R 8	input	bd38eac2	c2795842	4d999f6b	16c6adac	8f6ef659	6161db5e	60ec4240 a5daf03c
	T	fca38584	91f2417f	fee931fb	ad824e56	0ed0e8c6	4f38e13f	7e52c1b1 a02e1f7f
R 9	input	03834f14	dc16f821	1dcdabc5	fbf21d33	208d76d2	d6b582db	9af34eb4 8b1bee7b
	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70 d6fedb80
R 10	input	85eba3e2	591f5818	594d7207	39a367c9	130f96fb	8f37a018	aa244d20 f2942424
	T	bd70219b	e306ea8e	9b098080	0c044df1	64bde32a	8037396a	397ce87f a75eded2
R 11	input	0a78fb95	4b210cd7	aaaf00fb	5e71ee65	5ee258b9	84c8de95	62ac9c5b c5af5fc8
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986 08f6d3d5
R 12	input	69801186	175c2d7c	0c134339	923dbbf7	6ba43667	c583f9fe	d3e1a5d8 031494d9
	T	ca94c5b2	182d61f6	f4ae98a0	26a9504a	44a00488	77ea1897	1040087c f5908a53
R 13	input	10df70ed	5e9d2f4e	13e7254b	d684442a	08b8d65c	8d99bd7b	099612a0 a32d88bd
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f 4e5ce9ab
R 14	input	53a2e3ad	7ac0efa7	76b4769c	c81fb506	8fb09ff8	242f09f9	a37431d1 126a92ad
	T	9027b8cb	ae41ee99	c5b13668	dc81ed45	80f6e2ce	b86ef0f0	cfb479c3 7259f3d3
R 15	input	9e2705c0	861913e2	ea06072	947277bd	2b714ede	f54546ea	87a56c6b 14a1ab00
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16ffff ab5ddab3
R 16	input	3aa5cffe	8ed8f983	b166eaa2	c3366d00	3fa97f3c	90f972a5	5f65e1ca 43f21447
	T	a9b8d5b1	d813c7b2	f1a27ac9	e2a9300e	d73e7f54	188a0697	ee3b886e 7e1c30a5
R 17	input	467717e2	7bc02230	0a1d8378	8735d6bd	d00e1aab	cc7b0d1f	aabba058 d46206e5
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c f80a6bd0
output		6c096c35	15a3530d	1de45201	fc09d583	ca5a17f1	1d37e515	55c5c3e9 c49111c0
output		6c096c35	15a3530d	1de45201	fc09d583	ca5a17f1	1d37e515	55c5c3e9 c49111c0

AURORA-256M final mixing (M_1 : 1 block message)

$MS_{R,9}^M$								
input		6c096c35	15a3530d	1de45201	fc09d583	ca5a17f1	1d37e515	55c5c3e9
R 1	input	f317e9bf	1de45201	4b2deee1	ca5a17f1	f38c4279	55c5c3e9	7b0bf5ce
R 2	input	195c3af2	7e867933	8f0d5136	24fb6ce5	51db75e8	50cacee6	879b4cf2
R 3	input	63b1725c	0bd6f00a	17363a7c	24e54e9a	6e0a61de	0d81326c	0ced1e38
R 4	input	bf79cb34	05e9a428	ac3e35c8	f63abf7d	b8e54d81	c8418d62	ab4d26ec
R 5	input	233cfac1	60f37bb7	162565b9	fc0e367e	8b535e82	fa9faccb	633efb34
R 6	input	aa03d251	28df92f8	085786dd	ce75a241	f91db133	fe402851	5f864de2
R 7	input	1416a352	5ce77866	6c333f50	6a11a09e	114d12ad	8c8bf188	fb4aa00e
R 8	input	51b571bf	f7348583	b4188d3d	3521dc3b	2d742492	bc0716ed	57c6d17c
output		d43f1885	230b9d06	7301db45	4620077e	6bc7bb04	d7c0ade9	b204c723
$CP_{L,9}^M$								
input		4729fb66	5fc8ff5c	b87b738d	d968fc1e	e065d931	abd07d17	f1e94c2b
	mask							09090909
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	d6122044	b87b738d	95669d4c	e065d931	c5926e1a	f1e94c2b	17ec4c9f
	T	6c096c35	f996a167	1de45201	25c67adf	ca5a17f1	f30be9e1	55c5c3e9
R 2	input	d368fea9	fbdc143f	4c600dd0	95545502	819140d5	31972d59	2e9da50a
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 3	input	2309593f	aa8e6355	418624e1	9605e435	1f21fd07	abb61ed7	1e638ee6
	T	7ba9f8a9	0c86baf9	7e867933	47eda679	24fb6ce5	519b3a36	50cacee6
R 4	input	c049aed8	bc9f0bc7	659d32c7	bedcccb7	21ff8143	a5cbece4	904174fa
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 5	input	0766042a	87b69cf9	4bcb2734	7c2f1f67	5b1a1c22	dee5d269	bf726a22
	T	05cafd36	319b309c	0bd6f00a	0b850f2e	24e54e9a	6eed727c	0d81326c
R 6	input	b741799a	c66e0fbf	cafc2597	5f027318	fe5db11a	ae5dae1b	cb6aea94
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 7	input	a4305ec3	bd8c7d68	470fb20d	837d3378	76c6cc1b	1e4ea49e	d9820c8a
	T	184b01ef	5f9f26f6	05e9a428	5672931a	f63abf7d	b84dccb8	c8418d62
R 8	input	d61d93f8	38f4dcfb	f3d750ca	92c9ce53	45c19ef8	dc320dd0	0e1c4143
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 9	input	d70d0e76	b511bea3	b79c5af5	241b132f	c75ef5af	0f3eeef78	1558bcf8
	T	8d13ba92	9192af1a	60f37bb7	0b29fde0	fc0e367e	8b3efab9	fa9faccb
R 10	input	2f929ac7	da4abea8	940bc22b	c2433adf	c4bf0769	0c7e7aad	b4af55f2
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 11	input	aaa72233	c835a6b3	431f6f21	517e5574	909bd563	08cb923a	616c3bc3
	T	fc89f8c6	d52bd8f1	28df92f8	040ea6a8	ce75a241	f986d2dd	fe402851
R 12	input	cf2d0803	f6515b88	32c7c384	695b528d	cc67cd9e	fd9f14ed	a4bae9c5
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 13	input	76aa5526	88d0597c	20368ce1	f41a3b3c	0c2862ad	59f9fa19	3e9ee2e2
	T	fd09fa12	0a198907	5ce77866	3626d029	6a11a09e	114aa350	8c8bf188
R 14	input	b18c00c6	95fc095e	f6a1dcf7	d0a9ae1f	f8994e7b	2792b51e	613d6ea7
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 15	input	f3889fdc	8f6c17e2	68c58c56	1a9a2769	296d6228	ec96b3f7	93645bee
	T	bb0b3789	a88c123e	f7348583	5a3a68df	3521dc3b	2dc6713d	bc0716ed
R 16	input	405609a1	1c77ced0	f934eb4b	d38aeea7	0f40b055	f3763bda	8323ed14
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 17	input	57b3c4a4	54423aa1	3317b6e0	c21c866e	50f622bc	9636ce94	3872e053
	T	d43f1885	1185ce83	7301db45	231003bf	6bc7bb04	d7c0ade9	b204c723
output		01ec20c0	9014cc67	c48031cf	568d6f5b	40edf3fa	6adc2b83	6dcd92a
output		46c5dba6	cfdc333b	7cfb4242	8fe59345	a0882acb	c10c5694	9c248501

AURORA-224M (M_1 : 1 block message)

$MS_{L,0}^M$								
input		61626380	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	1395bab4	00000000	995db9b6	00000000	dcf52307	00000000	3e786087
R 2	input	64104673	2f020ca3	d20f62c9	d36967d2	a2e76192	3f2fdc05	408a7c2c
R 3	input	540bc035	db0f9d2f	ecd96797	21bcf3fd	1b864056	909b4c75	6abe8e5c
R 4	input	e76745bc	3da52426	56a0f574	09258fdd	2e890aa3	3f0a29ed	f7fbd2a5
R 5	input	482ee12b	fee931fb	d6f91f3f	0ed0e8c6	4fc1207f	7e52c1b1	a03827bf
R 6	input	f15e39f8	9b098080	0683de6a	64bde32a	800275d2	397ce87f	a7372647
R 7	input	0c901825	f4ae98a0	13168a97	44a00488	7754b053	1040087c	f5eaa8fb
R 8	input	d759f0a2	c5b13668	ee20f3f0	80f6e2ce	b840f7d3	cfb479c3	726ef64c
output		a9b8d5b1	6c09e3d9	f1a27ac9	71549807	d73e7f54	188a0697	ee3b886e
$MS_{R,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	e6860c3c	00000000	b78efff4	00000000	ee8511b8	00000000	bf3c20c3
R 2	input	1965be14	3c0b1724	07499ef2	5be32bc8	7b0cecf9	31fa6dc2	8a4635c1
R 3	input	03f34c0a	a5d11471	c67d8dd9	2858d31b	03159cee	b4634e6e	a860bdfc
R 4	input	38a99268	c8af06f5	6dd1364d	d37a9afa	241ed6db	b4571deb	f5ef192e
R 5	input	59feb000	92deccf1	c18ddbc4	b726ec8a	bc3ef880	66b56d70	d60069d8
R 6	input	baf60d2a	28dcae77	4304d31c	7890bc3b	d33651d5	1e5b7986	0849ab05
R 7	input	4f5ce121	5838946f	dec9e98f	d851b396	437790ab	dbbf702f	4e1152b6
R 8	input	ab5d889b	7b17fbaf	8afada61	6bf3a4c0	24172bb3	1b16fffb	ab20bc30
output		2abebf6a	51a944c5	9dc1026a	f632a6aa	ae5b0319	b54dfce2	bd3cbf1c
$CP_{L,0}^M$								
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask							00000000
	T	61626380	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000
R 1	input	502018cd	ffffff	80eb9a12	ffffff	4def297b	ffffff	5ebb8e33
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000
R 2	input	7a9edac5	07b72c5d	4c1be807	9b1930e5	56809732	28887486	76a203ee
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05
R 3	input	216cb2c5	bf878b0d	d03cc7ef	34d777ff	d5a07c1d	30c2d476	fb4df7bb
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2
R 4	input	a2821638	a2d51709	5f774761	89d07d59	d881b142	2d30688f	a7fc29ae
	T	3d5fb62d	a9b280b9	db0f9d2f	d90d1c6a	21bcf3fd	1bbec097	909b4c75
R 5	input	ab75c67f	ddda4807	24c28902	a5526a50	307802b4	2d0e0172	d5f68e85
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e
R 6	input	b6d9f08c	f40a114e	e7ef4ee2	2c7b8a52	1fcc4af2	a7c23335	f0c8b4fe
	T	1398df30	cf40154a	3da52426	ad13a579	09258fdd	2efb4574	3f0a29ed
R 7	input	e849e93e	66a3fa80	7ff10e08	521cd3fa	89267cf3	e4cf8f94	aba2f307
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb
R 8	input	bc368c46	9583c6f0	22944a92	e5be8603	716c435b	fb94e9af	a0088636
	T	fca38584	91f2417f	fee931fb	ad824e56	0ed0e8c6	4f38e13f	7e52c1b1
R 9	input	c946784f	1cb4a067	3ad1336e	329088ba	b7e71d75	6b73b9a0	7d9d95ca
	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70
R 10	input	27eb7f9f	9b639843	5a51ae16	bf2d19b3	a1864b19	678d56eb	219a968c
	T	bd70219b	e306ea8e	9b098080	0c044df1	64bde32a	8037396a	397ce87f
R 11	input	88ed3813	86c3ec8e	e77dbc7f	c146b9a4	8f0ea217	1cef7b17	492d9f33
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986
R 12	input	6836343e	c3be90d7	32331495	bd57460a	9026577b	0f5e543e	d5b8016a
	T	ca94c5b2	182d61f6	f4ae98a0	26a9504a	44a00488	77ea1897	1040087c
R 13	input	7a2d5b6f	54ac5e58	fa443ae3	122669f2	2b5f6424	47f2b0f6	4f2939b3
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f
R 14	input	65f161af	a945c4c9	71be9271	c3a3d4a1	15de64fe	cebccc79	882764e0
	T	9027b8cb	ae41ee99	c5b13668	dc81ed45	80f6e2ce	b86ef0f0	cfb479c3
R 15	input	59e17d2c	cdface81	20e95473	81eeae15	63c19fa4	707c3a6a	45a623fc
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16fffb
R 16	input	9ac5ee14	c86cd9a7	25f5fbd	7b20410b	6c3db1db	53e6fabd	d957bb3f
	T	a9b8d5b1	d813c7b2	f1a27ac9	e2a9300e	d73e7f54	188a0697	ee3b886e
R 17	input	a2869935	0fdd135b	d34d699e	4ae463b4	b7c8995d	39369c1c	15ae6caa
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c
output		b12d1542	bc9a1b11	cdf4cb50	e1c8f9db	7de69442	5fc6f7a5	90d90e61
output		4ed2eabd	4365e4ee	320b34af	1e370624	82196bbd	a039085a	6f26f19e

$CP_{R,0}^M$									
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask								00000000
	T	61626380	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000	3e95b907
R 1	input	943caf45	ffffff	ab31a292	ffffff	52c036e4	ffffff	3b65bcec	9e9d9c7f
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000	bf86ffb8
R 2	input	46aaf23c	097a2716	5573d331	0ec3ce74	fc15c2de	a3de4b82	7ac04bfa	a22a29da
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05	40106292
R 3	input	7a9572c0	ee3d8ab2	9d22d039	b4a09ccd	a1a7ef36	b9f73327	1d1173eb	747bde6e
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2	8a659ef9
R 4	input	f1f6298a	362cbdea	8d8185ee	1fc0dc51	8c73cb48	23ed982e	55cb0f15	811c71fb
	T	3d5fb62d	a9b280b9	db0f9d2f	d90d1c6a	21bcf3fd	1bbec097	909b4c75	6a0b6756
R 5	input	8a478d24	0b180d13	8547e519	d4c69be1	d95be1fa	7a74af6e	589e837f	32958148
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e	a8f38dee
R 6	input	b26cbfdd	44d44cfb	d43a75d2	5df8af7f	a0b1439f	9ef636e0	199b361d	183ebd44
	T	1398df30	cf40154a	3da52426	ad13a579	09258fdd	2efb4574	3f0a29ed	f767f5a3
R 7	input	d177ac69	b933a6d4	5e9f6b4d	ef4a4b76	8b3dbfff	c0eda37a	c4749d5f	f54e1b36
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb	f5a936db
R 8	input	768f59ac	5b2e94f3	94f8760c	21239f55	29d81596	031b1bc6	d83f1dce	283be6c1
	T	fca38584	91f2417f	fee931fb	ad824e56	0ed0e8c6	4f38e13f	7e52c1b1	a02e1f7f
R 9	input	81a3f234	38f5c8f8	cef5d9b7	e36d60d9	5a8b43fb	b174e60f	70164cc5	907417bb
	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70	d6fedb80
R 10	input	f61e932f	3b88a13f	23622d44	919633ce	dc07739d	efad09be	d1d0c90f	6558f1d2
	T	bd70219b	e306ea8e	9b098080	0c044df1	64bde32a	8037396a	397ce87f	a75eded2
R 11	input	d2885370	ebf52135	a2b4d173	be63ef4b	de039290	4af4da4a	3b24e59c	7f236c28
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986	08f6d3d5
R 12	input	e53c5f0c	e76298d8	1c4ef02f	652cf13e	52889581	d1b379f8	7dcc1134	2f9d1ad7
	T	ca94c5b2	182d61f6	f4ae98a0	26a9504a	44a00488	77ea1897	1040087c	f5908a53
R 13	input	a1ffd8c1	abd417ab	119976bd	b81c6cda	72e022c5	193060ec	b13e60bb	e26dc902
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f	4e5ce9ab
R 14	input	f47d821b	169b9ee1	7421c5eb	41d709e6	92739bd3	2ab0fb6d	ec156848	40b6aed1
	T	9027b8cb	ae41ee99	c5b13668	dc81ed45	80f6e2ce	b86ef0f0	cfb479c3	7259f3d3
R 15	input	2d2f6c26	a25d35e4	47e7d6b0	9509eceb	24fd49a9	2891cce1	0841f6d9	cbbdddf4
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16ffff	ab5ddab3
R 16	input	d68f2e71	bff58c5a	816c9fb9	9bb60610	baff4166	66cf710b	76310fd3	8bbc0c58
	T	a9b8d5b1	d813c7b2	f1a27ac9	e2a9300e	d73e7f54	188a0697	ee3b886e	7e1c30a5
R 17	input	6f80f2b9	06714d7b	2f721452	75143039	d43fc5f6	26c2825d	88aca498	cc20acfc
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c	f80a6bd0
output		ed2efecb	e935aeb8	f10a9d3b	e2c6fc3d	5980b5f3	6454c855	e70b116d	6e1d695d
output		12d10134	16ca5147	0ef562c4	1d3903c2	a67f4a0c	9bab37aa	18f4ee92	91e296a2

AURORA-224M final mixing (M_1 : 1 block message)

$MS_{R,9}^M$								
input	12d10134	16ca5147	0ef562c4	1d3903c2	a67f4a0c	9bab37aa	18f4ee92	91e296a2
R 1	input	f0643bfe	0ef562c4	aa44695e	a67f4a0c	75bc401b	18f4ee92	2e972384
R 2	input	d09d9d75	56f33149	cb060fa4	a184e60c	998bb535	a8d3fd3a	01d55962
R 3	input	0d7d9296	c52a8e29	5ceaaafb	e2979dc1	508972a4	72575243	a986ea34
R 4	input	c42c9981	593344c6	369b42b4	c2a88d2e	f34d63e4	3abda171	1f091548
R 5	input	0ae2e6e1	36ac75c4	74a130f8	e0f2062c	659ebf9c	a718a952	8b3ec72e
R 6	input	e187843b	c99e8cc0	f5504e34	2ab8f131	40a0b42e	429ae1b8	96cc63af
R 7	input	e31c6ab8	e76afefc	33c506a9	590da08e	9e0d49aa	1cd9c3b1	768c7564
R 8	input	f484d71a	2d3bed36	5dfd257c	b7454843	3f67d4c1	9481fbec	69f0b9e6
output	811641d4	ac2dace2	3600bedc	8145f69f	d9d6b582	4d574e6e	ba4a0614	1f29479d
$CP_{L,9}^M$								
input	4ed2eabd	4365e4ee	320b34af	1e370624	82196bbd	a039085a	6f26f19e	9c3be9bb
mask								09090909
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	ca7857e	320b34af	52cb3c01	82196bbd	cecd7531	6f26f19e	0a05b62d
T	12d10134	78222042	0ef562c4	555e11ff	a67f4a0c	75973b5e	18f4ee92	2e64691b
R 2	input	be4d09b9	0d9dbb46	bb2c030e	35dc902b	55250ce5	000b98ab	0e6ae3d6
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 3	input	a8ce500e	7bcf1f4d	30c72257	0f6c5871	b7e1c4dc	1f21ffd6	b2963748
T	a1b308fc	e8035ab1	56f33149	65c5acba	a184e60c	99d59da4	a8d3fd3a	019d0f35
R 4	input	12a45c57	f257d8b5	b804a8bf	6326f2b5	0503cee3	d4fe8d92	e21d59e1
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 5	input	e019eaa3	695dd772	78df682a	eb0c900f	bd0b4b81	58ddbed4	04641f2d
T	4363a640	06f5391a	c52a8e29	2e44f54b	e2979dc1	508692fb	72575243	a97daaa4
R 6	input	77690972	244eb479	541ea7a5	39cb5c4b	e6635c11	43b35838	55825a96
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 7	input	e61231a0	fefaa058	62cd63ea	1c74aabc	047921e8	7ca28114	e465fe50
T	ad125168	e24db1a4	593344c6	1b268ac0	c2a88d2e	f30999b4	3abda171	1f2c42e4
R 8	input	83a3b7e8	32ae3c5f	77a21cb4	cd5eaf88	071c1a96	37c74cd4	03b1c183
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 9	input	c5f4bf2f	ceaac521	93c557a4	df4be37a	d7325fa0	dd4f7c52	d9fda673
T	f84dbb66	8550df97	36ac75c4	3a4f63f0	e0f2062c	653ee6f8	a718a952	8be2309c
R 10	input	69a0a54c	f9f8a115	2bcd970a	50b4bac7	7664e5a5	9616358d	83d52ae6
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 11	input	80ce2f35	652d01ad	7cce48b0	8f8b17c5	d474451b	d5035dad	e0f11c1a
T	e1d1f3f8	f0a85a57	c99e8cc0	fad0319d	2ab8f131	40cc8434	429ae1b8	96874e2e
R 12	input	37e84ed1	ceb99ae6	cbd86ff1	d015def6	f5e51de8	9567360b	b0bbe32e
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 13	input	e45aaec5	7b2583e4	6a88f19c	8b8be2a7	1b93f874	00d579ad	0af7b4a7
T	ebbebf40	71e2a4b2	e76afefc	1986badc	590da08e	9e8c6aa9	1cd9c3b1	761c06aa
R 14	input	f14f821f	e4175d73	6c2ecfbd	24e06608	e9ce783a	955ff64a	64820f72
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 15	input	e90063c8	4c7612e1	5f9b8a3d	e7419856	663e5918	f428316d	557296a9
T	a5634189	7a7eea73	2d3bed36	2eb3dc8d	b7454843	3ff0d77c	9481fbec	698425c1
R 16	input	b4d6dc3d	b4ec1f94	02b685ae	f252cbe1	a68605fc	d4f47f4b	d9175fa3
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 17	input	0728b1f5	8efa35b6	c80a087a	2bd4b765	9e963292	87af4e43	d2388a3e
T	811641d4	d616d671	3600bedc	40a2fb4f	d9d6b582	4d574e6e	ba4a0614	1f29479d
output	989c40d5	4166e2c6	423549cc	1f43bb3a	ad820bc7	beacbe68	0d2d53c3	b609a107
output	d64eaa68	02030628	703e7d63	0174bd1e	2f9b607a	1e95b632	620ba25d	2a3248bc

AURORA-256 (M_2 : 2 block message (1/2))

MS _L									
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a	68696a6b
R 1	input	3384f0ee	63646566	f0646159	65666768	74c48974	6768696a	f6b3564f	61626364
R 2	input	a4613e56	a28efce1	044e1ec7	a2691ba5	ef1cde73	6140215c	3601fff8	42156e60
R 3	input	f0ac8947	95174c80	490bd175	815ee4a3	486fd342	92815e8c	2d1ed661	d738787e
R 4	input	4e10c638	02a3a13e	3a2c1fce	1daed6c0	2fa58f57	549f41cf	ed2d8dde	5c8e9ca2
R 5	input	9910c9ed	1259c7f8	c762c075	46c0ce18	927cfa7f	9fcb0be8	09550bf0	1454243a
R 6	input	a527b0e4	cf467de1	89a62e58	6a59dd92	f5617cc7	7db695a4	7ab8c5a0	18ea448c
R 7	input	b8eb80d6	7a15bdc2	8a75fcb1	db24f137	a68101c3	1af1bd3c	463a3df1	5a268346
R 8	input	641269ca	bee774c9	4d332107	fc0c687b	859cf816	55a015b0	6e0c4abf	6b51d972
output		7d958d0b	c372f9c2	47741056	bb78782d	2bd47149	7e7464f9	12fd84bb	79ac5dc9
MS _R									
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000	00000000
R 1	input	a1890954	6b6c6d6e	1027db70	6d6e6f70	e7231aa1	80000000	ab0544f8	696a6b6c
R 2	input	60cadf65	8b4d9ba4	10152cb7	8c73ccaa	99877f78	fc3c165f	eb7334ce	aa29785f
R 3	input	b40e0396	1d23e63a	d0149223	e4890620	cc485f2b	d1d48c83	fc355643	9e48ef18
R 4	input	c78a1075	847efb6b	9970eb6c	1f798eb7	1e06f1ea	f140daec	baace88a	7a46384e
R 5	input	67ebcbcd	c01ac220	4232156c	438c07c8	72a4f635	20e79753	e3c96fd5	47493244
R 6	input	3ef20884	d448b68f	132b2d67	77e1993c	d70e5326	bdc3bc47	d8131f23	4a74eee9
R 7	input	24525223	21dae585	8b4b7c12	2964a95d	14b8d8ad	dcece828	a6f39b58	0546117c
R 8	input	9cb174e0	fba4fa5b	73cdf10f	0c8ca306	f91db167	7ec56629	77ccea27	307b82f1
output		2e23147d	d587ee26	e7c0804c	eb4c234a	d5ae72f3	ab6b14da	8de1e351	bd9a61a0
CP									
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask								00000000
	T	61626364	66c9129f	63646566	e188addc	65666768	74b3f059	6768696a	f6846174
R 1	input	4ef2bc98	63646566	2b4ae441	65666768	7dd8e4fb	6768696a	39d9350a	61626364
	T	696a6b6c	50938d7c	6b6c6d6e	0811a22a	6d6e6f70	e7050970	80000000	ab89dba1
	input	a6631bf9	40ea93a3	be16bb4c	9195e625	6e6d49e2	d99bb464	c4426f8e	6a1327d3
	T	42156e60	489dbdf0	a28efce1	0839fead	a2691ba5	ef013ec7	6140215c	36611e73
R 3	input	21d635e9	0d6114ef	d712e975	d1ad8277	50b988c3	4fc55f1a	e95ec297	29ef225b
	T	aa29785f	b00abfe7	8b4d9ba4	08439a32	8c73ccaa	9973dfb7	fc3c165f	ebca2c78
R 4	input	9bdfb538	78df7dba	c7da21c0	245adffc	5435d202	f5fe9be8	369f7fd1	ce38d479
	T	d738787e	e017a6c2	95174c80	92dfac8f	815ee4a3	481e8975	92815e8c	2dacd142
R 5	input	27704f73	a90a9e31	b5646f55	20b29f2e	4890904a	0df9442a	020c61e1	2a4a9818
	T	9e48ef18	5a0a2fa1	1d23e63a	e8242b4b	e4890620	ccb50323	d1d48c83	fc0e922b
R 6	input	7c42048d	7a26a6de	2df3fcf2	e5846362	68a35453	6534b70c	6d410c5a	53995d2d
	T	5c8e9ca2	9c591fbc	02a3a13e	754b1a70	1daed6c0	2f2dc6ce	549f41cf	ed101f57
R 7	input	77777046	c877c638	861f8b5d	7d81f01e	7ab78097	df3a1b51	02377a9a	8e340aa4
	T	7a46384e	e3b878c5	847efb6b	4c83743a	1f798eb7	1eac106c	f140daec	ba8aebca
R 8	input	09cc5fdb	98fb74e9	dec9ed40	75a4fe7b	0b65ae1f	0e376a80	604921d6	186a7798
	T	1454243a	32c5f5e1	1259c7f8	8ef817db	46c0ce18	9255c975	9fcb0be8	0910c07f
R 9	input	c92eeeba	f67ba888	fbdc1cf9	4995a024	d33bd9bb	fdb5d82e	96320bf8	3071c330
	T	47493244	b3997b6a	c01ac220	a15237e6	438c07c8	72c9cb6c	20e79753	e3eb1535
R 10	input	f1c227a9	0f5da5fe	1cd621ed	2db31ff6	610ee123	ca2a1424	4b49b620	bb777f73
	T	18ea448c	4b4cf941	cf467de1	12c38bc9	6a59dd92	f5b8b058	7db695a4	7a272ec7
R 11	input	7555e7bd	6c26fb6d	1cc66aeb	f2a9ad14	a7632d4f	4c5161f3	7977a9e6	7eb7ca3f
	T	4a74eee9	1f15a991	d448b68f	89870fc2	77e1993c	d7130867	bdc3bc47	d8f22d26
R 12	input	add4f7a9	157cec77	b3508064	0cd20bdd	e08f2d67	05a39d73	5a5ba534	fc9d6ef4
	T	5a268346	70ea03e3	7a15bdc2	15027bad	db24f137	a63a80b1	1af1bd3c	46ebfcc3
R 13	input	b873cd15	72798264	5c7a8727	42d753c3	3adab44f	238caafd	213ee14d	91402734
	T	0546117c	9225ec2c	21dae585	45dc4d91	2964a95d	14f35212	dcece828	a6527cad
R 14	input	4ce39ac1	dd971823	40b12713	fb2545b0	e541aba2	8d8960cb	07962c28	43212b4b
	T	6b51d972	c867f17e	bee774c9	9b389594	fc0c687b	850c6907	55a015b0	6e122116
R 15	input	f823e738	6ba7104f	a1a9b446	af6b58d1	6a727501	ec7af01c	a41a5392	3cb38bba
	T	307b82f1	4e66d893	fba4fa5b	b98ef570	0c8ca306	f9cc740f	7ec56629	77b1f167
R 16	input	996a4442	584cf975	f65bbd93	47241dc4	0db64a7e	d1c8adee	fc46dd70	9638acfa
	T	7d958d0b	86e5f385	47741056	76f0f05b	2bd47149	7e7464f9	12fd84bb	79ac5dc9
R 17	input	916f85c3	f18197ec	ef5fcb82	52d7ab6b	70502011	f2349937	830fd398	c04ffe2c
	T	2e23147d	6ac3f713	e7c0804c	75a611a5	d5ae72f3	ab6b14da	8de1e351	bd9a61a0
output		5882f386	ede38704	5bbae979	9b0bd3fb	3347aecd	bfb651d3	698ee3d8	99ba9f05
output		5882f386	ede38704	5bbae979	9b0bd3fb	3347aecd	bfb651d3	698ee3d8	99ba9f05

AURORA-256 (M_2 : 2 block message (2/2))

MSF_L								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	51ed9889	00000000	94070b30	00000000	12a1ed1f	00000000	9ed4302a
R 2	input	ea873565	a4c205ba	67a558c1	dded79c9	f7368b6b	8fc40420	b9ed61e0
R 3	input	aab4335b	d03474f0	73c98359	200a7bf3	07c853e6	66163c56	f4ce8cda
R 4	input	bbe130ff	5464dea9	cd44dd21	e21742f5	2436d890	94e0fae8	71036d44
R 5	input	8f103d9b	95e399bb	bf75eb71	0c48813b	187f8dce	a4804fb3	82a2c184
R 6	input	d741b168	48df6e4e	441d36aa	d568983b	71702010	91008590	d6c29915
R 7	input	b54d395e	bb7f7fe3	f48a7a49	ac2158fb	3ddadfec	985639e5	3189ba71
R 8	input	17da5952	f3ef589d	77db39ce	06ffdc6b	fd911f9b	a50ec012	1458cf71
output		4d1acddd	bef59540	aa4adc3b	acb50050	4880026f	ed8ec27d	5a5f7a8d
MSF_R								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cb89793b	00000000	7c4cbb01	00000000	894e76a0	00000000	ab6a2a95
R 2	input	4582b27d	78cd79cc	8e3b287a	d635a167	4369b531	e11e797a	9f35b9d6
R 3	input	6f1220fa	c3b5f49b	54940b63	01b04a45	34980f62	278ab2bc	44ae2904
R 4	input	c3f81c5f	27b88024	df1a2d77	0be6bc93	fcf9e001	b932ae28	da6ddfa1
R 5	input	2806b3b8	ab89ce71	3d41fff9	67f60b9c	1ea8ab42	a3f67eae	bac1516c
R 6	input	25764152	41bca70d	a28e7730	97c03996	b4801dcc	e8f2c05b	61230217
R 7	input	a98357fb	4b1778f7	01d28e22	4ea2d071	2654d09a	800b587a	8a04a61c
R 8	input	044dc5e8	b6c27a7f	59e33ea1	e3b2a2fa	4abd9eec	0654b064	17151311
output		9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543
CPF								
input		5882f386	ede38704	5bbae979	9b0bd3fb	3347aecb	bfb651d3	698ee3d8
	mask							99ba9f05
	T							01010101
R 1	input	00000000	a20fda55	00000000	29426112	00000000	12d49830	00000000
	T	672085ad	5bbae979	786f10fb	3347aecb	a419ab94	698ee3d8	c9082ac4
R 2	input	00000000	e5a63b4a	00000000	b627151d	00000000	896a7901	00000000
	T	a6084b50	a84676f6	dd43dc79	750c23a3	87baa1ea	b311428e	163c99d5
R 3	input	6f9a5e1e	d54b17c0	a4c205ba	ce6cc2cb	dded79c9	f7ed35c1	8fc40420
	T	0818b49b	44e2d226	bae99377	91af9cf5	1dba57f9	26bcfe5b	04be044a
R 4	input	e46bdf29	a29ddaeb	78cd79cc	4734dcbe	d635a167	4335b27a	e11e797a
	T	69c07416	4e1ec8f2	0db32338	b87fbf45	21019936	4f845377	95c370f6
R 5	input	8bb6019e	5592a7b4	d03474f0	e79118b7	200a7bf3	07ce3359	66163c56
	T	5e13af24	1b4ad297	ab7b25b5	397d922d	059890f1	692b707a	ad3dc113
R 6	input	b6485d37	37ca0782	c3b5f49b	2a4c14fd	01b04a45	34ae2063	278ab2bc
	T	964d12ef	9307d3a8	c1ca0c79	6b522e9c	9fb37c57	d7ad2c53	366759c8
R 7	input	ecc5f348	7689b089	5464dea9	9a6cd8ff	e21742f5	24033021	94e0fae8
	T	d2570059	90f5c0c1	e976245d	fe29799b	bf03fec8	5b2c32d7	c6918f5a
R 8	input	a0ba3bc4	e18d7050	27b88024	effcefaf	0be6bc93	fc6d1c77	b932ae28
	T	b5066ab0	346a4cdd	f114e91d	58eddc9f	54e5be9e	052f1646	54487034
R 9	input	54842cd9	1eeb1b09	95e399bb	7eff8337	0c48813b	18a23d71	a4804fb3
	T	d4e22d01	28cc7a78	7fd2d37e	2174a423	7078d48b	cea5b7f1	28b431f4
R 10	input	abfc14b2	1420d5b6	ab89ce71	1ed428dc	67f60b9c	1ec1b3fc	a3f67eae
	T	9352c565	ec53835e	43fcc732	71fde632	46f452eb	bc2b2354	3b65871a
R 11	input	edeb467a	ae3a402a	48df6e4e	88e132d1	d568983b	71c2b1aa	91008590
	T	b167451b	797384b8	486cb9fd	9d897c29	85c3e222	5d23529c	de1d8579
R 12	input	3a42ac8c	12c70e8b	41bca70d	d1400129	97c03996	b4234130	e8f2c05b
	T	31eed213	2defd299	294cdbc9	7a80f4e4	040f8ea4	1cfeb3e5	996a558a
R 13	input	d0404e69	6b15bee3	bb7f7fe3	e9b574bd	ac2158fb	3d893949	985639e5
	T	25ab7bc8	c0ba4db1	a5ca9567	1543db21	9896fcf2	30f982a3	32411c9d
R 14	input	1d2b08ba	d4e9680e	4b1778f7	00aa537d	4ea2d071	26045722	800b587a
	T	a8fe099f	dee7c801	3ba1ac7c	3547829d	6d1eb34a	f219ae56	3db0f75f
R 15	input	d9d3fc9d	2fb63ee2	f3ef589d	ef239ea4	06ffdc6b	fd5859ce	a50ec012
	T	0bd292ea	42f95ed4	7f81ebcc	012f671f	395d3f90	2c9e29e5	e769fcd9
R 16	input	c29830b5	0271cf08	b6c27a7f	acde89f4	e3b2a2fa	4a15c5a1	0654b064
	T	84b7d786	26d614df	7ed82bcf	b2e4e733	645e6380	8b7253dd	1a85f39f
R 17	input	4d1acddd	7deb2a81	aa4adc3b	596a00a1	4880026f	ed8ec27d	5a5f7a8d
	T	ed345d62	70cefa2d	59da49ef	48ea5897	c07b3c48	fcc5fd2b	b426788a
output		9143bac2	93c0e05e	7688bebb	ca9d0e20	549bad3e	52cf1d5a	11429543
output		79e0e3ef	0bad435e	b775fd73	438a157f	7784ae4c	8d15e303	802f3ab9
output		21621069	e64ec45a	eccf140a	d881c684	44c30081	32a3b2d0	e9a1d961

AURORA-224 (M_2 : 2 block message (1/2))

MS_L								
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a
R 1	input	3384f0ee	63646566	f0646159	65666768	74c48974	6768696a	f6b3564f
R 2	input	a4613e56	a28efce1	044e1ec7	a2691ba5	ef1cde73	6140215c	3601fff8
R 3	input	f0ac8947	95174c80	490bd175	815ee4a3	486fd342	92815e8c	2d1ed661
R 4	input	4e10c638	02a3a13e	3a2c1fce	1daed6c0	2fa58f57	549f41cf	ed2d8dde
R 5	input	9910c9ed	1259c7f8	c762c075	46c0ce18	927cfa7f	9fcb0be8	09550bf0
R 6	input	a527b0e4	cf467de1	89a62e58	6a59dd92	f5617cc7	7db695a4	7ab8c5a0
R 7	input	b8eb80d6	7a15bdc2	8a75fcb1	db24f137	a68101c3	1af1bd3c	463a3df1
R 8	input	641269ca	bee774c9	4d332107	fc0c687b	859cf816	55a015b0	6e0c4abf
output		7d958d0b	c372f9c2	47741056	bb78782d	2bd47149	7e7464f9	12fd84bb
MS_R								
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000
R 1	input	a1890954	6b6c6d6e	1027db70	6d6e6f70	e7231aa1	80000000	ab0544f8
R 2	input	60cadf65	8b4d9ba4	10152cb7	8c73ccaa	99877f78	fc3c165f	eb7334ce
R 3	input	b40e0396	1d23e63a	d0149223	e4890620	cc485f2b	d1d48c83	fc355643
R 4	input	c78a1075	847efb6b	9970eb6c	1f798eb7	1e06f1ea	f140daec	baace88a
R 5	input	67ebcbcd	c01ac220	4232156c	438c07c8	72a4f635	20e79753	e3c96fd5
R 6	input	3ef20884	d448b68f	132b2d67	77e1993c	d70e5326	bdc3bc47	d8131f23
R 7	input	24525223	21dae585	8b4b7c12	2964a95d	14b8d8ad	dcece828	a6f39b58
R 8	input	9cb174e0	fba4fa5b	73cdf10f	0c8ca306	f91db167	7ec56629	77ccea27
output		2e23147d	d587ee26	e7c0804c	eb4c234a	d5ae72f3	ab6b14da	8de1e351
CP								
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
mask								00000000
T		61626364	66c9129f	63646566	e188addc	65666768	74b3f059	6768696a
R 1	input	b1044367	9c9b9a99	d4b51bbe	9a999897	82271b04	98979695	c626caf5
T		696a6b6c	50938d7c	6b6c6d6e	0811a22a	6d6e6f70	e7050970	80000000
R 2	input	d1a1c4a0	e036f405	e12fd7b4	0dcdc622	0d4e5109	6da62770	8fe5f74a
T		42156e60	489dbdf0	a28efce1	0839fead	a2691ba5	ef013ec7	6140215c
R 3	input	b9e8c581	201eb180	6621ace9	d290e1ff	e79e5a1a	9a3dfd8f	b45e4724
T		aa29785f	b00abfe7	8b4d9ba4	08439a32	8c73ccaa	9973dfb7	fc3c165f
R 4	input	4210336e	c6920964	7a0d5dc6	5c27fb18	f945d1ec	0dde5213	f61a6876
T		d738787e	e017a6c2	95174c80	92dfac8f	815ee4a3	481e8975	92815e8c
R 5	input	02e29522	89b8df84	ed1207c7	4abb8c47	da5f90d8	8bc38a70	702504d3
T		9e48ef18	5a0a2fa1	1d23e63a	e8242b4b	e4890620	ccb50323	d1d48c83
R 6	input	e817a0a2	5bd61e98	6621eaa9	9e8e0963	955a9be0	d45ad553	4771a7d1
T		5c8e9ca2	9c591fbc	02a3a13e	754b1a70	1daed6c0	2f2dc6ce	549f41cf
R 7	input	ce787bb8	f192b4c7	c408623f	be869923	08583bfa	b6557c02	df5e62ac
T		7a46384e	e3b878c5	847efb6b	4c83743a	1f798eb7	1eac106c	f140daec
R 8	input	0350ffc0	1c5397cf	99f3c7f1	67233999	70ca3d59	444c43b6	b2a1ab20
T		1454243a	32c5f5e1	1259c7f8	8ef817db	46c0ce18	9255c975	9fcb0be8
R 9	input	e3c33531	7bd781e1	64d6fa95	fc9e521f	2c107734	3d870ca8	6542e552
T		47493244	b3997b6a	c01ac220	a15237e6	438c07c8	72c9cb6c	20e79753
R 10	input	14fd21b8	9a718bd4	3c62f5e4	510bcd79	dd29b180	baba8d0b	95c36af3
T		18ea448c	4b4cf941	cf467de1	12c38bc9	6a59dd92	f5b8b058	7db695a4
R 11	input	3fa989a0	14f966ff	18d736aa	65415a7a	40043253	32b54455	6f0fe674
T		4a74eee9	1f15a991	d448b68f	89870fc2	77e1993c	d7130867	bdc3bc47
R 12	input	aa00e7b1	94851301	a5bd4e43	5d183e5c	cf9efe7e	5d4a62d2	dd75ad37
T		5a268346	70ea03e3	7a15bdc2	15027bad	db24f137	a63a80b1	1af1bd3c
R 13	input	bc2ad9ea	6fede31a	101fe506	c535b843	e5848c58	cfe7867b	b235b56c
T		0546117c	9225ec2c	21dae585	45dc4d91	2964a95d	14f35212	dcece828
R 14	input	4906c405	6f24b067	75b08cc7	55ce37e2	a710dea3	b8f00c9d	b7166f79
T		6b51d972	c867f17e	bee774c9	9b389594	fc0c687b	850c6907	55a015b0
R 15	input	718f0764	a4a76341	c0e441ee	5f51d42f	af998d29	5d43111b	0d595235
T		307b82f1	4e66d893	fba4fa5b	b98ef570	0c8ca306	f9cc740f	7ec56629
R 16	input	534da5ef	97e63426	c9bcaa37	2abe1d67	d126df6a	0011ea19	16e59c06
T		7d958d0b	86e5f385	47741056	76f0f05b	2bd47149	7e7464f9	12fd84bb
R 17	input	8afe9cc3	2f4cea4f	5ccbe411	e937f50f	1a07026f	7e425031	0a36ae0a
T		2e23147d	6ac3f713	e7c0804c	75a611a5	d5ae72f3	ab6b14da	8de1e351
output		2dab7a66	46077347	9227247a	e976409c	6c675c69	6ce06a71	9a5ea506
output		d2548599	b9f88cb8	6dd8db85	1689bf63	9398a396	931f958e	65a15af9

AURORA-224 (M_2 : 2 block message (2/2))

MSF_L								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	51ed9889	00000000	94070b30	00000000	12a1ed1f	00000000	9ed4302a
R 2	input	ea873565	a4c205ba	67a558c1	dded79c9	f7368b6b	8fc40420	b9ed61e0
R 3	input	aab4335b	d03474f0	73c98359	200a7bf3	07c853e6	66163c56	f4ce8cda
R 4	input	bbe130ff	5464dea9	cd44d21	e21742f5	2436d890	94e0fae8	71036d44
R 5	input	8f103d9b	95e399bb	bf75eb71	0c48813b	187f8dce	a4804fb3	82a2c184
R 6	input	d741b168	48df6e4e	441d36aa	d568983b	71702010	91008590	d6c29915
R 7	input	b54d395e	bb7f7fe3	f48a7a49	ac2158fb	3ddadfec	985639e5	3189ba71
R 8	input	17da5952	f3ef589d	77db39ce	06ffdc6b	fd911f9b	a50ec012	1458cf71
output		4d1acddd	bef59540	aa4adc3b	acb50050	4880026f	ed8ec27d	5a5f7a8d
MSF_R								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cb89793b	00000000	7c4cdb01	00000000	894e76a0	00000000	ab6a2a95
R 2	input	4682b27d	78cd79cc	8e3b287a	d635a167	4369b531	e11e797a	9f35b9d6
R 3	input	6f1220fa	c3b5f49b	54940b63	01b04a45	34980f62	278ab2bc	44ae2904
R 4	input	c3f81c5f	27b88024	df1a2d77	0be6bc93	fcf9e001	b932ae28	da6ddfa1
R 5	input	2806b3b8	ab89ce71	3d41fff7	67f60b9c	1ea8ab42	a3f67eae	bac1516c
R 6	input	25764152	41bca70d	a28e7730	97c03996	b4801dcc	e8f2c05b	61230217
R 7	input	a98357fb	4b17787f	01d28e22	4ea2d071	2654d09a	800b587a	8a04a61c
R 8	input	044dc5e8	b6c27a7f	59e33ea1	e3b2a2fa	4abd9eec	0654b064	17151311
output		9143bac2	2781c0bd	7688bebb	953a1c41	549bad3e	52cf1d5a	11429543
CPF								
input		d2548599	b9f88cb8	6dd8db85	1689bf63	9398a396	931f958e	65a15af9
	mask							01010101
	T	00000000	a20fda55	00000000	29426112	00000000	12d49830	00000000
R 1	input	33314135	6dd8db85	f57446a6	9398a396	889ba074	65a15af9	11a14678
	T	00000000	e5a63b4a	00000000	be27151d	00000000	896a7901	00000000
R 2	input	d0042f84	af8a9979	7a07b5a6	9da5fe5d	63a94821	1dcb5d5a	32ba7b96
	T	6f9a5e1e	d54b17c0	a4c205ba	ce6cc2cb	dded79c9	f7ed35c1	8fc40420
R 3	input	ff344346	5a2a0e05	4c64f1a4	e52574f2	c7db4312	e6b6470f	84ee051e
	T	e46bdf29	a29ddaeb	78cd79cc	4734dcbe	d635a167	4335b27a	e11e797a
R 4	input	f89db979	a020379a	97339dba	1478cb93	4db525a0	af98163a	85ce678c
	T	8bb6019e	5592a7b4	d03474f0	e79118b7	200a7bf3	07ce3359	66163c56
R 5	input	6305cb87	2fd2bae2	333102b5	8ffbb360	53077c89	8175375b	caa7ddc6
	T	b6485d37	37ca0782	c3b5f49b	2a4c14fd	01b04a45	34ae2063	278ab2bc
R 6	input	68a909af	c1a173a5	25e49bea	b597722e	a9935a0d	133da8b4	21fcd865
	T	ecc5f348	7689b089	5464dea9	9a6cd8ff	e21742f5	24033021	94e0fae8
R 7	input	a06f08c0	e8a3a7ea	4f195e5d	fb32f57c	7e90d88c	07a2064b	501ab47b
	T	a0ba3bc4	e18d7050	27b88024	effcefaf	0be6bc93	fc6d1c77	b932ae28
R 8	input	ccf1cd54	451f5fde	854ad4ec	b3c04ff2	e38bbdea	ae11ad1e	dfebef7a
	T	54842cd9	1eeb1b09	95e399bb	7eff8337	0c48813b	18a23d71	a4804fb3
R 9	input	86e04211	01e56805	bd71548b	4b20708e	b17cda73	cdaf546c	2adeb0b1
	T	abfc14b2	1420d5b6	ab89ce71	1ed428dc	67f60b9c	1ec1b3fc	a3f67eae
R 10	input	e50c92f7	9077b561	5531313a	021952a7	36849cec	24a3c815	808b657c
	T	edeb467a	ae3a402a	48df6e4e	88e132d1	d568983b	71c2b1aa	91008590
R 11	input	35c19fa8	76bda99e	340c2527	2a994db2	aae9069c	16611239	ca851cc0
	T	3a42ac8c	12c70e8b	41bca70d	d1400129	97c03996	b4234130	e8f2c05b
R 12	input	88935208	3dfe7b19	8ec87e4e	b82334c0	8d0e265a	4cc7c49d	318bcd94
	T	d0404e69	6b15bee3	bb7f7fe3	e9b574bd	ac2158fb	3d893949	985639e5
R 13	input	be3ffc1f	9c660042	3b7c0dcf	978f2bf1	4ae94a11	fa279f78	4eb49187
	T	1d2b08ba	d4e9680e	4b1778f7	00aa537d	4ea2d071	26045722	800b587a
R 14	input	0fb4e90b	d1761d45	b667ad4f	1a337f75	884313d0	47f4b056	031ad202
	T	d9d3fc9d	2fb63ee2	f3ef589d	ef239ea4	06ffdc6b	fd5859ce	a50ec012
R 15	input	77f00081	d9b40c57	cb894c0e	4f42ebdd	7964d5aa	1da66371	2d5952b6
	T	c29830b5	0271cf08	b6c27a7f	acde89f4	e3b2a2fa	4a15c5a1	0654b064
R 16	input	4571ab9c	72d85b07	df0fc2f8	79b1d190	9e8d41df	382d85b9	dae830e1
	T	4d1acddd	7deb2a81	aa4adc3b	596a00a1	4880026f	ed8ec27d	5a5f7a8d
R 17	input	e4e9fb59	6ae558b5	88933684	8be12898	b0057e43	5082f2dd	4272ec83
	T	9143bac2	93c0e05e	7688bebb	ca9d0e20	549bad3e	52cf1d5a	11429543
output		d7d3ccd1	bfb5cef8	a7382423	90ccbc20	d2f82ec1	842e6c78	3dbdf241
output		05874948	064d4240	cae0ffa6	86450343	41608d57	1731f9f6	581ca8b8

AURORA-512 (M_2 : 2 block message (1/2))

MS _{L,0}									
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a	68696a6b
R 1	input	b205f1ae	63646566	e1d20b61	65666768	7a8c874f	6768696a	7ec49239	61626364
R 2	input	3896619e	ca006e90	85585b15	d23deb79	a61e74d8	67c7f609	338d6cf2	f183fdb3
R 3	input	903aa0e9	18a4869c	8bc7b6c6	b547ad57	5f04df12	dc5c2ef1	d040ecc7	e8eac368
R 4	input	22bf7611	5c76fff9	1a69b6ce	c520c1df	ec64c023	aed562d2	28de1a7a	ea944cbb
R 5	input	2ea2259b	34608397	6e0e7497	2fb05744	95a735dd	2e6e434c	ce4eb810	2bc0213d
R 6	input	7d6fe9f7	942016ae	ebf704bb	6de53db3	134298af	2269918c	6a268f80	976ab445
R 7	input	84f89189	c30abfbc	655d46c7	a8b3da7c	a9c09238	b663dd9e	b93ab195	83f35824
R 8	input	46901702	03c62d37	ae6003a6	a455d560	5f94c6d9	7e0fbad1	fa120bfb	d38cb9c
output		ae03a1cb	adc58fcf	e0d4a094	448175f4	6bd241b6	15ddfb67	424d5ef0	91c6956c
MS _{R,0}									
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000	00000000
R 1	input	a7996fdc	6b6c6d6e	0cce99ba	6d6e6f70	60581d06	80000000	9a3edcc3	696a6b6c
R 2	input	383f586b	6a921b9d	d207da0f	3ffd2edb	2e3b89af	e3a79d37	7445b424	f7d10a0d
R 3	input	172b7bcf	a6e3711f	414a376c	c0b39cc0	fda53832	21129cb7	d1a06300	d52d82d6
R 4	input	26714005	43bd88f8	6df9ce9b	0eca978b	cdecc1e8	09d85bef	e95d712f	19d32d4a
R 5	input	100d47fc	0a4d6f2d	0d6228fd	edec75d	eeff6f81	40957580	5821871b	5afe9209
R 6	input	debf00a2	e639933c	9b30d76c	13096d01	7b4b17e5	3539ac41	a3cacd47	1efe2fc3
R 7	input	7bc5b2b1	3c464fc0	8c35cd3a	1615f437	aaae5457	ca25b846	e788444b	a52e312c
R 8	input	7d2b5037	5b1fc4a3	3d643f0d	bf33e0b0	cb3e1195	17bc87be	2ad083f0	9bb79f09
output		0be8c520	50f70183	0d2d3989	b21ed939	bbf79371	ac4b14cf	f0cb865e	6b7c1957
CP _{L,0}									
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask								00000000
	T	61626364	65a50e73	63646566	c319255d	65666768	7ac4f161	6768696a	7e050b4f
R 1	input	0d333d39	63646566	01fd3be5	65666768	74edffdd	6768696a	7595dffd	61626364
	T	696a6b6c	53e70ee1	6b6c6d6e	862c6e6e	6d6e6f70	603e6fba	80000000	9a999906
R 2	input	368aed9b	2fe75095	67a2c79a	cc8dbbac	baaa028b	8a420fe4	c4175150	f401e1e6
	T	f183fdb3	70b0e9e5	ca006e90	0a3cd93c	d23deb79	a68d6115	67c7f609	33965bd8
R 3	input	912b8f4f	a985bcfc	b0c0d1c5	c5e37bce	32088d04	7be27a69	41fd824b	ea4b3f9b
	T	f7d10a0d	9c03c492	6a921b9d	691dda35	3ffd2edb	2e45580f	e3a79d37	743fdaaf
R 4	input	a41cbcc5	60d1a5ae	0d15c42f	c8df5d3b	813269ff	842be515	04f59e33	2f37c7df
	T	e8eac368	2197bf8f	18a4869c	1609d9d3	b547ad57	5f40a0c6	dc5c2ef1	d03a7612
R 5	input	8ef64e00	d62608f2	30d8cbb8	8fe4dbf2	a79ae469	475586fd	1a28ca1c	fe64844a
	T	d52d82d6	8ba51c00	a6e3711f	20d2b1e7	c0b39cc0	fda07b6c	21129cb7	d12b3732
R 6	input	523e2302	c9e6b61f	717007e4	b05bb782	7745f6c2	b7b26b1d	b675d532	8b352281
	T	ea944cbb	44d380f4	5c76fff9	34c83422	c520c1df	ecde76ce	aed562d2	28bfb623
R 7	input	9638b449	81259b4f	a02dfb56	7b6424aa	9f6aaa2b	7a270697	c0f9439a	19a055e4
	T	19d32d4a	937ce097	43bd88f8	b6f63882	0eca978b	cd5d409b	09d85bef	e971cee8
R 8	input	8c81e5ab	1a388800	49544348	3692a380	4ad392bd	9980acfc	0b28d64d	b44dfe2a
	T	2bc0213d	5c1c6a20	34608397	dd4f7136	2fb05744	954e2597	2e6e434c	cea274dd
R 9	input	1ba970aa	95a8f0e2	85052ba1	e4ea268e	4de65442	9404df6c	c5815c96	5a3de261
	T	5afe9209	0831378d	0a4d6f2d	86ffc3fe	edec75d	ee2147fd	40957580	580d2881
R 10	input	dc042cd4	45c4483d	3fe999d4	a99ec586	2a6ce80c	5937c6fa	197c3ca3	09cc5611
	T	976ab445	fbef3101	942016ae	d6851fee	6de53db3	1326e9bb	2269918c	6a6f04af
R 11	input	c6840874	05fcc2bc	466ff3a0	9464d1f0	9bae7604	b1ad6a39	c1c669db	80506c0b
	T	1efe2fc3	6f180ba3	e639933c	cda5e6d1	13096d01	7bca006c	3539ac41	a3bfd7e5
R 12	input	ce223323	73d738b9	ed7e1819	e3c00597	6a12d500	e405dcf4	6a02affa	2f629c75
	T	83f35824	08bb252a	c30abfbc	cb816313	a8b3da7c	a93a91c7	b663dd9e	b9f84638
R 13	input	ae2f2ee3	5ddf3518	d39510e1	520dd4b5	260353a8	eeae808a	02717521	9fcd7899
	T	a52e312c	bd9aaa25	3c464fc0	c6572258	1615f437	aa88b23a	ca25b846	e7c5cd57
R 14	input	675b6f2e	f087f9e2	1fb759cc	19fb7dd2	5859f7b8	e54ae194	31818c09	5299b5ae
	T	d38cb9c	8cc18df7	03c62d37	5d281604	a455d560	5f1217a6	7e0fbad1	fa9003d9
R 15	input	e908fe42	a8492f87	6d73e8c5	ab9dd23b	93acb596	66b894a6	b3029753	edced3b7
	T	9bb79f09	beb208f8	5b1fc4a3	1e9f419b	bf33e0b0	cbd0500d	17bc87be	2a2b3f95
R 16	input	3c257a4b	d2c5410e	dc24ff82	45fc4f6e	2ab135ee	7f0f867d	9e2b71c0	04430fc5
	T	ae03a1cb	5b8b19f8	e0d4a094	8902ebe9	6bd241b6	15ddfb67	424d5ef0	91c6956c
R 17	input	599afec9	6dbe1679	44137817	41b3effa	8ba9167f	a5eb4b7d	ea0321de	f7c3dbac
	T	0be8c520	a87b80c1	0d2d3989	d90f6c9c	bbf79371	ac4b14cf	f0cb865e	6b7c1957
output		06b6138b	c89b4013	d8bdd696	4d2c6c79	93c14bb3	21968770	d2fc89a7	be88cd02
output		06b6138b	c89b4013	d8bdd696	4d2c6c79	93c14bb3	21968770	d2fc89a7	be88cd02

$CP_{R,0}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626364	65a50e73	63646566	c319255d	65666768	7ac4f161	6768696a 7e050b4f
R 1	input	27b4957b	63646566	d4628f41	65666768	08be83df	6768696a	274af600 61626364
	T	696a6b6c	53e70ee1	6b6c6d6e	862c6e6e	6d6e6f70	603e6fba	80000000 9a999906
R 2	input	e40e34f4	a91af7aa	2228576e	da74a17e	556711da	6d6c3dd1	bf5db82d 67960b2a
	T	f183fdb3	70b0e9e5	ca006e90	0a3cd93c	d23deb79	a68d6115	67c7f609 33965bd8
R 3	input	ce2c9dc3	feac6b89	4d4edde6	5425a643	02052050	3924417f	de9ae89b 4c9873f9
	T	f7d10a0d	9c03c492	6a921b9d	691dda35	3ffd2edb	2e45580f	e3a79d37 743fdaaf
R 4	input	bff89a31	d98cb6b7	d23b6380	699ac062	5a5ae845	b8da986b	8c81d927 61eba94b
	T	e8eac368	2197bf8f	18a4869c	1609d9d3	b547ad57	5f40a0c6	dc5c2ef1 d03a7612
R 5	input	6aebd481	e99a939d	88642f15	7b07af8d	1edbc639	1af04bd2	80d908d2 b210c47c
	T	d52d82d6	8ba51c00	a6e3711f	20d2b1e7	c0b39cc0	fda07b6c	21129cb7 d12b3732
R 6	input	c93149da	ee500212	98913fe5	25734c26	e9d5a748	59924831	65d7adae f1d9be5f
	T	ea944cbb	44d380f4	5c76fff9	34c83422	c520c1df	ecde76ce	aed562d2 28bf6b23
R 7	input	4b9d944d	03d69c4f	83f5d65e	9d5c0cfd	3b4e6e0c	712ee2c7	bcba39d9 4a8889f3
	T	19d32d4a	937ce097	43bd88f8	b6f63882	0eca978b	cd5d409b	09d85bef e971cee8
R 8	input	0f4ef403	3ca16e5a	bad5a6d5	31297b7c	ab908bc3	b320c724	41c481f6 1a350dcd
	T	2bc0213d	5c1c6a20	34608397	dd4f7136	2fb05744	954e2597	2e6e434c cea274dd
R 9	input	0d7ebe6b	0824a6f8	af42d83c	815e4bcf	d8bdb3e4	6ee60e10	bd2cc4a1 20dc39b7
	T	5afe9209	0831378d	0a4d6f2d	86ffc3fe	edec75d	ee2147fd	40957580 580d2881
R 10	input	aad4a2b4	37870708	adf81309	c22d9849	0eecb2d3	ab2773d5	875b1509 6204efd5
	T	976ab445	fbef3101	942016ae	d6851fee	6de53db3	1326e9bb	2269918c 6a6f04af
R 11	input	1518ef6e	7a50b412	b9ea0548	e0271584	779329d6	2a00af59	8f751de2 351e16e5
	T	1efe2fc3	6f180ba3	e639933c	cda5e6d1	13096d01	7bca006c	3539ac41 a3bfd7e5
R 12	input	1719f8d7	ebfe4a87	29cdfbec	b5d9b40a	72acbb20	bc0f0cbd	d87bb679 b44e5197
	T	83f35824	08bb252a	c30abfbc	cb816313	a8b3da7c	a93a91c7	b663dd9e b9f84638
R 13	input	577832e5	2f8bf75b	be0b862d	d1111df7	e365855e	7a69f3e1	a2145153 7986c2a4
	T	a52e312c	bd9aaa25	3c464fc0	c6572258	1615f437	aa88b23a	ca25b846 e7c5cd57
R 14	input	7975a43e	62456f5b	7798d91a	8ffab53e	d3538e79	3af6c3ef	5f407808 cc8887e9
	T	d38bcb9c	8cc18df7	03c62d37	5d281604	a455d560	5f1217a6	7e0fbad1 fa9003d9
R 15	input	2241f23e	2af2c317	ecf859ed	8e088ea5	7b6132d8	c6e5e389	9329bc95 4471d0c8
	T	9bb79f09	beb208f8	5b1fc4a3	1e9f419b	bf33e0b0	cbd0500d	17bc87be 2a2b3f95
R 16	input	6e9c29a9	411fc303	894d5537	b9f9f5b8	e7dc881c	abe2ad86	599ff22c c8e6cf57
	T	ae03a1cb	5b8b19f8	e0d4a094	8902ebe9	6bd241b6	15ddfbb7	424d5ef0 91c6956c
R 17	input	5a0a5f88	2ec81a55	d7acb54a	8ce72213	040e14c7	2fa80bd0	f18b3903 a2d2cd4f
	T	0be8c520	a87b80c1	0d2d3989	d90f6c9c	bbf79371	ac4b14cf	f0cb865e 6b7c1957
output		381d933f	b546cc8b	0dad2e94	55685992	85dd3ed9	bdc9b2b7	fe8c6751 c7e93517
output		381d933f	b546cc8b	0dad2e94	55685992	85dd3ed9	bdc9b2b7	fe8c6751 c7e93517

AURORA-512 (M_2 : 2 block message (2/2))

$MS_{L,1}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	d06c99c9	00000000	85b16108	00000000	1ce9e324	00000000	16a3f45c
R 2	input	581c39b0	40502cd6	6a73a0c5	bdd1dac3	ae288d68	072f6edd	320949e9
R 3	input	4a15fa26	a12219e9	5d052b54	add66f11	276e760d	6b3cef93	643942d5
R 4	input	874883ad	598d5f03	072e9574	d2caf507	4c0e8331	22bcaa94	f45478c0
R 5	input	c04954e8	2f5e603c	62decba9	2dd3ee3c	1b735d4e	92442010	6e446fa6
R 6	input	0f91b793	4c05afb2	31affa3a	59e4006e	9b045b40	2ebca72f	8d0d8f3b
R 7	input	0a5c0d44	5c3b37ac	cecab602	0509701a	08f00fd8	c8a10d6e	ae55048f
R 8	input	c3b1890c	fe65c45f	fe7f8d74	0e419b42	8b8db691	459c109f	97c448ef
output		da806814	24e5ac4b	42084eef	4c49d5ad	ed7a3bf5	a8e62b6a	f5c634bc
$MS_{R,1}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cd991fb3	00000000	60a599cb	00000000	0e357107	00000000	9a51b2ae
R 2	input	99e09a92	de175c14	0b164a1a	da1fecce	4bd0c990	9b126664	65a79c85
R 3	input	717d5404	7abadec1	788127c0	031e483f	461e3244	4139a10e	7bb80eb1
R 4	input	77e71c40	51a68c42	bc9f4c1d	c17af6b4	625af1a9	12009496	20c6a1be
R 5	input	25098541	6c025baf	a4872a66	f041cabf	e800d5c1	55aee88f	c054d2a5
R 6	input	26554ea2	7cbbb6de	1c46a563	997bbe01	e464ba1b	792d60cb	c883e59c
R 7	input	d969560d	1a6c957c	20d99453	a203acd4	52f6817e	59b07836	ea8a4d28
R 8	input	bf6d27a9	961993de	443c6b27	9a7157ea	7d2ec78d	72942327	7707fceb
output		3f5d49f9	a944da27	2ad57a20	b0a42dca	cd8681f4	bf12a2d3	ce73702b
$CP_{L,1}$								
input		06b6138b	c89b4013	d8bdd696	4d2c6c79	93c14bb3	21968770	d2fc89a7
	mask							be88cd02
	T							01010101
R 1	input	00000000	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000
	T	01d3d28e	d8bdd696	84a09dfc	93c14bb3	330b77b5	d2fc89a7	a2647f04
R 2	input	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000
	T	9b124316	f56f039a	9655281b	2128eae1	e1df29dd	1b0f915d	b327f437
R 3	input	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd
	T	2c47c045	61214da1	c1f10aec	68bbc334	69354744	129c8681	82802acd
R 4	input	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664
	T	992bc312	c4207e76	5c9761a8	69b4de54	c9eb377b	8cd6dd3f	c0e02ef1
R 5	input	b874283c	940aedaa	a12219e9	badc844c	add66f11	2739fa54	6b3cef93
	T	7f4e1700	70be8e77	221943f6	5f482240	1f3a33a6	a070b14e	10910ded
R 6	input	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e
	T	f0659148	d08441dc	f8ec94c5	c861c943	900f3559	8ca66110	f6dfc218
R 7	input	f6559074	0e5d0780	598d5f03	0e1cf15b	d2caf507	4c548374	22bcaa94
	T	802e8446	9b847692	fdb65b17	99b6df84	f1de0619	4581c13f	cb5fb50d
R 8	input	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496
	T	bbcd989f	9b4d9b82	d0e7ebf7	7a73242e	59b4ab41	223548d6	3a445294
R 9	input	c0ebe971	81bcb4c	2f5e603c	c4e6dfd1	2dd3ee3c	1b4454a9	92442010
	T	86c53e5c	afc7d0f6	f1a679f1	e0d544b2	7eff72ff	f436031c	b062b68c
R 10	input	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f
	T	744a60df	72fe2956	3e487aa9	f0499af2	08d97fb0	f81a97b0	1e41a15e
R 11	input	fe0c9455	1f5eb676	4c05afb2	62091f26	59e4006e	9b0db73a	2ebca72f
	T	9f2ec871	eb924b19	9df47813	aab02355	b8be78fa	1beffc70	ae150684
R 12	input	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb
	T	b027c09b	0efb5a46	f7f41cdd	8bbefd15	bdff2aa9	6289af7b	29058eec
R 13	input	d5417c22	15941f1f	5c3b37ac	9de00888	0509701a	08550d02	c8a10d6e
	T	31522be9	3b7ac71b	14716302	e324947a	1d8885ea	42526bde	b4089c73
R 14	input	9d40c1ad	eccecc094	1a6c957c	107b2686	a203acd4	528a5653	59b07836
	T	fb0aa2e7	49a95286	e79fa982	ffea9742	5e518575	5f76239f	bd78b9f4
R 15	input	c9a53398	86ff6ddf	fe65c45f	fd1a9019	0e419b42	8bc48974	459c109f
	T	1220a288	681643a8	162a7a7c	46dd9c79	ba73a2b2	8bb6394b	9abc7e37
R 16	input	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327
	T	ce43318d	f7305e38	657b9fb3	d3c269c2	c28a3279	b461b346	3e8e482a
R 17	input	da806814	49cb5896	42084eef	9893ab5a	ed7a3bf5	a8e62b6a	f5c634bc
	T	445b2bb7	44249963	48fb0996	14dea50e	2e409218	925bcf70	7193268d
output		3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b
output		3cd70a77	130cb7fe	e92c7fa4	0f75b66f	0d01afa5	edce43f2	53ebb8b0
output		3a6119fc	db97f7ed	3191a932	4259da16	9ec0e416	cc58c482	81173117

$CP_{R,1}$									
input		381d933f	b546cc8b	0dad2e94	55685992	85dd3ed9	bdc9b2b7	fe8c6751	c7e93517
	mask								01010101
	T	00000000	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000	166c6124
R 1	input	56354f27	0dad2e94	49e2d19f	85dd3ed9	d31c87a2	fe8c6751	89e46341	381d933f
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000	9a999907
R 2	input	2c3a9fcb	e4e9467d	524a970f	877c1b25	9275a79d	76210ccd	7cb08aa2	1d622b0d
	T	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd	321ca068
R 3	input	9f8f8f7f	6fda0b74	d5cc654c	0922ec9f	234769ed	2e10bb80	d3b83a49	93f1e5b6
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664	65e04a90
R 4	input	a3bd69e0	410c1a4f	4fdd8949	2e7dc954	8aad271a	cc9d8e16	4f52ec42	f68e8b4c
	T	b874283c	940aedaa	a12219e9	badc844c	add66f11	2739fa54	6b3cef93	64152b0d
R 5	input	169d4a26	fd7164e6	ce35d082	1acebfb3	6b84a182	faad0b12	f5bf34c4	b3c2b6e3
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e	7b7d2744
R 6	input	7b40af91	852d295c	d27a006e	7951113e	2de533e7	694d29cf	9f1d8fa1	36f2154b
	T	f6559074	0e5d0780	598d5f03	0e1cf15b	d2caf507	4c548374	22bcaa94	f4489531
R 7	input	7a044835	e24357ac	01bb4559	158c7066	34d6a7d8	d4033052	8fd5cad4	46fa300b
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496	20e74ca9
R 8	input	788b85ce	7bede794	8fbc0973	654fe5f6	3acceb45	92d69d63	bfa418d6	a9452109
	T	c0ebe971	81bcb4c	2f5e603c	c4e6dfd1	2dd3ee3c	1b4454a9	92442010	6e49cb4e
R 9	input	9238ceea	d64bd1bf	2783858b	5ed1a979	aa23893d	cd10a2c3	b03c605b	ceda93a3
	T	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f	c0092ac1
R 10	input	3f63b09a	c0aac6cc	b7d3ebb6	f979e95c	8dfec230	8da8bf6c	c321a871	944c8bf9
	T	fe0c9455	1f5eb676	4c05afb2	62091f26	59e4006e	9b0db73a	2ebca72f	8d91fa40
R 11	input	27c172f9	89516944	1dbf01be	ceea2797	c36f8cde	e1bb0630	581d0821	7db1d585
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb	c855a51b
R 12	input	233257ad	8f72200c	3afbfb94	40c62f14	59f895c6	2274764e	28e45f7e	917b6d72
	T	d5417c22	15941f1f	5c3b37ac	9de00888	0509701a	08550d02	c8a10d6e	ae5cb6d8
R 13	input	87332d75	d518c05e	7864b97f	f1f04ef5	51b9ce9c	5270d1d7	c75b1e5c	86f8fd13
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203dcd4	528a5653	59b07836	ea69947e
R 14	input	e6ac1fe9	362fb7ec	f3928a84	4ab5e01c	72de6712	7c69376b	79022de4	c009c330
	T	c9a53398	86ff6ddf	fe65c45f	fd1a9019	0e419b42	8bc48974	459c109f	97b18d91
R 15	input	9478feab	657c46d5	3b2bf9ab	d2f2a697	1f318d6f	00ee22e0	0e8e0306	b6d8afc0
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327	776d6b8d
R 16	input	5a638169	0fe38643	ea2d5824	fb555cb2	f054d109	bfdb2e1b	86adf72d	3656743e
	T	da806814	49cb5896	42084eef	9893ab5a	ed7a3bf5	a8e62b6a	f5c634bc	3c630724
R 17	input	d5b2c922	725b7b3d	7a7ebbcc	36a79d46	917c93f8	a18f4783	9a615f86	053f873b
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b	b1b6e385
output		d3aadcf58	ca0e838f	6a751f7c	ae55eeff	7497b4f8	a78cd05c	8fbcfb785	f546a310
output		ebb74f67	7f484f04	67d831e8	fb3db76d	f14a8a21	1a4562eb	7130d0d4	32af9607

AURORA-512 final mixing (M_2 : 2 block message)

MS _{L,9}									
input		3a6119fc	db97f7ed	3191a932	4259da16	9ec0e416	cc58c482	81173117	3bbb2e64
R 1	input	0bd75ddf	3191a932	c7264f8a	9ec0e416	d0b01440	81173117	2dfb2eb1	3a6119fc
R 2	input	3fdf76b8	be3bacc8	0a9e2195	c697a484	54837968	bf8df621	b0582db9	a4b03cac
R 3	input	cd3c497a	e655b7f2	6172042d	04b94494	365f4d3c	8f699dc0	d6f4923d	c16893ca
R 4	input	935b90e1	37160aca	c0d52cf2	89da94d2	f3fa2a53	5eb3a800	f11106ff	a5d99750
R 5	input	28ed5d87	c1383d86	d73227bf	0a9fe5be	4005b514	c56ccb6e	6a07530f	469c5411
R 6	input	1ede11b2	f4791911	ae53ab30	faa24d1a	6f34d12e	c2844b21	e76332ec	01964338
R 7	input	4922a5cd	85ab1351	b4c5b75c	cb42344a	2a2643e9	7045db32	e9266da2	2e3286ac
R 8	input	f93dddfc	488a05fd	866c8eff	a09a1995	9d292565	1163e9e5	38fbcde7	2a26846d
output		078dd63e	4f07d3c3	faca5b4f	5a5042da	c118ed17	d07b04f2	ef9e6d5e	c5b8e933
MS _{R,9}									
input		ebb74f67	7f484f04	67d831e8	fb3db76d	f14a8a21	1a4562eb	7130d0d4	32af9607
R 1	input	b2367dde	67d831e8	9bed0f20	f14a8a21	14083e01	7130d0d4	a81405aa	ebb74f67
R 2	input	9207fc7f	92ca9fd8	b66dc74b	a30e5a4b	43472b11	7f42a482	6a86d5ba	510ff415
R 3	input	a1b154b8	05cb90f8	7ee39a15	35428a0c	947e6f37	aa56cfaa	fc4b4f64	9bdc5167
R 4	input	c9f54daf	f4bf109e	2f757ee3	5052c9ee	181f65c2	a3ad3874	0d81ff31	557768b3
R 5	input	900df4b5	9d5d3001	c4f09109	92b41732	3b772a01	c43189f9	900c86ae	6d6e4fda
R 6	input	4aad986b	2180fa9a	23607353	34160947	d8aaa129	2cbbd55e	8d7174f7	1dbec65f
R 7	input	b06aaa74	a43dc643	33d439b0	374795a2	92cae286	f8caa50b	d658a920	a976eee1
R 8	input	7bf6791d	e1a5501c	a643d22a	6deb44da	2bd61649	ff39b5af	cee776ff	05eb1185
output		c030f8e8	2195abf4	880f8856	e5e45c8c	6af2111d	95cba4b2	7e9b3f58	7b702edd
CP _{L,9}									
input		3a6119fc	db97f7ed	3191a932	4259da16	9ec0e416	cc58c482	81173117	3bbb2e64
	mask								09090909
	T	3a6119fc	164c2963	3191a932	8f605dbe	9ec0e416	d0fb5d8a	81173117	2dd74f40
R 1	input	a55355cc	00000000	0f83588c	00000000	12cd2fbf	00000000	14f27d20	00000000
	T	ebb74f67	59769f55	67d831e8	4d8402ef	f14a8a21	14147d20	7130d0d4	a8360f01
R 2	input	d75dbe8f	9469dcee	7e1ad6b6	ed237621	145ee44c	7161329d	94df8ae5	fe91d78a
	T	a4b03cac	7f3cf372	be3bacc8	15065b70	c697a484	54587695	bf8df621	b0df2168
R 3	input	7b367e55	a2da457f	f19bd5d6	42a4efd9	a8f8173d	f9653bad	9be6f673	e121f250
	T	510ff415	c93695dd	92ca9fd8	5b23eabf	a30e5a4b	4386fc4b	7f42a482	6a07c711
R 4	input	b0b17254	b69dfce7	9671dbe3	f53c02e7	cf5f9a92	d0381ab1	d0a1e793	c3e762ab
	T	c16893ca	9ae49a7a	e655b7f2	c2bf24f5	04b94494	36f4492d	8f699dc0	d63c043c
R 5	input	59414589	bcee8eef	4d9c4aa8	a6ae2f6c	02f6e012	f9086ae4	143bdf85	6d9daccd
	T	9bdc5167	50f1b7fa	05cb90f8	3f3f7b5c	35428a0c	94b45415	aa56cfaa	fc4b19a37
R 6	input	1b718992	0c04cc4d	21c434d2	f54bc818	1028607d	92d38734	afdd7023	3dec4ac6
	T	a5d99750	27aa55ff	37160aca	81f40dc3	89da94d2	f31190f2	5eb3a800	f15b2c53
R 7	input	9b6bb953	a3aa391d	191d380d	9e4576e9	0ca9f430	9f26f460	b38c52e9	fd467f25
	T	557768b3	e4bab298	f4bf109e	978fffd7	5052c9ee	18814de3	a3ad3874	0df57ec2
R 8	input	6a3b911f	1027d3c4	303f446a	26707648	3496a1c9	ad245bf1	9c8f8005	4bcb78c6
	T	469c5411	50656a1f	c1383d86	ae0aa70e	0a9fe5be	40075dbf	c56ccb6e	6aed2714
R 9	input	c1eab24e	9a1f37e7	1c33125a	0209d9aa	6faef9b5	f385b295	1ba02636	eb316116
	T	6d6e4fda	c8781557	9d5d3001	623bc35a	92b41732	3b0cf409	c43189f9	900d9101
R 10	input	31eedc78	31e5df3d	deb8ea00	9d3f3b30	d37a3874	397c7a05	8d290b2d	1cf3be93
	T	01964338	3ca7a3d9	f4791911	5c686564	faa24d1a	6f631130	c2844b21	e7deab2e
R 11	input	404971f2	0a8e0fb9	97369152	8d3c9cdf	09c96a74	820a9cee	83d52f31	239c8244
	T	1dbec65f	a53050fb	2180fa9a	91d53a35	34160947	d8719853	2cbbd55e	8dad7329
R 12	input	e174e1cb	a483383c	b8157242	1f4fdd62	21d503e8	87068c89	948e5728	c6133566
	T	2e3286ac	938a8745	85ab1351	684cdb9a	cb42344a	2a26a55c	7045db32	e922b7e9
R 13	input	3cf22ef9	77c34093	e09f3d27	b2a25ea3	45fc04ca	a5f7fa8f	3f30cc4a	ec635390
	T	a976eee1	586a7110	a43dc643	19e554ba	374795a2	9258aab0	f8caa50b	d66a3986
R 14	input	e1acbfd9	fb400f42	b34e28db	cb4eacdf	d8f86495	045a5b25	a9ef0fa6	17d45772
	T	2a26846d	f2d84bcf	488a05fd	0c539bfd	a09a1995	9dfbddff	1163e9e5	383d8e65
R 15	input	dc160902	303caff9	3d1bf660	c33d9983	dc5baece	4923bfa3	7d946322	54d5b7af
	T	05eb1185	bda18b7f	e1a5501c	d36b3b0e	6deb44da	2be7792a	ff39b5af	cef6d249
R 16	input	1939b3c2	7627c415	671b9fa5	924fb001	e0bdf763	dd59542c	80ec510d	246407d
	T	078dd63e	9e0fa786	faca5b4f	b4a085b4	c118ed17	d07b04f2	ef9e6d5e	c5b8e933
R 17	input	161ff5ac	fbe8c7f5	228a025d	961865d5	91f0cab4	eccf38f6	73929ad3	70b24b31
	T	c030f8e8	10cad5fa	880f8856	72f22e46	6af2111d	95cba4b2	7e9b3f58	7b702edd
output		f1952b3f	da87c2d8	c15ea915	adb66ad0	be86a558	ad702801	3ac78dd8	4f9ed76c
output		cbf432c3	01103535	f0cf0027	efe2b0c6	2046414e	6128ec83	bbd0bccf	7425f908

CP _{R,9}									
input		ebb74f67	7f484f04	67d831e8	fb3db76d	f14a8a21	1a4562eb	7130d0d4	32af9607
	mask								09090909
	T	3a6119fc	164c2963	3191a932	8f605dbe	9ec0e416	d0fb5d8a	81173117	2dd74f40
R 1	input	2bc05bf5	564998da	63c35441	6f8a6e37	b8faebde	f027e1c3	4f303914	d1d6569b
	T	ebb74f67	59769f55	67d831e8	4d8402ef	f14a8a21	14147d20	7130d0d4	a8360f01
R 2	input	8dba5355	8585ac53	c331d15b	a01bb929	50083e09	9efac127	3673dae4	b3ee6ce0
	T	a4b03cac	7f3cf372	be3bacc8	15065b70	c697a484	54587695	bf8df621	b0df2168
R 3	input	93c91feb	b6276ce2	141c526c	71448042	32e0f0ca	0ab3dabe	6b12b78b	67ea2398
	T	510ff415	c93695dd	92ca9fd8	5b23eabf	a30e5a4b	4386fc4b	7f42a482	6a07c711
R 4	input	bd48a3ab	234e16e3	c75392d8	b154b22f	409f883a	10cc1477	84e8eb3f	d8e3616f
	T	c16893ca	9ae49a7a	e655b7f2	c2bf24f5	04b94494	36f4492d	8f699dc0	d63c043c
R 5	input	f6df96fd	c414eae4	57199af9	cbc86155	dedc83c0	51f6fe19	2e4acfe7	465e544a
	T	9bdc5167	50f1b7fa	05cb90f8	3f3f7b5c	35428a0c	94b45415	aa56cfad	fc1b19a37
R 6	input	cfb84765	f181d529	8b5fedee	1e71ce5a	050e00a9	6782fdf7	00369ff0	4f3c1833
	T	a5d99750	27aa55ff	37160aca	81f40dc3	89da94d2	f31190f2	5eb3a800	f15b2c53
R 7	input	d853301b	a3bf2bb7	c6400241	8707ae15	4c79d2d8	c88ec9d4	9bc4c0a7	ead6ec56
	T	557768b3	e4bab298	f4bf109e	978fffd7	5052c9ee	18814de3	a3ad3874	0df57ec2
R 8	input	c74b71c9	ad455f4b	a7a6ffac	5f07860b	f754e4fe	e58d2104	f00e4d54	494dc261
	T	469c5411	50656a1f	c1383d86	ae0aa70e	0a9fe5be	40075dbf	c56ccb6e	6aed2714
R 9	input	56b7545f	c7a92a92	88133d0d	6df98d0c	920322ee	f313f654	3540ddee	8b4cecfad
	T	6d6e4fda	c8781557	9d5d3001	623bc35a	92b41732	3b0cf409	c43189f9	900d9101
R 10	input	870b53ba	3edb184d	3b7e862c	0993f2b3	f2c34423	c4c57f98	06659319	77d66aa6
	T	01964338	3ca7a3d9	f4791911	5c686564	faa24d1a	6f631130	c2844b21	e7deab2e
R 11	input	78f24e5c	ee4689ef	0ccb7e47	705030e4	638f8b89	ae6d2d50	7ae23f25	00d7cec2
	T	1dbec65f	a53050fb	2180fa9a	91d53a35	34160947	d8719853	2cbbd55e	8dad7329
R 12	input	99a2e708	3b86507a	f266a60f	4699d599	816a6908	c8e45d68	a7f23c50	679b0c87
	T	2e3286ac	938a8745	85ab1351	684cdb9a	cb42344a	2a26a55c	7045db32	e922b7e9
R 13	input	6714bf25	bcf0ae6c	3b03d7b7	8afd1b15	2c322450	3125018b	a5fe7de0	af06050d
	T	a976eee1	586a7110	a43dc643	19e554ba	374795a2	9258aab0	f8caa50b	d66a3986
R 14	input	451a616a	8891ba8c	814ff682	2e34fbd3	20a22ce5	6b50cb4f	d2405465	8a8c784b
	T	2a26846d	f2d84bcf	488a05fd	0c539bfd	a09a1995	9dfbddff	1163e9e5	383d8e65
R 15	input	94cce482	1878a675	6528fbb9	8df596fd	ef1276e1	b2a46993	05543253	9fc1c810
	T	05eb1185	bda18b7f	e1a5501c	d36b3b0e	6debd4da	2be7792a	ff39b5af	cef6d249
R 16	input	431f96ae	70b07376	cc5eebf3	a094dd2b	b8c02600	0880dd86	245cb47b	4a300969
	T	078dd63e	9e0fa786	faca5b4f	b4a085b4	c118ed17	d07b04f2	ef9e6d5e	c5b8e933
R 17	input	e6dab3c6	8ca64c0e	4b43eeaf	f6c3edc2	b2b12a74	b70ad0a5	1ba1d28a	43988a38
	T	c030fbe8	10cad5fa	880f8856	72f22e46	6af2111d	95cba4b2	7e9b3f58	7b702edd
output		4eb15b5f	12ed3943	e849fcaa	e477b778	8a652f06	c2564a0c	078ee2b6	41fd790b
output		a5061438	6da57647	8f91cd42	1f4a0015	7b2fa527	d81328e7	76be3262	7352ef0c

AURORA-384 (M_2 : 2 block message (1/2))

$MS_{L,0}$									
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a	68696a6b
R 1	input	b205f1ae	63646566	e1d20b61	65666768	7a8c874f	6768696a	7ec49239	61626364
R 2	input	3896619e	ca006e90	85585b15	d23deb79	a61e74d8	67c7f609	338d6cf2	f183fdb3
R 3	input	903aa0e9	18a4869c	8bc76c6	b547ad57	5f04df12	dc5c2ef1	d040ecc7	e8eac368
R 4	input	22bf7611	5c76fff9	1a69b6ce	c520c1df	ec64c023	aed562d2	28de1a7a	ea944cbb
R 5	input	2ea2259b	34608397	6e0e7497	2fb05744	95a735dd	2e6e434c	ce4eb810	2bc0213d
R 6	input	7d6fe9f7	942016ae	ebf704bb	6de53db3	134298af	2269918c	6a268f80	976ab445
R 7	input	84f89189	c30abfbc	655d46c7	a8b3da7c	a9c09238	b663dd9e	b93ab195	83f35824
R 8	input	46901702	03c62d37	ae6003a6	a455d560	5f94c6d9	7e0fbad1	fa120bfb	d38bcb9c
output		ae03a1cb	adc58cfc	e0d4a094	448175f4	6bd241b6	15ddf6b7	424d5ef0	91c6956c
$MS_{R,0}$									
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000	00000000
R 1	input	a7996fdc	6b6c6d6e	0cce99ba	6d6e6f70	60581d06	80000000	9a3edcc3	696a6b6c
R 2	input	383f586b	6a921b9d	d207da0f	3ffd2edb	2e3b89af	e3a79d37	7445b424	f7d10a0d
R 3	input	172b7bcf	a6e3711f	414a376c	c0b39cc0	fda53832	21129cb7	d1a06300	d52d82d6
R 4	input	26714005	43bd88f8	6df9ce9b	0eca978b	cdecc1e8	09d85bef	e95d712f	19d32d4a
R 5	input	100d47fc	0a4d6f2d	0d6228fd	edec75d	eeff6f81	40957580	5821871b	5afe9209
R 6	input	debf00a2	e639933c	9b30d76c	13096d01	7b4b17e5	3539ac41	a3cacd47	1efe2fc3
R 7	input	7bc5b2b1	3c464fc0	8c35cd3a	1615f437	aaae5457	ca25b846	e788444b	a52e312c
R 8	input	7d2b5037	5b1fc4a3	3d643f0d	bf33e0b0	cb3e1195	17bc87be	2ad083f0	9bb79f09
output		0be8c520	50f70183	0d2d3989	b21ed939	bbf79371	ac4b14cf	f0cb865e	6b7c1957
$CP_{L,0}$									
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask								00000000
	T	61626364	65a50e73	63646566	c319255d	65666768	7ac4f161	6768696a	7e050b4f
R 1	input	f2ccc2c6	9c9b9a99	fe02c41a	9a999897	8b120022	98979695	8a6a2022	9e9d9c9b
	T	696a6b6c	53e70ee1	6b6c6d6e	862c6e6e	6d6e6f70	603e6fba	80000000	9a999906
R 2	input	9b46f352	a447cea3	13d4e5f9	59fd75a30	d0f5c018	6e71d288	dfb23044	a688dc0d
	T	f183fdb3	70b0e9a5	ca006e90	0a3cd93c	d23deb79	a68d6115	67c7f609	33965bd8
R 3	input	58683a65	3c41414a	b082a4cd	b9d013aa	aa9680d4	5f283252	37fd9e56	a8a9acb0
	T	f7d10a0d	9c03c492	6a921b9d	691dda35	3ffd2edb	2e45580f	e3a79d37	743fdaaf
R 4	input	64f54f9a	95ae1895	84b68517	627ae638	0f7e22d8	69203719	ab9a4b9a	7a5071c0
	T	e8eac368	2197bf8f	18a4869c	1609d9d3	b547ad57	5f40a0c6	dc5c2ef1	d03a7612
R 5	input	99b214cc	38e73b3d	74207abe	837153fa	46fe36a2	7e768129	76b642ca	1ce3eba7
	T	d52d82d6	8ba51c00	a6e3711f	20d2b1e7	c0b39cc0	fda07b6c	21129cb7	d12b3732
R 6	input	33032435	150a7320	a1605b82	f5b0b730	0b3c45ab	1f085899	fcdb98e8	04e4a294
	T	ea944cbb	44d380f4	5c76fff9	34c83422	c520c1df	ecde76ce	aed562d2	28bf623
R 7	input	d934aabb	6c8dae0f	080e1bfe	d6e0986	9129e9a2	d1fa660b	e4c176f8	8a6fd3b9
	T	19d32d4a	937ce097	43bd88f8	b6f63882	0eca978b	cd5d409b	09d85bef	e971cee8
R 8	input	8adce245	8671b7c2	73a33d84	f900c4d0	2e18cf15	a0125409	a167c4cb	5f1296ec
	T	2bc0213d	5c1c6a20	34608397	dd4f7136	2fb05744	954e2597	2e6e434c	cea274dd
R 9	input	0898bf21	8025c139	5f654a10	c11a11ca	51f943ca	1d6ad622	a7e30a09	d514ca3c
	T	5afe9209	0831378d	0a4d6f2d	86ffc3fe	edec75d	ee2147fd	40957580	580d2881
R 10	input	ca2593f3	e0ef425e	bf7bf312	f001730e	fab7e99c	203f8437	ef8d0199	0ad366f0
	T	976ab445	fbef3101	942016ae	d6851fee	6de53db3	1326e9bb	2269918c	6a6f04af
R 11	input	2ed37636	3ff26876	252541c8	32aed55	443ff751	6ce5e88d	1f0475e5	cd31e756
	T	1efe2fc3	6f180ba3	e639933c	cda5e6d1	13096d01	7bca006c	3539ac41	a3bfd7e5
R 12	input	c48991cc	0c3ea3f3	34afcfc	f48225f4	a031ee0c	25cf80a5	e6080837	1fbd0d72
	T	83f35824	08bb252a	c30abfbc	cb816313	a8b3da7c	a93a91c7	b663dd9e	b9f84638
R 13	input	a60a38cb	2a088c53	b34b6fcb	1aab9ece	af96baf	c0546edb	1c1dec0c	e8fa0afe
	T	a52e312c	bd9aaa25	3c464fc0	c6572258	1615f437	aa88b23a	ca25b846	e7c5cd57
R 14	input	41101d83	d20b0434	75df52a2	abbbe1ed	c473cea9	eb3698e2	483b3b1d	032635f1
	T	d38bcb9c	8cc18df7	03c62d37	5d281604	a455d560	5f1217a6	7e0fbad1	fa9003d9
R 15	input	1b0168d1	5813712b	2f91cc52	21843dda	17b6b08a	180e30e5	9c67554b	3da02b79
	T	9bb79f09	beb208f8	5b1fc4a3	1e9f419b	bf33e0b0	cbd0500d	17bc87be	2a2b3f95
R 16	input	040b98a4	1e014100	9a2146fc	a13c0953	b06c5748	d24fc715	e35d9ea5	cc1c330c
	T	ae03a1cb	5b8b19f8	e0d4a094	8902ebe9	6bd241b6	15ddf6b7	424d5ef0	91c6956c
R 17	input	40fdf5f6	49a2a67b	8414eee5	e8e0a560	8f757e77	dfd3e1bc	5810d7d1	2200b3ad
	T	0be8c520	a87b80c1	0d2d3989	d90f6c9c	bbf79371	ac4b14cf	f0cb865e	6b7c1957
output		876ef97d	6d5f1ae7	806621d5	bca4d1a0	0dbdf2c7	c5d294c5	8235fcd1	3b82d075
output		78910682	92a0e518	7f99de2a	435b2e5f	f2420d38	3a2d6b3a	7dca032e	c47d2f8a

$CP_{R,0}$								
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask							00000000
	T	61626364	65a50e73	63646566	c319255d	65666768	7ac4f161	6768696a
R 1	input	d84b6a84	9c9b9a99	2b9d70be	9a999897	f7417c20	98979695	d8b509ff
	T	696a6b6c	53e70ee1	6b6c6d6e	862c6e6e	6d6e6f70	603e6fba	80000000
R 2	input	d56a94d9	8fb46278	fb8ef9ae	ee78fe41	9e3692b3	f9f76c47	d4aed2eb
	T	f183fdb3	70b0e9e5	ca006e90	0a3cd93c	d23deb79	a68d6115	67c7f609
R 3	input	526dea4c	023ee239	85838b80	249f80b3	e69bb87b	f53c6b6d	dcbb3e0b
	T	f7d10a0d	9c03c492	6a921b9d	691dda35	3ffd2edb	2e45580f	e3a79d37
R 4	input	e219b42e	8cbcf58	f75a0f8b	8afac47b	75d0e10e	8d58f962	03f9b4e8
	T	e8eac368	2197bf8f	18a4869c	1609d9d3	b547ad57	5f40a0c6	dc5c2ef1
R 5	input	384d382d	750fac28	f78c6d0a	aa51229b	fa2e92f8	8da5896c	b60d3316
	T	d52d82d6	8ba51c00	a6e3711f	20d2b1e7	c0b39cc0	fda07b6c	21129cb7
R 6	input	77a3dccf	3a622b11	9ddb2da5	bf981bd8	e4b12a5b	88d84509	b369099c
	T	ea944cbb	44d380f4	5c76fff9	34c83422	c520c1df	ecde76ce	aed562d2
R 7	input	a46165c3	14a4e53f	0ea0530e	fe12f095	89d7ace1	460dd5ad	a9be17ca
	T	19d32d4a	937ce097	43bd88f8	b6f63882	0eca978b	cd5d409b	09d85bef
R 8	input	9e90c404	c215d435	27e19871	72de7cb2	df6a0a4c	579912bb	9e10c7b4
	T	2bc0213d	5c1c6a20	34608397	dd4f7136	2fb05744	954e2597	2e6e434c
R 9	input	6862e8d7	0ca1328a	e81287ca	7c20c8a6	c1cfe81f	04bca9d9	51eb5715
	T	5afe9209	0831378d	0a4d6f2d	86ffc3fe	edec75d	ee2147fd	40957580
R 10	input	7da08359	6f89e78c	0843034e	d3351ec7	759ca9b8	76b78265	c11976eb
	T	976ab445	fbef3101	942016ae	d6851fee	6de53db3	1326e9bb	2269918c
R 11	input	245d2e48	37ec71ba	e52c56f0	12e2258c	5837d3a4	dd7b73bb	ab205e4f
	T	1efe2fc3	6f180ba3	e639933c	cda5e6d1	13096d01	7bca006c	3539ac41
R 12	input	845089fa	6007c7a2	5077f175	7a3d1971	4a90491b	b18e1caf	bce40b43
	T	83f35824	08bb252a	c30abfbc	cb816313	a8b3da7c	a93a91c7	b663dd9e
R 13	input	0334f32a	96052cef	c88c0b46	6d52cc8e	520f26c1	fb2349ec	fdd6273e
	T	a52e312c	bd9aaa25	3c464fc0	c6572258	1615f437	aa88b23a	ca25b846
R 14	input	770aa952	d559984e	7c6262b6	2971029f	f40c5922	31f756fc	8b815ed0
	T	d38bcb9c	8cc18df7	03c62d37	5d281604	a455d560	5f1217a6	7e0fbad1
R 15	input	132e4bcf	6dfed847	0d8de881	243ba2da	dae65d02	8bfe5e3f	691b1041
	T	9bb79f09	beb208f8	5b1fc4a3	1e9f419b	bf33e0b0	cbd0500d	17bc87be
R 16	input	a284203c	803d2ee9	e239e045	0bad417c	18cd4805	8893805e	fc033ba
	T	ae03a1cb	5b8b19f8	e0d4a094	8902ebe9	6bd241b6	15ddf6b7	424d5ef0
R 17	input	4e88fc8b	241c0992	6f5c31c0	3dc8ac41	968ec1e5	e0525434	b5d59eb0
	T	0be8c520	a87b80c1	0d2d3989	d90f6c9c	bbf79371	ac4b14cf	f0cb865e
output		c5a7c4c5	422888b6	11c13346	f82bca12	9ca73a80	6b49e90a	49064e9a
output		3a583b3a	bdd77749	ee3eccb9	07d435ed	6358c57f	94b616f5	b6f9b165
								5a4edb7a

AURORA-384 (M_2 : 2 block message (2/2))

$MS_{L,1}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	d06c99c9	00000000	85b16108	00000000	1ce9e324	00000000	16a3f45c
R 2	input	581c39b0	40502cd6	6a73a0c5	bdd1dac3	ae288d68	072f6edd	320949e9
R 3	input	4a15fa26	a12219e9	5d052b54	add66f11	276e760d	6b3cef93	643942d5
R 4	input	874883ad	598d5f03	072e9574	d2caf507	4c0e8331	22bcaa94	f45478c0
R 5	input	c04954e8	2f5e603c	62decba9	2dd3ee3c	1b735d4e	92442010	6e446fa6
R 6	input	0f91b793	4c05afb2	31affa3a	59e4006e	9b045b40	2ebca72f	8d0d8f3b
R 7	input	0a5c0d44	5c3b37ac	cecab602	0509701a	08f00fd8	c8a10d6e	ae55048f
R 8	input	c3b1890c	fe65c45f	fe7f8d74	0e419b42	8b8db691	459c109f	97c448ef
output		da806814	24e5ac4b	42084eef	4c49d5ad	ed7a3bf5	a8e62b6a	f5c634bc
$MS_{R,1}$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	cd991fb3	00000000	60a599cb	00000000	0e357107	00000000	9a51b2ae
R 2	input	99e09a92	de175c14	0b164a1a	da1fecce	4bd0c990	9b126664	65a79c85
R 3	input	717d5404	7abadec1	788127c0	031e483f	461e3244	4139a10e	7bb80eb1
R 4	input	77e71c40	51a68c42	bc9f4c1d	c17af6b4	625af1a9	12009496	20c6a1be
R 5	input	25098541	6c025baf	a4872a66	f041cabf	e800d5c1	55aee88f	c054d2b5
R 6	input	26554ea2	7cbbb6de	1c46a563	997bbe01	e464ba1b	792d60cb	c883e59c
R 7	input	d969560d	1a6c957c	20d99453	a203cd4d	52f6817e	59b07836	ea8a4d28
R 8	input	bf6d27a9	961993de	443c6b27	9a7157ea	7d2ec78d	72942327	7707fceb
output		3f5d49f9	a944da27	2ad57a20	b0a42dca	cd8681f4	bf12a2d3	ce73702b
$CP_{L,1}$								
input		78910682	92a0e518	7f99de2a	435b2e5f	f2420d38	3a2d6b3a	7dca032e
	mask							c47d2f8a
	T							01010101
R 1	input	00000000	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000
	T	5b263ea8	7f99de2a	8a9b7fb6	f2420d38	287cd23d	7dca032e	d8df3d0f
R 2	input	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000
	T	01236fb1	24ca69b6	262458c8	c93b4cbb	a6f939b0	d419f439	0202d8f4
R 3	input	f2cc61ce	b0e71bd2	40502cd6	d4509360	bdd1dac3	ae0939c5	072f6edd
	T	bd5cbe6d	24486dd3	6cffd03b	54f5d887	9a4fe060	97d244da	3ad8ac5e
R 4	input	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664
	T	ca6c5cfe	ed582829	49928b6b	cf7e83cc	eadd7f06	6c3afafd	606463ef
R 5	input	b874283c	940aadaa	a12219e9	badc844c	add66f11	2739fa54	6b3cef93
	T	0cdae8b6	33d32b59	c75a4953	d28dfa27	729dfdf7	fc88d353	5ab8f5f3
R 6	input	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e
	T	df55dfbd	46acc14e	e375b4f9	34af6562	30e27e72	3ba5db7a	1be99aba
R 7	input	f6559074	0e5d0780	598d5f03	0e1cf15b	d2caf507	4c548374	22bcaa94
	T	6433223d	abb5cd58	31b95242	6546c3bb	ba211613	b76826b9	55aca2d3
R 8	input	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496
	T	b6b7b0e2	3cb219c0	8bf8c241	b00ceb1e	61bbf75b	5a68f180	30d2cc50
R 9	input	c0ebe971	81bcb4c	2f5e603c	c4e6dfd1	2dd3ee3c	1b4454a9	92442010
	T	a6734fee	33a4ae74	a78ab4af	eab28cba	0ce3581e	15ae29f3	6c580705
R 10	input	7d002c7d	92c3eaea	6c025baf	d2006920	f041cabf	e8548566	55aee88f
	T	1ec168f7	1a951a76	5ca1ed73	3a45b8c7	23d5da4a	1242a881	73d55a61
R 11	input	fe0c9455	1f5eb676	4c05afb2	62091f26	59e4006e	9b0db73a	2ebca72f
	T	8423af53	f2fee40e	4edf73e0	2d077b97	d5de2b2d	56682c1a	15fa8b88
R 12	input	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb
	T	94363b1e	6c42f001	12708bcf	ca68d66d	b1f1b9bb	18d85845	20547c43
R 13	input	d5417c22	15941f1f	5c3b37ac	9de00888	0509701a	08550d02	c8a10d6e
	T	f611922a	771d05a0	19f50073	8f12da35	0b398b80	baf9340c	71667591
R 14	input	9d40c1ad	eccecc094	1a6c957c	107b2686	a203dcd4	528a5653	59b07836
	T	5e72188f	3095d4a1	f2fa6890	ae187282	f7522218	9e334657	d92171ed
R 15	input	c9a53398	86ff6ddf	fe65c45f	fd1a9019	0e419b42	8bc48974	459c109f
	T	c3261d01	f8701de1	d7f94ccd	9ea34600	a3e7fda1	f3b26afa	0b87c5d5
R 16	input	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327
	T	4b32c713	00affcdf	4a874f5b	68d2cc9b	016b1327	a8ffbadb	8a9a3024
R 17	input	da806814	49cb5896	42084eef	9893ab5a	ed7a3bf5	a8e62b6a	f5c634bc
	T	2c31bd4f	ec8fd7c2	5b0f774b	70f73a48	56fbc0bc	41abce93	b724cdd1
output		3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b
output		e7959e3d	60e56d15	5d5d444e	df2d12c3	0cd16a61	3fee87d5	e8e44b0f
output		9f0498bf	f245880d	22c49a64	9c763c9c	fe936759	05c3ecef	952e4821

CP _{R,1}									
input		3a583b3a	bdd77749	ee3eccb9	07d435ed	6358c57f	94b616f5	b6f9b165	5a4edb7a
	mask								01010101
	T	00000000	a163c6b9	00000000	0bd3e993	00000000	1ca39908	00000000	166c6124
R 1	input	5e92eb58	ee3eccb9	1b733fdd	6358c57f	faa03ccf	b6f9b165	149b0f83	3a583b3a
	T	00000000	e6d2b8d7	00000000	301ad959	00000000	0e511fcb	00000000	9a999907
R 2	input	1467841a	af80bd0a	ff771192	23b2d68c	7e99969e	ed3e22cb	e50b8a5e	c6ccf8dc
	T	f2cc61ce	b0e71bd2	40502cd6	4d450936	bdd1dac3	ae0939c5	072f6edd	321ca068
R 3	input	5ce9ec48	fad93eea	e42937d9	0d4da10c	bc8a85ad	02d83a11	24c8c213	1b7df29b
	T	3dac27c2	4c8b64c2	de175c14	85e84e49	da1fecce	4ba79a1a	9b126664	65e04a90
R 4	input	fac4e6b2	7b0ccf8e	7173b52f	6efbc7a3	e6c273a5	5e68a584	551c7499	3a23ea09
	T	b874283c	940aead4	a12219e9	badc844c	add66f11	2739fa54	6b3cef93	64152b0d
R 5	input	17062c69	821cf65e	f150aefc	186ff25f	fb6f00d6	dd9b1403	1eeba877	88a7c291
	T	0763cfee	38c09958	7abadec1	bc0f0702	031e483f	46b854c0	4139a10e	7b7d2744
R 6	input	f4baa058	2b023d79	7eef09df	5a99019e	296b330e	acd25454	61e3d6ea	c60a87b8
	T	f6559074	0e5d0780	598d5f03	0e1cf15b	d2caf507	4c548374	22bcaa94	f4489531
R 7	input	7382686f	f7d52156	377536a4	a8072d00	4c88f6e1	947dd198	3fc1acad	e11b7557
	T	94ecb205	3bcff8df	51a68c42	5e2d50a0	c17af6b4	62c61c1d	12009496	20e74ca9
R 8	input	d36c3657	d500ec6b	9c7286d4	ae88b79b	b1aad156	28d0572c	a21d4e26	171d6d03
	T	c0ebe971	81bcb4c	2f5e603c	c4e6dfd1	2dd3ee3c	1b4454a9	92442010	6e49cb4e
R 9	input	2d037faa	810ece92	bb509821	265bd29c	68a1fb63	1a73f397	d9b02d97	dfe4ea90
	T	7d002c7d	92c3aea	6c025baf	d2006920	f041cabf	e8548566	55aee88f	c0092ac1
R 10	input	a128f42d	470edc9e	48b411d9	90d0fc67	33d0aa72	36dd3c1d	69ebc9ea	5d6efc4f
	T	fe0c9455	1f5eb676	4c05afb2	62091f26	59e4006e	9b0db73a	2ebca72f	8d91fa40
R 11	input	660b2810	174ee296	ea16c237	e04efe6f	56d9d911	6f53b249	1fcc966a	bbbc9a9c
	T	80c7b69a	13235d4e	7cbbb6de	0e3272d1	997bbe01	e4834e63	792d60cb	c855a51b
R 12	input	13ca7dd1	08e47c88	9356aace	e69bb137	71ca52af	a8816e3e	6451dada	3fc92104
	T	d5417c22	15941f1f	5c3b37ac	9de00888	0509701a	08550d02	c8a10d6e	ae5cb6d8
R 13	input	e50b18dc	16ca18d4	1de4875c	5ef463a6	7436493f	d5faa302	eeaa58e0	63ee262b
	T	9d40c1ad	eccecc094	1a6c957c	107b2686	a203dcd4	528a5653	59b07836	ea69947e
R 14	input	5be16174	d1e58d22	bbd64d62	0bb7ec2f	b41019c0	79322b81	998a3a14	be9f654a
	T	c9a53398	86ff6ddf	fe65c45f	fd1a9019	0e419b42	8bc48974	459c109f	97b18d91
R 15	input	2e09c76c	f885f021	e7547072	4ba783a4	83ca9d69	b3090d9c	c380b94b	eb6d8543
	T	7fc593ae	df9e63f5	961993de	a2177e54	9a7157ea	7d072727	72942327	776d6b8d
R 16	input	b2e24621	07f06738	7b9f1f21	a8c3b4cb	10121b60	5eef43f1	3adc33fe	431d0819
	T	da806814	49cb5896	42084eef	9893ab5a	ed7a3bf5	a8e62b6a	f5c634bc	3c630724
R 17	input	f7e50b08	2a60016e	71f7ad37	28c73257	6ed1d0d0	ab932d8c	e535cd25	2fa525e3
	T	3f5d49f9	54a26d13	2ad57a20	d85216e5	cd8681f4	bf12a2d3	ce73702b	b1b6e385
output		094638da	48d91d5e	14378104	ce77df96	15889b06	cc8f95ad	5ea6e4d2	0ec6529f
output		331e03e0	f50e6a17	fa094dbd	c9a3ea7b	76d05e79	58398358	e85f55b7	548889e5

AURORA-384 final mixing (M_2 : 2 block message)

$MS_{L,9}$								
input	9f0498bf	f245880d	22c49a64	9c763c9c	fe936759	05c3ecef	952e4821	652aefe8
R 1	input	22467555	22c49a64	19f48ee7	fe936759	199f6bcc	952e4821	7360c851
R 2	input	c4f5d68d	954791b2	4186ae9c	17ab7dbb	91ac6574	c6c2f87e	6c5d93d2
R 3	input	ddedd9f0	2e73ce47	780e776e	2152da88	6a456407	cef5c1c6	7f503224
R 4	input	ef3eb179	0744474e	d562619e	563be9b8	6d436483	4ed6f1b3	da6cd572
R 5	input	816c9ee4	29ab8f8f	e00b088c	16be7f3e	4c7701cb	dd7cd389	c6439cb1
R 6	input	7e124fb7	19037894	5f783cc5	c2e10b08	4f6f2f88	db2325bd	6730c90d
R 7	input	9c4008aa	a8782924	a16fc120	6240f7aa	9ab656f3	9a9fe1c0	8b831165
R 8	input	8580fe4b	73d5d8a8	14ef20cd	4e5f0055	99747a6e	0b0e33ac	1ae4d359
output	3f4d289e	4c98f036	d76034c8	993f349d	d85becd1	d355df7d	d4b38fec	afc56e4a
$MS_{R,9}$								
input	331e03e0	f50e6a17	fa094dbd	c9a3ea7b	76d05e79	58398358	e85f55b7	548889e5
R 1	input	38119cc8	fa094dbd	a9ab1093	76d05e79	56961be3	e85f55b7	ce6858b9
R 2	input	998ccca3	56e16e5c	f5c7d7ed	ec89ef8e	95f69243	c460f857	096ef027
R 3	input	a15fb04f	d30975ca	e70d6b99	082c3255	123b381c	9cc3fb49	5cf8a601
R 4	input	c6e08996	3f99e0fe	d96d1815	8e0239fb	f057880d	767df8ca	1c44b742
R 5	input	00df5e6e	00494bcf	87de0ca7	8d787d22	f13343e6	78391c5f	f5100dbe
R 6	input	3e67aa61	81dc6080	9c168aa1	7198ae13	213a451e	a979b519	53f784bd
R 7	input	5cdb2af0	874cca93	5531efbe	adc975eb	8d352dfb	a519ecf2	621402c8
R 8	input	7cce8b1c	56b4b254	8b5b614f	7d1f6f46	66492713	39b85307	44c074c6
output	bee15a8c	e855e8d8	8b946de1	f68b02a7	3071bab0	09c9e9b7	f57745bd	d4f569d1
$CP_{L,9}$								
input	9f0498bf	f245880d	22c49a64	9c763c9c	fe936759	05c3ecef	952e4821	652aefe8
	mask							09090909
	T	9f0498bf	45e8d6a2	22c49a64	333f90aa	fe936759	196075e7	952e4821
R 1	input	df535552	00000000	6df5588c	00000000	12bdafbf	00000000	14f25601
	T	331e03e0	1c558ddc	fa094dbd	d4cb2c64	76d05e79	56689c93	e85f55b7
R 2	input	34300f42	dd8e42fd	33a8fbc9	7a27f2b5	4627c1db	af44858b	b53d46ce
	T	4cf4d1391	890ccb44	954791b2	8359271b	17ab7dbb	915dd69c	c6c2f87e
R 3	input	4ccbd2b0	8b39a81f	f265689a	68948db5	483ca53e	43c57cc8	facade98
	T	c77431dd	cce3c913	56e16e5c	fafbf7851	ec89ef8e	956ecced	c460f857
R 4	input	95183e73	7e6301c6	1139202a	e3948c28	fa62f02e	485c9699	f0c61b0d
	T	fa6887a9	ba1cc848	2e73ce47	f08a65e1	2152da88	6a50d96e	cef5c1c6
R 5	input	83ef1b5c	18c3b754	050cf6d3	95d1f360	d0601d40	68eee773	f26f50ff
	T	5f19f716	d0869c00	d30975ca	f39dd327	082c3255	12f8b099	9cc3fb49
R 6	input	e8f2217e	97bbcc4e	9363b61f	c5d2b197	0a883c28	41bd86a3	e380e1cb
	T	1148a068	dec4c8e5	0744474e	aa87aaf3	563be9b8	6d6cb19e	4ed6f1b3
R 7	input	f0b7cb44	49040fa1	d8f1488b	e2e259fe	e2bff1f7	1dc2781c	19d9f7bb
	T	8cad60f2	6336c421	3f99e0fe	6cabdbcb	8e0239fb	f0448915	767df8ca
R 8	input	b0578e93	972bca23	fbf5ced3	5d2cd16e	fb3f7f95	d921d805	91a262f6
	T	dff7ad2b	02160363	29ab8f8f	c0ef39c9	16be7f3e	4c439e8c	dd7cd389
R 9	input	23d79931	861c8f70	fd3a5932	2e902885	2787880c	a91b58a3	9b5915c2
	T	3666d6aa	006f21df	00494bcf	439986b7	8d787d22	f1105ea7	78391c5f
R 10	input	ee7d6c1f	a8ac6456	d74647db	a800a163	691c2353	06282736	c5587f04
	T	892e0fd0	fcf05e1a	19037894	bedf936e	c2e10b08	4f304fc5	db2325bd
R 11	input	83db1962	753e9df5	d28dccc8	0592b151	a68be3a5	7f113643	b73db04b
	T	f4dc59db	9f0b22de	81dc6080	ce1d4230	7198ae13	21f7aaa1	a979b519
R 12	input	4c8ce175	5b7a2b13	30ead636	040be21d	7b141649	d7eb3262	8dd98b4c
	T	16e2f2ee	38deaccb	a8782924	436c2355	6240f7aa	9a830820	9a9fe1c0
R 13	input	275ef6f4	b93ce75b	33e49197	c4525664	7ab484fd	daf570d9	c98a9698
	T	e5cfbb13	2e1896e4	874cca93	2a9a8178	adc975eb	8d142abe	a519ecf2
R 14	input	ae1a62be	871ff9d0	a9905540	17db9955	fe59ece7	0a8875e2	39ba28fc
	T	7b76e1a6	0bdef4b2	73d5d8a8	28e9a697	4e5f0055	99e4fecb	0b0e33ac
R 15	input	4210873e	b131f170	7fdf4208	f00703de	0b26e200	381fe2bb	8fa6e80b
	T	21822c6c	3e2d93e3	56b4b254	45a4ba0e	7d1f6f46	66c08b4f	39b85307
R 16	input	81cc8d9c	7aaf4a5e	79191406	8f019a43	d1d151c8	09d8ea78	524d2642
	T	3f4d289e	9931e06d	d76034c8	327e693a	d85becd1	d355df7d	d4b38fec
R 17	input	14106a76	0b0f4964	64be5362	8bf49ef7	422d7767	117ad15d	6192bd52
	T	bee15a8c	f42af46c	8b946de1	7b458153	3071bab0	09c9e9b7	f57745bd
output	6e6f20c7	2fabcf43	a72bcbfd	dc0eb9b8	9f3d8945	b7ff0b1f	f6d52cb9	96a7c1b5
output	f16bb878	ddee4f4e	85ef5199	40788524	61aeee1c	b23ce7f0	63fb6498	f38d2e8d

CP _{R,9}									
input		331e03e0	f50e6a17	fa094dbd	c9a3ea7b	76d05e79	58398358	e85f55b7	548889e5
	mask								09090909
R 1	T	9f0498bf	45e8d6a2	22c49a64	333f90aa	fe936759	196075e7	952e4821	73468ecc
	input	f27692f7	d8cdd7d9	ed218a9f	88433920	333b31b0	7d711d96	77d7a9c6	ac1a9b5f
R 2	T	331e03e0	1c558ddc	fa094dbd	d4cb2c64	76d05e79	56689c93	e85f55b7	ce1110e3
	input	4bae05b7	9a7c3d78	3f4e2a37	6eb526fb	d6a68173	956a6d18	bf6d4e4c	669fc245
R 3	T	4cfd1391	890ccb4a	954791b2	8359271b	17ab7dbb	915dd69c	c6c2f87e	6cf5ae74
	input	3b768dbf	2ed1cd75	ff98343f	56b4c718	0a9befb0	09189322	184bc8e3	ceeaba30
R 4	T	c77431dd	cce3c913	56e16e5c	fafb7851	ec89ef8e	956eccdd	c460f857	098cd743
	input	a780dead	d8a053d5	7e1856ae	ddb703a6	b672060d	ccad056f	29cf8a65	c9f0d7a4
R 5	T	fa6887a9	ba1cc848	2e73ce47	f08a65e1	2152da88	6a50d96e	cef5c1c6	7fed7707
	input	8ee744c0	95b450f1	90ccc194	65e7ac7f	d58cf7ee	2a903cc1	ac4bfc8b	de9d2341
R 6	T	5f19f716	d0869c00	d30975ca	f39dd327	082c3255	12f8b099	9cc3fb49	5c5f6b1c
	input	706c6ef1	8f41bade	417b955e	a5a379ee	7e81fbe8	59ee3775	30a07046	e50ad41b
R 7	T	1148a068	dec4c8e5	0744474e	aa87aaf3	563be9b8	6d6cb19e	4ed6f1b3	da3e6183
	input	34aabe5a	4c978af6	89df8972	4ddf6ba2	f9a23197	1e419ad0	dcce3c11	3576ca35
R 8	T	8cad60f2	6336c421	3f99e0fe	6cabdbcb	8e0239fb	f0448915	767df8ca	1ce0180d
	input	891837f5	aa2f72bc	5a79e039	b6e5a779	fee4731e	81bbbef6	8fb6acb9	b6ec8a35
R 9	T	dff7ad2b	02160363	29ab8f8f	c0ef39c9	16be7f3e	4c439e8c	dd7cd389	c66c08cb
	input	e4e749e0	b143ce91	91128ec7	95935687	1e7dbcb2	4b733a64	c67934a9	f53fcf0c
R 10	T	3666d6aa	006f21df	00494bcf	439986b7	8d787d22	f1105ea7	78391c5f	f5df0ce6
	input	f519487b	9fdac124	deedae5a	b02ae54b	261e210b	b87e7c07	dd6caf71	e0b04635
R 11	T	892e0fd0	fcf05e1a	19037894	bedf936e	c2e10b08	4f304fc5	db2325bd	67123c88
	input	a1a28548	6ab36f8c	3effc540	af05e09b	d80e260c	b930437c	631c597e	300d0bdb
R 12	T	f4dc59db	9f0b22de	81dc6080	ce1d4230	7198ae13	21f7aaa1	a979b519	53678a1e
	input	7d6f2ce4	9e8e30f6	77f46349	4b62e555	27a319f3	48fbc4fa	4c5c6eab	d4a577be
R 13	T	16e2f2ee	38deaccb	a8782924	436c2355	6240f7aa	9a830820	9a9fe1c0	8b40c1f3
	input	967f4ab7	2a88f888	a629de59	74a619f5	4b423b4b	d5c83f41	7a1dd9b9	68a02514
R 14	T	e5cfbb13	2e1896e4	874cca93	2a9a8178	adc975eb	8d142abe	a519ecf2	62dbeffb
	input	8702dea8	f2f95cbc	1548519e	ae8b1a42	c19f454a	af8cd37d	38d0697e	e438f5b2
R 15	T	7b76e1a6	0bdef4b2	73d5d8a8	28e9a697	4e5f0055	99e4fecdd	0b0e33ac	1a80206e
	input	d642024c	bda6bf15	5fa28a5f	2f8c52db	6396aeb5	224ee17c	c32b2a10	0f752cd5
R 16	T	21822c6c	3e2d93e3	56b4b254	45a4ba0e	7d1f6f46	66c08b4f	39b85307	44ce6113
	input	326f0bd2	11ffb064	2e251aea	a7d28124	722856d7	03fd9d66	f323d0b5	397045b2
R 17	T	3f4d289e	9931e06d	d76034c8	327e693a	d85becd1	d355df7d	d4b38fec	afc56e4a
	input	485a2ea4	b8136f6a	d389ed44	b33cea80	e636fc39	549afaf8	da4e2e1f	b3e326f4
	T	bee15a8c	f42af46c	8b946de1	7b458153	3071bab0	09c9e9b7	f57745bd	d4f569d1
	output	c8f2f7fe	3a2a3674	7a56c695	39bbc0a7	13b64e88	7e94e777	fc5f5f88	6e3e5510
output		fbecf41e	cf245c63	805f8b28	f0182adc	656610f1	26ad642f	14000a3f	3ab6dcf5

AURORA-256M (M_2 : 2 block message (1/2))

$MS_{L,0}^M$								
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a
R 1	input	71fcd2d3	63646566	fd3ed3df	65666768	ba90476c	6768696a	561f06e2
R 2	input	8586ba97	711f5b2f	e9c3232b	0237f25a	149c60ae	43b99ddd	3cbc4cf4
R 3	input	471793af	44cfef3d	a28cbc8d	ace2e13f	ea18fc8e	a62ff313	de76698f
R 4	input	d38e5264	5ed1883c	b8eb0a31	0a2f27fe	1ba3f637	abab3d26	2e456cad
R 5	input	c2f004c4	a9763137	821a674d	7bb2197f	ae5479e2	2c073736	59fb8fa8
R 6	input	62325d7b	46d09aba	ae97c138	61cc71ff	d7b9915e	068702fe	7113cdf4
R 7	input	792c3ea0	9e1f93f0	7c860e04	3c54c89a	3094ba1a	9e77684a	bfe5312b
R 8	input	5f3d2431	4e5a29e9	1dda1536	e254563e	545f4dc0	0f998f3a	1afb253b
output		1fdeec7d	5184c594	bd1e7a57	5f4a2c69	db557c0f	d4ccf335	d2a4b559
$MS_{R,0}^M$								
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000
R 1	input	8c867c53	6b6c6d6e	dbe5ff85	6d6e6f70	80e87db9	80000000	bf534eae
R 2	input	2eb7d33a	fcfd807a	aa28a97e	c0634644	6094867d	a642312a	74c6cdce
R 3	input	1bfb13f9	9b02c40e	6319eeeb	b61cd0c1	0a466794	45662a75	059c00de
R 4	input	31c899ff	8bc2e8b8	b0b6da18	20acf5b4	26378b15	03a49d59	9a3cf4f2
R 5	input	85f99fec	e3d05753	434d93de	2e834322	92e6cc61	9306a832	14569dfa
R 6	input	edad921e	6eab2deb	9c946dbf	e961e6da	b7e47dc8	2fad1df4	a60b8763
R 7	input	d802cb02	bd676bad	aa233284	9218fdef	38d91675	617f1c35	d2aef77e
R 8	input	8d569831	a6c1307c	1dc218cc	2f83d877	da88bd88	fa803894	9b903922
output		9d7276b6	3bb346ca	862bfa10	a9a82267	213d136b	dbbd2bff	484408aa
$CP_{L,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626364	e27c8fc5	63646566	fb200da6	65666768	ba1fd2df	6768696a
R 1	input	6bb68ffc	63646566	b7d20f84	65666768	d4da1eef	6768696a	c923bd06
	T	696a6b6c	c672bed7	6b6c6d6e	6df42729	6d6e6f70	80537c85	80000000
R 2	input	224d31da	26a9b58c	2ab53aee	2d515298	7b5dc995	8da4593b	ac7cd86b
	T	6e578b8e	0b86c1e9	711f5b2f	d338992f	0237f25a	14bcba2b	43b99ddd
R 3	input	26139bc2	02926d32	f3134fda	3d501a1d	1e168be8	c6d74521	158e45e5
	T	3a0434fa	17144367	fcfd807a	554a669d	c0634644	60c6d37e	a642312a
R 4	input	a89bd1f8	374ddff62	d5ee5224	c5dd2b4b	e2a42c65	f6421f45	72e4673b
	T	70175d72	8f19f91f	44cfef3d	4430d35e	ace2e13f	ea76938d	a62ff313
R 5	input	3cb5ced8	6b2ebf94	dca62e85	5b9d45c5	697c0803	72570bb7	f8dd9205
	T	ff9e0299	8d8cb3ef	9b02c40e	31a3007c	b61cd0c1	0a9c13be	45662a75
R 6	input	2d9c8297	0c1ddc46	8d5db285	f143ae18	0a6e96e6	c8959852	aa114902
	T	b813512a	a7d7ed5b	5ed1883c	7146d8c9	0a2f27fe	1b455231	abab3d26
R 7	input	682eb5e6	4a344eb8	31f0fb78	04ea9b8b	86a8db9a	a106ab20	dab7b28b
	T	0617f3f5	98db45f9	8bc2e8b8	581bfa7f	20acf5b4	263c9918	03a49d59
R 8	input	b62ceb7b	09157b3a	c55125e8	0ffda1d6	2ff5a044	7a16f643	42876b23
	T	15347089	8434f351	a9763137	04a91f89	7bb2197f	aefb044d	2c073736
R 9	input	ad572491	77924b7f	459dcae9	e923df92	79368214	9ebcbabb	b60d084e
	T	a55064cc	42a6e67d	e3d05753	21f34ef6	2e834322	92569fde	9306a832
R 10	input	7fc4df97	e1c0e3b7	cb53d5ac	df3b3aa0	83f44328	759dc514	00b05b2d
	T	79fbc5e4	c52f23e9	46d09aba	5d739af6	61cc71ff	d7135d38	068702fe
R 11	input	f5dc80a3	dd386410	50e4a1da	166364f1	184d5098	d8a0b052	a64df9cc
	T	386918a3	76ca3eb1	6eab2deb	ce72438f	e961e6da	b70b92bf	2fad1df4
R 12	input	27f6670f	f94e5635	f6a36ae0	dd951b78	c16d5590	55ab54a9	f5868f78
	T	62ddd558	f30d7456	9e1f93f0	f9286340	3c54c89a	30e53e04	9e77684a
R 13	input	f2283eeb	61b329f4	1a423be6	2fb5e6e1	73b24d32	7f417ee4	aab42b66
	T	776d4171	6c118b3f	bd676bad	556cfb81	9218fdef	38aecb84	617f1c35
R 14	input	be6df16d	f9fb864b	c3c53246	2a3aeeef	f5fb590c	1c213132	8d6b0432
	T	726c09ec	bfb49a76	4e5a29e9	3abe4a62	e254563e	54fb2436	0f998f3a
R 15	input	3877b2f0	67f61bac	0e2894a2	08e8fcb9	1610addd	faafe6b7	930a744a
	T	8651bd1c	c6e15e91	a6c1307c	a0ec41c98	2f83d877	da9098cc	fa803894
R 16	input	975e47d0	05f955c9	57131fca	2f3e58db	08b7c2ef	8821ae21	115a6c98
	T	1fdeec7d	a3098b28	bd1e7a57	be9458d2	db557c0f	d4ccf335	d2a4b559
R 17	input	4d42efca	82027436	1a2693fc	2e50b7b3	c8881d55	81285360	38f07a7f
	T	9d7276b6	9dd9a365	862bfa10	54d41133	213d136b	dbbd2bff	484408aa
output		58c77094	da6ed171	a0eef702	5c41ab92	1c12bcf3	67bad707	4c7cb398
output		58c77094	da6ed171	a0eef702	5c41ab92	1c12bcf3	67bad707	4c7cb398

$CP_{R,0}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
	mask							00000000
	T	61626364	e27c8fc5	63646566	fb200da6	65666768	ba1fd2df	6768696a
R 1	input	afaa3874	63646566	9c083704	65666768	cbf50170	6768696a	acfd8fd9
	T	696a6b6c	c672bed7	6b6c6d6e	6df42729	6d6e6f70	80537c85	80000000
R 2	input	d9c8fb22	c3e09fc6	d8d6229a	fe524e4b	974cb256	72434510	d4c7b163
	T	6e578b8e	0b86c1e9	711f5b2f	d338992f	0237f25a	14bcba2b	43b99ddd
R 3	input	b5644b8a	7b98aa82	d0cd5a78	ea7bc274	49780324	fc678e8b	873fe503
	T	3a0434fa	17144367	fcfd807a	554a669d	c0634644	60c6d37e	a642312a
R 4	input	a8e5a8d5	5836f945	ab81278c	4ca4e09f	1a8840de	74d162e2	2f3ffe3b
	T	70175d72	8f19f91f	44cfef3d	4430d35e	ace2e13f	ea76938d	a62ff313
R 5	input	a5000cfa	af338d25	70ed055d	24b2a1b1	02e9f188	fb8332da	d0408245
	T	ff9e0299	8d8cb3ef	9b02c40e	31a3007c	b61cd0c1	0a9c13eb	45662a75
R 6	input	73fd8680	b9b4dd70	b5b62e94	f6f85765	1ddfcecd	ae39acbf	5fd49385
	T	b813512a	a7d7ed5b	5ed1883c	7146d8c9	0a2f27fe	1b455231	abab3d26
R 7	input	ea655d30	7d70c83d	8e84e1bf	9d349fbd	ff5faa0d	22b0de94	5a78da69
	T	0617f3f5	98db45f9	8bc2e8b8	581bfa7f	20acf5b4	263c9918	03a49d59
R 8	input	aed48205	5fc03f17	cfaf8d77	30b95ddb	2bb84c61	71b57efb	77fd7ae9
	T	15347089	8434f351	a9763137	04a91f89	7bb2197f	ae6b044d	2c073736
R 9	input	41a21a2d	66b2ad7c	7fb72b93	17d8f90b	48e2c902	bbed8e6f	7eacbafe
	T	a55064cc	42a6e67d	e3d05753	21f34ef6	2e834322	92569fde	9306a832
R 10	input	d437e184	258f8d92	f99574da	18f5a912	e8d7f314	93cdb46e	a2d99d28
	T	79fbc5e4	c52f23e9	46d09aba	5d739af6	61cc71ff	d7135d38	068702fe
R 11	input	929fb0c6	3aad2462	761d1aeb	f77b4784	b996d1e7	8009c1ed	9509b7c6
	T	386918a3	76ca3eb1	6eab2deb	ce72438f	e961e6da	b70b92bf	2fad1df4
R 12	input	fcblfc35	c99016a8	521b8303	eb818cf7	e3fc24f7	639f920e	ec2fa26e
	T	62ddd558	f30d7456	9e1f93f0	f9286340	3c54c89a	30e53e04	9e77684a
R 13	input	5f4d4849	70d034b0	f151788c	27ccfd9c	6079d661	15529fcd	bc3906f1
	T	776d4171	6c118b3f	bd676bad	556cfb81	9218fdef	38aecb84	617f1c35
R 14	input	250c121b	45e63ef4	675b3fc3	db3b029d	35d6b822	830cc928	f06df400
	T	726c09ec	bfb49a76	4e5a29e9	3abe4a62	e254563e	54fb2436	0f998f3a
R 15	input	ae25a614	66cb520b	749463be	b3397496	25532a99	fec42f58	66fa2207
	T	8651bd1c	c6e15e91	a6c1307c	0ec41c98	2f83d877	da9098cc	fa803894
R 16	input	3b74ea9b	b86358cb	367787b1	dbb34dbb	964092f0	6f196aca	8da14ab2
	T	1fdeec7d	a3098b28	bd1e7a57	be9458d2	db557c0f	d4ccf335	d2a4b559
R 17	input	9f66d5da	06b048f1	7f881728	cbcafa7b	a37a074a	9c99a691	298982b6
	T	9d7276b6	9dd9a365	862bfa10	54d41133	213d136b	dbbd2bff	484408aa
output		4f1dee95	490673b7	e8da3b29	f1ef2a71	0243a1ef	645a3fea	d55629fd
output		4f1dee95	490673b7	e8da3b29	f1ef2a71	0243a1ef	645a3fea	d55629fd

AURORA-256M (M_2 : 2 block message (2/2))

$MS_{L,1}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	1395bab4	00000000	995db9b6	00000000	dcf52307	00000000	3e786087
R 2	input	64724673	2f020ca3	d20f01c9	d36967d2	a2e76112	3f2fdc05	218a7c2c
R 3	input	ac452d7d	e0d7b967	d7a5446c	37511e06	0d5ec484	b7d56fa7	4d53aaa4
R 4	input	331ad165	b48ee104	c92ffb22	37643859	374ffd8c	c60ba33a	f6f4fa1d
R 5	input	d0e10cd6	68200582	7ef7e60b	d7b78f25	6f492dbd	26cae83	175ea4d9
R 6	input	7fc92e36	b02c7bad	f4fe6208	59a7de7a	e540fc2c	cbce9cc5	44b5ba2d
R 7	input	27c1afb7	af9ef662	7592e684	38f2c721	f97e3863	28a5d95f	d50afbca
R 8	input	9a5adcc9	8187f3aa	d64a49a0	31371fbd	31240036	b116b03a	0c4af077
output		15314b57	94b6b8fd	adca906b	9cfd8fd6	6b13f0ef	da0540d5	ea2d2ca3
$MS_{R,1}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	e6860c3c	00000000	b78efff4	00000000	ee8511b8	00000000	bf3c20c3
R 2	input	1965be14	3c0b1724	07499ef2	5be32bc8	7b0cecf9	31fa6dc2	8a4635c1
R 3	input	03f34c0a	a5d11471	c67d8dd9	2858d31b	03159cee	b4634e6e	a860bdc
R 4	input	38a99268	c8af06f5	6dd1364d	d37a9afa	241ed6db	b4571deb	f5ef192e
R 5	input	59feb000	92deccf1	c18ddbc4	b726ec8a	bc3ef880	66b56d70	d60069d8
R 6	input	baf60d2a	28dcae77	4304d31c	7890bc3b	d33651d5	1e5b7986	0849ab05
R 7	input	4f5ce121	5838946f	dec9e98f	d851b396	437790ab	dbbf702f	4e1152b6
R 8	input	ab5d889b	7b17fbaf	8afada61	6bf3a4c0	24172bb3	1b16fffb	ab20bc30
output		2abebf6a	51a944c5	9dc1026a	f632a6aa	ae5b0319	b54dfce2	bd3cbf1c
$CP_{L,1}^M$								
input		58c77094	da6ed171	a0eef702	5c41ab92	1c12bcf3	67bad707	4c7cb398
	mask							9384bf80
	T	00000000	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000
R 1	input	755a30a0	a0eef702	237adbea	1c12bcf3	d5510705	4c7cb398	33fedabd
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000
R 2	input	7d75081f	0c3ac88b	a44982ec	3a06ae69	44e0ce21	b738f37f	2e3ea44f
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05
R 3	input	26595eed	77050da9	b941f8e6	89fb1c0f	f73df67c	5cd7d8ca	afdlfbc
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2
R 4	input	f9e22beb	3b07af2a	7b79a09e	f7434c1a	ca7f4afc	fca1e0e1	7b7afa2a
	T	c52332d5	594b8949	e0d7b967	aebd54fb	37511e06	0d532d6c	b7d56fa7
R 5	input	e0b45486	15feff64	deb1989f	bc9070a3	f8a7b00b	08426cec	62a5646a
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e
R 6	input	09b4f248	e145b279	eba0b623	afd5e50d	b9415639	018a4d35	8d2a0dc2
	T	fccf0cc0	665ffa3b	b48ee104	929ff4ca	37643859	37f4d122	c60ba33a
R 7	input	ade5f2cc	7b5da1bc	57271d34	4a9a9514	10d1a4c6	7875b207	b92253e5
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb
R 8	input	a545c2da	22587c82	8dbc0ec7	9193f5c5	9931ded2	5237eb73	1e9f7aee
	T	ed864dc0	a1ee5bb2	68200582	fc9349ad	d7b78f25	6f5e0c0b	26cae83
R 9	input	63a1097a	54ede316	c125c487	80cb71d0	554bd503	a6145ac3	5a6496db
	T	3afd3ea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70
R 10	input	4726eeac	cb11771a	b848d646	29086b80	faaf46ea	be578ff3	c5d8806a
	T	a5c49c88	fffd85b	b02c7bad	e881746c	59a7de7a	e5b52e08	cbce9cc5
R 11	input	58fdf717	cb99c509	f3528835	b250854c	7dd1bf0b	ed9bc8d9	80790644
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986
R 12	input	88efbc56	dff7c857	5d02790b	75647d5a	a979cfff	82946553	ddff6543
	T	ca35b6ae	4f247194	af9ef662	eaafd76e	38f2c721	f90aaf84	28a5d95f
R 13	input	fc38ff2a	429a13ab	b3b9d1eb	2500882d	633eaa73	1e39561d	a2778628
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f
R 14	input	bc8ee670	5523c7c9	ba701e06	082ab53d	879e9ba2	a7deb441	2ded86ef
	T	867d2132	349400ef	8187f3aa	ac49e193	31371fbd	314adca0	b116b03a
R 15	input	f6be30a0	a8382685	bab8975e	78004a23	cbfc2fc3	687b39ec	93cf634d
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16fffb
R 16	input	245dd7c8	da8f794d	ce13814c	7ea17b1c	713038a1	c9c745f8	9dd1ffcb
	T	15314b57	296d71fb	adca906b	39fb1fad	6b13f0ef	da0540d5	ea2d2ca3
R 17	input	04eac15b	f2942223	acb32b99	ba384d0f	a33a9f36	4625277f	a6f1a2f4
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c
output		612b2821	91d5170a	4c03cd6b	90e3d15b	691c773c	342fafb8	af9af860
output		39ec58b5	4bbbc67b	eced3a69	cca27ac9	750ecbfc	539578bf	e3e64bf8
								36e9d1de

CP _{R,1} ^M									
input		4f1dee95	490673b7	e8da3b29	f1ef2a71	0243a1ef	645a3fea	d55629fd	a5375bf4
	mask								01010101
R 1	T	00000000	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000	3e95b907
	input	22f56fcb	e8da3b29	a5c80787	0243a1ef	c9d0baee	d55629fd	60c069a4	4f1dee95
R 2	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000	bf86ffb8
	input	9088dba2	e0e83498	41a61dab	c58f31ec	1d3baed3	987df664	91250668	63da819e
R 3	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05	21720112
	input	927556fe	fc30c914	444eeb70	1da00562	33e6975d	fd84c289	f8b2cf3a	7585b6b9
R 4	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2	8a659ef9
	input	2457c94b	65693084	776cb314	ee19cd05	3936ebe2	fc3c34da	8a611bad	46fc12e5
R 5	T	c52332d5	594b8949	e0d7b967	aebd54fb	37511e06	0d532d6c	b7d56fa7	4d454484
	input	bf623d04	2a2b6abe	19f4e38c	77477780	a5d9bdbb	21b0cb30	c54199aa	5ce6ddfb
R 6	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e	a8f38dee
	input	11fb8f5a	9525611d	a6a81e52	d8acfba1	7ec112ef	b2130022	5a0bf7cd	9a9f8b39
R 7	T	fccf0cc0	665ffa3b	b48ee104	929ff4ca	37643859	37f4d122	c60ba33a	f61afb8c
	input	eb3d4c99	47697a6b	9347f186	f52abead	9a94357b	7d7b8a7a	02bf8111	582f801f
R 8	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb	f5a936db
	input	98294543	03c75bc7	d6ca9bd4	5100aa8d	e451c2f8	61dd6c80	168a27ad	3853ed1d
R 9	T	ed864dc0	a1ee5bb2	68200582	fc9349ad	d7b78f25	6f5e0c0b	26cae833	17e1e6bd
	input	2f87ff29	c843b8bf	891ac2b1	b777904e	95c6e00a	e96e24d3	d6cb3a06	474ba9c5
R 10	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70	d6fedb80
	input	d392ed12	4877f195	0454b797	f21b8f51	e7e263f6	8a1f23aa	624769a7	b0d8913d
R 11	T	a5c49c88	fffd85b5	b02c7bad	e881746c	59a7de7a	e5b52e08	cbce9cc5	44c9622c
	input	266786fe	a0c5ee94	45287a75	f8063a6b	a51e3dd7	5cbfd8a7	e86b5417	fc0f3ccf
R 12	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986	08f6d3d5
	input	6942c4bd	1e07a749	a38c771c	cb8768e0	ea88046d	d6e0aff2	f82cfb61	e86f4423
R 13	T	ca35b6ae	4f247194	af9ef662	eaafd76e	38f2c721	f90aaf84	28a5d95f	d5c1e663
	input	0d3f8da0	489290f2	cb08a134	516d9be3	6e699cea	f1b75525	87aeb7a3	e0312bf5
R 14	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f	4e5ce9ab
	input	c5f8c0c8	0c97fc0b	875d1a6b	5ce77eaf	670e0b17	1668c75f	d3a2fdbe	928cb97e
R 15	T	867d2132	349400ef	8187f3aa	ac49e193	31371fbd	314adca0	b116b03a	0c5a4936
	input	f4141fea	740f6775	b8c16a78	e4857232	5161b818	b83015e2	4bf01a65	8418392d
R 16	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16ffff	ab5ddab3
	input	c8e54b8a	36e67b78	79a2f41a	b374bab0	0260f8ff	0101ff4a	5f52661e	4320e704
R 17	T	15314b57	296d71fb	adca906b	39fb1fad	6b13f0ef	da0540d5	ea2d2ca3	6c500d91
	input	4de07c7b	0db6b018	8b9ea52a	7424f9f9	cc009960	5365406f	22f0206a	2a282f83
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c	f80a6bd0
output		84832785	8b5f8a95	f00ca71e	e2f00fd8	bf47aaae	f734153a	dc2e2f3f	b330d470
output		cb9ec910	c259f922	18d69c37	131f25a9	bd040b41	936e2ad0	097806c2	16078f84

AURORA-256M final mixing (M_2 : 2 block message)

$MS_{R,9}^M$								
input		cb9ec910	c259f922	18d69c37	131f25a9	bd040b41	936e2ad0	097806c2
R 1	input	24812695	18d69c37	a4d77024	bd040b41	7d9ae83d	097806c2	a95205e1
R 2	input	d3d8e648	fc601039	7a008d48	c74a75b0	ee637899	46d9b7b2	36973920
R 3	input	5c54f0b9	ad45c7ba	5231063b	17f5b589	4b28266a	655bcd3c	abee3060
R 4	input	d2fa552c	fd2ee723	67aabd42	facedefa7	dc32c596	b3232b27	6d639eaa
R 5	input	7647c8d0	86cec77c	fc38bbd2	9d01a250	919a70be	bae3cd01	e8532661
R 6	input	fa2b0a22	629833a5	23d7e964	ced61b32	b9556a73	bbb22a4f	b75978e1
R 7	input	511a4ca3	588848e4	681e29ac	531b4d7c	6d81a3cf	9d3a8022	5cb2291b
R 8	input	174ac0fe	77820820	0d3c0cc1	e49c1c6d	edc87785	219287b2	c5cab192
output		e53cb04d	92beb86d	175f7e90	f3c362fd	fd90dab1	dc025d03	d59b4ecd
$CP_{L,9}^M$								
input		39ec58b5	4bbbc67b	eced3a69	cca27ac9	750ecbcf	539578bf	e3e64bf8
	mask							09090909
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	c2aa2593	eced3a69	801504e4	750ecbcf	3d585754	e3e64bf8	a0a9cab8
	T	cb9ec910	926bf470	18d69c37	d24402ca	bd040b41	7d522624	097806c2
R 2	input	e6681caa	7569f2e1	a5c95cf6	31de6382	cef607ef	547984df	bb16e7c6
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 3	input	69a16ae2	4e0a3708	012fad44	678b7e16	8b26fb4e	ae4b6984	b603ecab
	T	b4963b4d	69803c10	fc601039	3d319ca4	c74a75b0	ee97e648	46d9b7b2
R 4	input	02e7d68f	237fda64	f349dba7	811106af	47abf13c	dfee402d	89cc6c31
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 5	input	625a85a9	b65a6b62	45fb0501	08e0329b	553b618f	7cb0915f	91985793
	T	b82bd364	ae189330	ad45c7ba	2914185c	17f5b589	4beef03b	655bcd3c
R 6	input	6e896692	454c5989	b97e03d8	a3b85635	b6b2288e	0f7ae779	5f96b180
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 7	input	1cc91b2d	d99a93ab	df7fc109	b4b63f1e	e06a28d4	08bb3420	056ec778
	T	d34cbe19	695562d5	fd2ee723	33994f16	facedefa7	dc635542	b3232b27
R 8	input	576680df	739525f9	125f9178	3805b20f	91478b37	65fa5089	31ff2b67
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 9	input	f9c1a203	600bd48a	c8d332e2	efa0e261	b58805aa	63a1874f	612baac0
	T	20c9d7cc	3b1c3830	86cec77c	fe4d1368	9d01a250	9153c8d2	bae3cd01
R 10	input	84ed80ec	31b9878e	a767aa93	b7abee15	a6ae1a52	3b28a41e	2dbacf61
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 11	input	51a44c28	bb949662	4585e9aa	a1e9e54c	57d2781e	51ea9989	41adddfef
	T	4a349f0e	7d6bb570	629833a5	91aabc11	ced61b32	b9590a64	bbb22a4f
R 12	input	492daf40	245c6717	cf9d6e5d	e7f09f2d	5b1ed6d0	122c40f7	f64cde6a
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 13	input	5b161b71	0c5bbc8b	2ad5de36	2a9c21f1	3d08c556	3b4389d5	b7abca6c
	T	f263ea5a	a88f518d	588848e4	b44094d1	531b4d7c	6db24cac	9d3a8022
R 14	input	63194103	5984642c	62214019	ce039e23	c16eae2f	ea54d593	e5df6d5a
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 15	input	e0854a3e	eab0ab3c	132e7366	341a92d4	ca1b0ae8	cb6c81ff	4f22d729
	T	f94054e5	0b9e3bc9	77820820	06e458ff	e49c1c6d	edcac0c1	219287b2
R 16	input	f90ef312	ce15aa5d	d9a302a6	e41917e8	0eca10b4	92d7c7c6	32fb8153
	T	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 17	input	32ed5923	05d42169	55b3e13f	f342e7ad	00f3b0ae	2b7acf84	b88d42b1
	T	e53cb04d	c95f5c3b	175f7e90	f9e1b17e	fd90dab1	dc025d03	d59b4ecd
output		05df0b6c	2c68c67e	32eff08f	2f13d8cc	64ed7867	6e053051	b57294b8
output		3c3353d9	67d30005	de02cae6	e3b1a205	11e3b3a8	3d9048ee	5694df40

AURORA-224M (M_2 : 2 block message (1/2))

$MS_{L,0}^M$								
input		61626364	62636465	63646566	64656667	65666768	66676869	6768696a
R 1	input	71fcd2d3	63646566	fd3ed3df	65666768	ba90476c	6768696a	561f06e2
R 2	input	8586ba97	711f5b2f	e9c3232b	0237f25a	149c60ae	43b99ddd	3cbc4cf4
R 3	input	471793af	44cfef3d	a28cbc8d	ace2e13f	ea18fc8e	a62ff313	de76698f
R 4	input	d38e5264	5ed1883c	b8eb0a31	0a2f27fe	1ba3f637	abab3d26	2e456cad
R 5	input	c2f004c4	a9763137	821a674d	7bb2197f	ae5479e2	2c073736	59fb8fa8
R 6	input	62325d7b	46d09aba	ae97c138	61cc71ff	d7b9915e	068702fe	7113cdf4
R 7	input	792c3ea0	9e1f93f0	7c860e04	3c54c89a	3094ba1a	9e77684a	bfe5312b
R 8	input	5f3d2431	4e5a29e9	1dda1536	e254563e	545f4dc0	0f998f3a	1afb253b
output		1fdeec7d	5184c594	bd1e7a57	5f4a2c69	db557c0f	d4ccf335	d2a4b559
$MS_{R,0}^M$								
input		696a6b6c	6a6b6c6d	6b6c6d6e	6c6d6e6f	6d6e6f70	6e6f7071	80000000
R 1	input	8c867c53	6b6c6d6e	dbe5ff85	6d6e6f70	80e87db9	80000000	bf534eae
R 2	input	2eb7d33a	fcfd807a	aa28a97e	c0634644	6094867d	a642312a	74c6cdce
R 3	input	1bfb13f9	9b02c40e	6319eeeb	b61cd0c1	0a466794	45662a75	059c00de
R 4	input	31c899ff	8bc2e8b8	b0b6da18	20acf5b4	26378b15	03a49d59	9a3cf4f2
R 5	input	85f99fec	e3d05753	434d93de	2e834322	92e6cc61	9306a832	14569dfa
R 6	input	edad921e	6eab2deb	9c946dbf	e961e6da	b7e47dc8	2fad1df4	a60b8763
R 7	input	d802cb02	bd676bad	aa233284	9218fdef	38d91675	617f1c35	d2aef77e
R 8	input	8d569831	a6c1307c	1dc218cc	2f83d877	da88bd88	fa803894	9b903922
output		9d7276b6	3bb346ca	862bfa10	a9a82267	213d136b	dbbd2bff	484408aa
$CP_{L,0}^M$								
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask							00000000
	T	61626364	e27c8fc5	63646566	fb200da6	65666768	ba1fd2df	6768696a
R 1	input	94497003	9c9b9a99	482df07b	9a999897	2b25e110	98979695	36dc42f9
	T	696a6b6c	c672bed7	6b6c6d6e	6df42729	6d6e6f70	80537c85	80000000
R 2	input	ece67b9d	7cbdd434	8f90399b	d3f1e712	7ab6a633	b6f0a562	6823467f
	T	6e578b8e	0b86c1e9	711f5b2f	d338992f	0237f25a	14bcba2b	43b99ddd
R 3	input	406383d0	102731aa	1f6f056b	2a46fef5	3203a0c8	f17d9fea	13ccac66
	T	3a0434fa	17144367	fcfd807a	554a669d	c0634644	60c6d37e	a642312a
R 4	input	b9afc1aa	6dd293d8	989f9e35	896ae191	992d438d	af1e9996	17f9cf09
	T	70175d72	8f19f91f	44cfef3d	4430d35e	ace2e13f	ea76938d	a62ff313
R 5	input	71035bb6	5b879b20	a0f78276	c3ee47e5	a8627ee2	e62594fc	6ff27cc3
	T	ff9e0299	8d8cb3ef	9b02c40e	31a3007c	b61cd0c1	0a9c13eb	45662a75
R 6	input	ded4ade2	1a6d3213	03e666a6	68bb1e70	076d748c	86137644	f39bb44f
	T	b813512a	a7d7ed5b	5ed1883c	7146d8c9	0a2f27fe	1b455231	abab3d26
R 7	input	f6098f92	2c089aa4	ce3f1d7c	1b434f99	d76ca9b2	5a338bf1	e298d686
	T	0617f3f5	98db45f9	8bc2e8b8	581bfa7f	20acf5b4	263c9918	03a49d59
R 8	input	648acbd8	ac84ae8f	7f027a17	257ba1f8	fecdbf95	ed0f35ca	5d346ac8
	T	15347089	8434f351	a9763137	04a91f89	7bb2197f	aefb044d	2c073736
R 9	input	7c246d2e	335245ee	2bb7cbd2	1cdc5520	1b705b0e	0da07056	91eb06b7
	T	a55064cc	42a6e67d	e3d05753	21f34ef6	2e834322	92569fde	9306a832
R 10	input	cd379293	63fd2301	bc6072ac	8fe7bd4d	40364aba	d6d56eca	d77011e9
	T	79fbc5e4	c52f23e9	46d09aba	5d739af6	61cc71ff	d7135d38	068702fe
R 11	input	db10c74e	072d7710	da7aa290	b2df8865	1f84e801	a09fb49e	28b96d02
	T	386918a3	76ca3eb1	6eab2deb	ce72438f	e961e6da	b70b92bf	2fad1df4
R 12	input	6bf12b09	ac3702a7	07fd4168	e3a4533c	87a8d71a	130f075b	1f883719
	T	62ddd558	f30d7456	9e1f93f0	f9286340	3c54c89a	30e53e04	9e77684a
R 13	input	1da13bcf	86055a94	c3fadc45	4029b0b0	5a356451	068308e6	458c10da
	T	776d4171	6c118b3f	bd676bad	556cfb81	9218fdef	38aecb84	617f1c35
R 14	input	c6bc53b7	20a5a8c0	75a4c175	65bf3ac7	c3395ba5	4631bfb5	6dbc7c49
	T	726c09ec	bfb49a76	4e5a29e9	3abe4a62	e254563e	54fb2436	0f998f3a
R 15	input	08ed36f2	3f597f9f	19eda142	e50df6de	01aa9c67	16e2a216	e0ffc428
	T	8651bd1c	c6e15e91	a6c1307c	0ec41c98	2f83d877	da9098cc	fa803894
R 16	input	a574ba73	343d280d	2beeb8c7	b3c3e177	7896d5ae	56901689	26ea1bc2
	T	1fdeec7d	a3098b28	bd1e7a57	be9458d2	db557c0f	d4ccf335	d2a4b559
R 17	input	193cc931	8da04461	895fee35	511929d2	69d71cf6	6a045daa	b908f359
	T	9d7276b6	9dd9a365	862bfa10	54d41133	213d136b	dbbd2bff	484408aa
output		58dcba88	d5d72b3a	e81aa7cb	6bfc653a	fbb2cd9d	6b36a8a3	7b2c9211
output		a7234577	2a28d4c5	17e55834	94039ac5	044d3262	94c9575c	84d36dee

$CP_{R,0}^M$									
input		ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff	ffffff
	mask								00000000
	T	61626364	e27c8fc5	63646566	fb200da6	65666768	ba1fd2df	6768696a	56fcd36c
R 1	input	5055c78b	9c9b9a99	63f7c8fb	9a999897	340afe8f	98979695	53027026	9e9d9c9b
	T	696a6b6c	c672bed7	6b6c6d6e	6df42729	6d6e6f70	80537c85	80000000	bf86ffb9
R 2	input	fd6cda1a	b8d79601	5c8959e2	fa7390cc	6c844728	2118c191	78194770	a6eb146c
	T	6e578b8e	0b86c1e9	711f5b2f	d338992f	0237f25a	14bcba2b	43b99ddd	3c8623ae
R 3	input	dd07b20d	b9824082	16b9822a	73aebfa7	83436312	95a45c51	35b1d1da	237d87ce
	T	3a0434fa	17144367	fcfd807a	554a669d	c0634644	60c6d37e	a642312a	74b7a97d
R 4	input	0f153957	7c3b7014	16f4455c	1655a395	29504065	41626947	090d0a55	6f6b82ed
	T	70175d72	8f19f91f	44cfef3d	4430d35e	ace2e13f	ea76938d	a62ff313	de17bc8e
R 5	input	65e6a38e	20d02b5b	a50cc616	2520055f	36fb2421	e40a1b1d	aa616770	fc2a1b40
	T	ff9e0299	8d8cb3ef	9b02c40e	31a3007c	b61cd0c1	0a9c13eb	45662a75	05fbee94
R 6	input	fb06352e	fd7aab30	f037e2d4	8176cde2	7583aa04	eb2e3c12	fed34181	2e5b637d
	T	b813512a	a7d7ed5b	5ed1883c	7146d8c9	0a2f27fe	1b455231	abab3d26	2e8e0a37
R 7	input	7f66d417	5b43f19d	df335e8b	ecde8624	cbe25981	f1d1a362	8e8c790c	21506ca5
	T	0617f3f5	98db45f9	8bc2e8b8	581bfa7f	20acf5b4	263c9918	03a49d59	9ac8da15
R 8	input	6c24b948	65b807c3	848cef3c	387e1b66	f023fb11	ee3c99ae	395b5b43	63387c48
	T	15347089	8434f351	a9763137	04a91f89	7bb2197f	aefb044d	2c073736	59f067e2
R 9	input	e754657d	31edc291	207f06b1	ac6e617c	6c7a3911	4d0b2d76	6c939313	3439b97e
	T	a55064cc	42a6e67d	e3d05753	21f34ef6	2e834322	92569fde	9306a832	14f99361
R 10	input	4baeff51	a423fd30	c3567399	9d4e1448	9bcd7432	4ee47b77	e3847533	20b93cf9
	T	79fbc5e4	c52f23e9	46d09aba	5d739af6	61cc71ff	d7135d38	068702fe	7132c15e
R 11	input	76dd1090	302c806e	f95133f2	57f02884	c4ac3be9	b2d70015	6fabaeef	a6cfb452
	T	386918a3	76ca3eb1	6eab2deb	ce72438f	e961e6da	b70b92bf	2fad1df4	a6ad6dc8
R 12	input	99a39d9b	1af1c706	213938f4	1bbb2cf8	2116c772	d36db31e	39cb1cd3	8565489c
	T	62ddd558	f30d7456	9e1f93f0	f9286340	3c54c89a	30e53e04	9e77684a	bf2c0e1a
R 13	input	ad784804	31332bf2	401a7215	69b9dc15	9ea01a57	aec4d24a	68beb960	5014ab4d
	T	776d4171	6c118b3f	bd676bad	556cfb81	9218fdef	38aecb84	617f1c35	d2023275
R 14	input	f07bcd02	fc156c64	9057b5d3	28d1900a	7d506fc9	33515efc	61118755	c44f20a5
	T	726c09ec	bfb49a76	4e5a29e9	3abe4a62	e254563e	54fb2436	0f998f3a	1a3d15c0
R 15	input	9de120ad	a128ca25	40fb5137	cc3765cb	ea5aa021	a3efd5f7	afa9285f	6291033f
	T	8651bd1c	c6e15e91	a6c1307c	0ec41c98	2f83d877	da9098cc	fa803894	9b561888
R 16	input	86e72448	e3ada545	120e8b64	3e9d79c1	2e802209	bf16befb	d7a4a6b8	08d0b22b
	T	1fdeec7d	a3098b28	bd1e7a57	be9458d2	db557c0f	d4ccf335	d2a4b559	a0c8bcb5
R 17	input	8160095a	ef11dc0b	7398c456	0071f234	b8f5e770	7d055d8f	b23d22bb	b3eed296
	T	9d7276b6	9dd9a365	862bfa10	54d41133	213d136b	dbbd2bff	484408aa	ce15b5b6
output		436cddc7	acd6d41f	0f5cbcb6	ddd2a5a1	8416b750	0393d24b	311919d0	04a6765a
output		bc932238	53292be0	f0a34349	222d5a5e	7be948af	fc6c2db4	cee6e62f	fb5989a5

AURORA-224M (M_2 : 2 block message (2/2))

$MS_{L,1}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	1395bab4	00000000	995db9b6	00000000	dcf52307	00000000	3e786087
R 2	input	64724673	2f020ca3	d20f01c9	d36967d2	a2e76112	3f2fdc05	218a7c2c
R 3	input	ac452d7d	e0d7b967	d7a5446c	37511e06	0d5ec484	b7d56fa7	4d53aaa4
R 4	input	331ad165	b48ee104	c92ffb22	37643859	374ffd8c	c60ba33a	f6f4fa1d
R 5	input	d0e10cd6	68200582	7ef7e60b	d7b78f25	6f492dbd	26cae83	175ea4d9
R 6	input	7fc92e36	b02c7bad	f4fe6208	59a7de7a	e540fc2c	cbce9cc5	44b5ba2d
R 7	input	27c1afb7	af9ef662	7592e684	38f2c721	f97e3863	28a5d95f	d50afbca
R 8	input	9a5adcc9	8187f3aa	d64a49a0	31371fbd	31240036	b116b03a	0c4af077
output		15314b57	94b6b8fd	adca906b	9cfd8fd6	6b13f0ef	da0540d5	ea2d2ca3
$MS_{R,1}^M$								
input		00000000	00000000	00000000	00000000	00000000	00000000	00000001
R 1	input	e6860c3c	00000000	b78efff4	00000000	ee8511b8	00000000	bf3c20c3
R 2	input	1965be14	3c0b1724	07499ef2	5be32bc8	7b0cecf9	31fa6dc2	8a4635c1
R 3	input	03f34c0a	a5d11471	c67d8dd9	2858d31b	03159cee	b4634e6e	a860bdfc
R 4	input	38a99268	c8af06f5	6dd1364d	d37a9afa	241ed6db	b4571deb	f5ef192e
R 5	input	59feb000	92deccf1	c18ddbc4	b726ec8a	bc3ef880	66b56d70	d60069d8
R 6	input	baf60d2a	28dcae77	4304d31c	7890bc3b	d33651d5	1e5b7986	0849ab05
R 7	input	4f5ce121	5838946f	dec9e98f	d851b396	437790ab	dbbf702f	4e1152b6
R 8	input	ab5d889b	7b17fbaf	8afada61	6bf3a4c0	24172bb3	1b16fffb	ab20bc30
output		2abebf6a	51a944c5	9dc1026a	f632a6aa	ae5b0319	b54dfce2	bd3cbf1c
$CP_{L,1}^M$								
input		a7234577	2a28d4c5	17e55834	94039ac5	044d3262	94c9575c	84d36dee
	mask							01010101
	T	00000000	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000
R 1	input	8548b0f7	17e55834	eb3c79b1	044d3262	26130291	84d36dee	9e8deb09
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000
R 2	input	6bd47068	0053986d	b0da23cf	2299083c	94d61e63	cf7d67de	a90e7a2a
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05
R 3	input	4d3b4428	d561ad39	039128b1	6b0e92f9	6dc6c218	c82d77f3	9a61e915
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2
R 4	input	d1ae1f3e	f3867a09	513628af	9127d712	380be6d3	b5540c81	55e4a1ed
	T	c52332d5	594b8949	e0d7b967	aebd54fb	37511e06	0d532d6c	b7d56fa7
R 5	input	6726e7c2	b4ce1328	1915f7e9	c3292fb5	cef31b22	00fb0f92	e0e91353
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e
R 6	input	5306d1bd	9bcc869a	eec46528	a576a578	bb715c16	401de00e	833066d0
	T	fccf0cc0	665ffa3b	b48ee104	929ff4ca	37643859	37f4d122	c60ba33a
R 7	input	f361c1a0	7f01f9a5	59790927	66be0b3c	7d2e2e62	0ba540fd	31c44b60
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb
R 8	input	e2bfd382	326f7df2	b13974e6	731e161e	0877720f	191a2fc8	71c2e53a
	T	ed864dc0	a1ee5bb2	68200582	fc9349ad	d7b78f25	6f5e0c0b	26cae83
R 9	input	95ae778f	b9870438	ceaeef37	c8b9cbdb	56aca9c8	b3c299c5	0c3b9299
	T	3afd3ea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70
R 10	input	bc3fec3e	874ce583	bcafaa9a	5685aa5a	908088f8	69f28ed3	f483a876
	T	a5c49c88	fffd85b	b02c7bad	e881746c	59a7de7a	e5b52e08	cbce9cc5
R 11	input	3f695c82	623cb746	25e25390	bf312fc9	a7f9e41c	9f823afc	e4bdb54c
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986
R 12	input	6bed14ba	4ee28b3e	c14c76c2	b4ac27b6	1a0d9d7d	9d7ba340	e92e8cd6
	T	ca35b6ae	4f247194	af9ef662	eaafd76e	38f2c721	f90aaf84	28a5d95f
R 13	input	895187cb	d60097a6	e6e64476	edc736a3	b46c7f4d	a4bbe3f9	525f58d2
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f
R 14	input	67f1ff50	22cef167	05be24be	86c01961	b3b4e251	18eb1821	760d0ef2
	T	867d2132	349400ef	8187f3aa	ac49e193	31371fbd	314adca0	b116b03a
R 15	input	7d6d41d5	b166f1ac	2d277bc9	c11697d4	cdc0f307	c6fc2838	72ec18be
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16fffb
R 16	input	074fc7b5	799bbdc7	d4fbcc5d	bcfb77ad9	1d32f836	1ea7e232	b640e67d
	T	15314b57	296d71fb	adca906b	39fb1fad	6b13f0ef	da0540d5	ea2d2ca3
R 17	input	1d9d6be3	a172ff5e	3d3164cb	173f4097	d9ca99ea	80e47f3c	5a967eb1
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c
output		ffeb97e1	5cf375b7	34003cb9	45e72d11	f476121c	6f8492db	d7b39305
output		58c8d296	76dba172	23e5648d	d1e4b7d4	f03b207e	fb4dc587	5360feeb
								5944dae0

$CP_{R,1}^M$									
input		bc932238	53292be0	f0a34349	222d5a5e	7be948af	fc6c2db4	cee6e62f	fb5989a5
	mask	01010101							
	T	00000000	26ba470f	00000000	33eac168	00000000	dc78bab6	00000000	3e95b907
R 1	input	389b7de4	f0a34349	76e7d5d9	7be948af	5112e2bf	cee6e62f	3ef619f3	bc932238
	T	00000000	734708e1	00000000	dbc2901e	00000000	ee3c0cf4	00000000	bf86ffb8
R 2	input	94bad2a8	ef1cc1d2	37af4c47	eb2cf7d2	28654949	44c16b53	be361ac4	7faa1e52
	T	ecffef30	c81ec259	2f020ca3	a5cef8e6	d36967d2	a28a46c9	3f2fdc05	21720112
R 3	input	e18d5767	a8071bb3	3eb96b85	Odd199a0	ff725e8b	7f0cd93	667fdb5c	09868a95
	T	6609339b	0ca4f660	3c0b1724	83861a8a	5be32bc8	7b46bef2	31fa6dc2	8a659ef9
R 4	input	e7b0b82f	577cc322	551079ea	b981a3e1	ec529e55	65573241	6f7174b9	d1b7b556
	T	c52332d5	594b8949	e0d7b967	aebd54fb	37511e06	0d532d6c	b7d56fa7	4d454484
R 5	input	0acd1538	57810966	3384a755	3ab7a9c2	71eb7d32	4154280a	325594fe	db83ee09
	T	270c6ee5	01bece7e	a5d11471	630ade85	2858d31b	03604cd9	b4634e6e	a8f38dee
R 6	input	a0cf239d	70620298	0e08f03d	d956b4f4	1f7604d0	de42ddef	b1154a08	5695fe24
	T	fccf0cc0	665ffa3b	b48ee104	929ff4ca	37643859	37f4d122	c60ba33a	f61afb8c
R 7	input	a1bd0ff6	1c40cb51	c93b4b02	e12620e4	e247e13f	42f14523	f1e27f3b	f71437b0
	T	31a37e56	1c68eb17	c8af06f5	368f0cb4	d37a9afa	24ef924d	b4571deb	f5a936db
R 8	input	a7684d9a	bc64e157	7df293bd	bc16dbd	36fec539	efa7d3ee	37b10394	5c425b1e
	T	ed864dc0	a1ee5bb2	68200582	fc9349ad	d7b78f25	6f5e0c0b	26caeb83	17e1ebd
R 9	input	9d7a6a01	75d9b0a7	d92bccb4	1fe6ba25	b3ed33ac	69829c76	3220f576	4ad9c025
	T	3afdbea3	2cc6fc6c	92deccf1	609f3480	b726ec8a	bc00b0c4	66b56d70	d6fedb80
R 10	input	7fb2ab33	c09e58df	2431bbc3	ad5271a0	389a2e9a	48ad4626	ade2eada	a127d458
	T	a5c49c88	ffdfdf85b	b02c7bad	e881746c	59a7de7a	e5b52e08	cbce9cc5	44c9622c
R 11	input	dd3150dc	79a43447	c37a393f	150689ad	8a36b7cf	5c16deda	f9d9703d	8fb41faf
	T	1ef7af67	5d022882	28dcae77	a19b5595	7890bc3b	d3490d1c	1e5b7986	08f6d3d5
R 12	input	b6e3be61	dfd30d53	8fbcba08	fbdd1489	da5c94f2	a3fa410d	fedfe297	ee3e0e06
	T	ca35b6ae	4f247194	af9ef662	eaafd76e	38f2c721	f90aaf84	28a5d95f	d5c1e663
R 13	input	fd7e7626	9128181d	228c2578	ab3d8e50	e189c0bd	92a79b57	e2e443b4	d161ddf8
	T	a6f04425	a7e4c85b	5838946f	6f3ba910	d851b396	4311e18f	dbbf702f	4e5ce9ab
R 14	input	3c1c87ab	246323db	55dd153e	8dfff788	d5aa1c3d	89dc3e78	7daa3788	b2b626a7
	T	867d2132	349400ef	8187f3aa	ac49e193	31371fbd	314adca0	b116b03a	0c5a4936
R 15	input	b47b39c6	2b91e87e	3689891f	7f83ad72	55e78086	5d6569a5	8e421c59	eca4dec1
	T	4536d4cc	d5fd1598	7b17fbaf	450bde4d	6bf3a4c0	24208861	1b16ffffb	ab5ddab3
R 16	input	c886e6d7	1a518965	cee34e9a	45676b77	11d1cc30	32dea269	04144b72	1cff5c63
	T	15314b57	296d71fb	adca906b	39fb1fad	6b13f0ef	da0540d5	ea2d2ca3	6c500d91
R 17	input	944713e3	3d2cba47	4dec3d4f	47b1cbbf	cc895922	c01d634a	eebafb95	dfed1d61
	T	2abebf6a	28d4a262	9dc1026a	fb195355	ae5b0319	b54dfce2	bd3cbf1c	f80a6bd0
output		1a2e32b7	256895f8	eb2c0452	ca459ed2	df772805	047cb4b4	26bb0baf	bc60c202
output		a6bd108f	7641be18	1b8f471b	e868c48c	a49e60aa	f8109900	e85ded80	47394ba7

AURORA-224M final mixing (M_2 : 2 block message)

$MS_{R,9}^M$								
input	a6bd108f	7641be18	1b8f471b	e868c48c	a49e60aa	f8109900	e85ded80	47394ba7
R 1	input	90bf95b0	1b8f471b	5fcfb4f4	a49e60aa	16edaf1e	e85ded80	f82ce4db
R 2	input	46f8fc7b	6d2cd2e1	f2dba966	4ff384dc	87b50b74	52da4ac0	4f0b9045
R 3	input	e6262db5	7b9544da	0c587a3b	0d0595fb	45415368	a3ab1977	fb1d424f
R 4	input	ba98324e	b581cc33	352208a4	6eea6d0a	8e6d2e98	626429de	97b795a1
R 5	input	8359927e	34c39a7f	da183f6d	2e8efa16	f3b351aa	b5a5217e	599bc879
R 6	input	273bb31d	2e41e4dc	dc449d1	49bf4ef8	3103f15b	4f2d806f	fe76f7aa
R 7	input	3a80a41f	94013c92	235626b8	efba0f48	256112ad	77ce4908	d98c0892
R 8	input	2eae13fc	c157f216	07286e35	d35106b3	2ebc5fe1	09e78326	caf3096e
output	2eca07ec	ef9df5fa	1e756a66	d3246cd5	f5b1560d	fc56d52b	dd0849af	d1d541c0
$CP_{L,9}^M$								
input	58c8d296	76dba172	23e5648d	d1e4b7d4	f03b207e	fb4dc587	5360feeb	5944dae0
mask								09090909
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 1	input	ff07988e	23e5648d	9d750fdc	f03b207e	951e306a	5360feeb	cf7107b1
T	a6bd108f	4867d7ed	1b8f471b	afff6f258	a49e60aa	162c95f4	e85ded80	f8fbfb41e
R 2	input	cbbc0a8a	0a60e3ce	218a629d	acef18c1	9128a97a	a4921f08	9a453645
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 3	input	f035ca00	71fe0da9	a3b4b131	8dde45b4	91e34717	7abb7fb8	37bdade7
T	22149304	a36d85a2	6d2cd2e1	f95ac83d	4ff384dc	870bfc66	52da4ac0	4ff8a974
R 4	input	01a3a77d	62df9275	0d326299	10428aef	e3799ad8	591b8d35	844a8904
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 5	input	0dee38ec	cbb2e667	a9e12806	2c764284	f780bf27	25e4fc98	a8fb56aa
T	930e6493	f32c29a7	7b9544da	8620a15a	0d0595fb	451d2d3b	a3ab1977	fb267a68
R 6	input	2700e995	c1fcf5f7	60c0b26c	51cf4934	09703851	afcb68c7	47b65732
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 7	input	98d5825a	f62fc4dd	022be9d1	4ddc2978	b9a839ed	f9e08cce	b6b58fa9
T	6d14d672	5d111750	b581cc33	9ab6caa7	6eea6d0a	8eb732a4	626429de	97980898
R 8	input	3cb8b0df	df15ae3e	a6133173	b444eea1	2a2d70dc	5de5fa3a	2215180f
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 9	input	fd3ad883	b3932da4	978cd8ca	945832fa	f6519787	49bf4c92	85cc0f32
T	9d46ddc4	418c28bc	34c39a7f	ed59e43f	2e8efa16	f39b926d	b5a5217e	59593faa
R 10	input	f49e4b3f	4b059492	07948a67	ddf07cc5	37f32444	62dcf556	62b8a62a
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 11	input	7cc611b0	64913e2a	f00faab1	0363e91f	ac8c5984	3dfc07f2	49d3e56e
T	255a5946	93da78d5	2e41e4dc	6e01fb8e	49bf4ef8	3176b3d1	4f2d806f	fe3b495b
R 12	input	e137b413	60a18af1	9af07706	03b6f672	dc1b557e	3d8f61cc	335aaf62
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 13	input	424b90ea	d5dc8a4f	171c75d1	087d8b2d	30c956ee	7fa902c0	05e9958e
T	d5f28caa	9d2b0949	94013c92	11b0840f	efba0f48	258ca4b8	77ce4908	d98026ad
R 14	input	b73965e4	b2597abf	c22489b1	21d19bbe	9e2b3bb2	982ea442	a578bd0e
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 15	input	037cf005	1b5e3e9a	0deac6fb	2c885998	a027b29a	6e22a929	f5ca4762
T	0cdd086f	17142fb7	c157f216	03de04fe	cd5106b3	2ef31335	09e78326	caae6ee1
R 16	input	66fbaf1b	2c63ca2f	906fdda5	635baa17	c6c15e10	69aad84a	e6038c0f
T	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
R 17	input	5b4178d6	c1844663	165626a1	cb67d9bf	c3e183a0	22e39b84	36d5989a
T	2eca07ec	f7cefafe	1e756a66	6992366a	f5b1560d	fc56d52b	dd0849af	d1d541c0
output	00b0ab46	18301034	f962d253	45e257e0	2be4049b	00e01c39	d8a023f9	0ee9fcc4
output	587879d0	6eebb146	da87b6de	9406e034	dbdf24e5	fbadd9be	8bc0dd12	57ad2624