HIGHT Algorithm
Test Vectors

2009.07

1. Test vectors 1

Key : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Plaintext : 00 00 00 00 00 00 00 00
Ciphertext : 00 f4 18 ae d9 4f 03 f2

Sub Key	Value	Sub Key	Value
$SK_3 \| SK_2 \| SK_1 \| SK_0$	e7135b59	$SK_{67} \| SK_{66} \| SK_{65} \| SK_{64}$	cfa7c7f6
$SK_7 \| SK_6 \| SK_5 \| SK_4$	c99cb0c8	$SK_{71} \| SK_{70} \| SK_{69} \| SK_{68}$	48555f62
$SK_{11} \| SK_{10} \| SK_9 \| SK_8$	906d96d7	$SK_{75} \| SK_{74} \| SK_{73} \| SK_{72}$	1f50a1b1
$SK_{15} \| SK_{14} \| SK_{13} \| SK_{12}$	2c6a5599	$SK_{79} \| SK_{78} \| SK_{77} \| SK_{76}$	a5986d86
$SK_{19} \| SK_{18} \| SK_{17} \| SK_{16}$	27032ade	$SK_{83} \| SK_{82} \| SK_{81} \| SK_{80}$	0706f33c
$SK_{23} \| SK_{22} \| SK_{21} \| SK_{20}$	b5e32d31	$SK_{87} \| SK_{86} \| SK_{85} \| SK_{84}$	fb2b7aff
$SK_{27} \| SK_{26} \| SK_{25} \| SK_{24}$	ced9de4e	$SK_{91} \| SK_{90} \| SK_{89} \| SK_{88}$	7a755a93
$SK_{31} \| SK_{30} \| SK_{29} \| SK_{28}$	48919180	$SK_{95} \| SK_{94} \| SK_{93} \| SK_{92}$	7bb39134
$SK_{35} \| SK_{34} \| SK_{33} \| SK_{32}$	f915b5f4	$SK_{99} \| SK_{98} \| SK_{97} \| SK_{96}$	bcdf15f0
$SK_{39} \| SK_{38} \| SK_{37} \| SK_{36}$	fadc0ee2	$SK_{103} \| SK_{102} \| SK_{101} \| SK_{100}$	ef018ca2
$SK_{43} \| SK_{42} \| SK_{41} \| SK_{40}$	bba15439	$SK_{107} \| SK_{106} \| SK_{105} \| SK_{104}$	2a436495
$SK_{47} \| SK_{46} \| SK_{45} \| SK_{44}$	9fadb9bf	$SK_{111} \| SK_{110} \| SK_{109} \| SK_{108}$	ae882255
$SK_{51} \| SK_{50} \| SK_{49} \| SK_{48}$	16b7f8e8	$SK_{115} \| SK_{114} \| SK_{113} \| SK_{112}$	c7e50f52
$SK_{55} \| SK_{54} \| SK_{53} \| SK_{52}$	e41e0239	$SK_{119} \| SK_{118} \| SK_{117} \| SK_{116}$	67d9bcf0
$SK_{59} \| SK_{58} \| SK_{57} \| SK_{56}$	d9451b36	$SK_{123} \| SK_{122} \| SK_{121} \| SK_{120}$	61a18fda
$SK_{63} \| SK_{62} \| SK_{61} \| SK_{60}$	a9b0ad97	$SK_{127} \| SK_{126} \| SK_{125} \| SK_{124}$	d1357c79

Round	Value	Round	Value
Initial	0000001100220033	Round 17	2c93a90ddd0283ae
Round 1	00ce1138223f33e7	Round 18	93570db102d9aec4
Round 2	cee138ef3fa3e78a	Round 19	57b7b1dbd998c4e4
Round 3	e14fef91a3708a8a	Round 20	b7bedb55989ae458
Round 4	4f8a91cd70518ad1	Round 21	be87559d9a515868
Round 5	8a53cd0951c3d1ee	Round 22	87ce9d5351786873
Round 6	534609c7c3e4ee7d	Round 23	ceab53d6784b73bc
Round 7	4673c7c5e41b7dd7	Round 24	ab30d6d74ba8bc69
Round 8	7359c58c1b33d79c	Round 25	30bfd7f7a83369df
Round 9	595f8cf333d59c07	Round 26	bf13f71733bfdf7d
Round 10	5f0cf317d507073f	Round 27	134617f1bfd57db2
Round 11	0ca0173007033fb6	Round 28	467bf187d5c4b277
Round 12	a03a3043030bb63e	Round 29	7b3187d2c4f5772b
Round 13	3a7943b40b2b3e37	Round 30	315dd246f5482bde
Round 14	7920b47a2b7c37b5	Round 31	5d3846d148a1def3
Round 15	20637a797ce4b5d0	Round 32	003818d1d9a103f3
Round 16	632c79a9e4ddd083	Final	00f418aed94f03f2

2. Test vectors 2

Key : ff ee dd cc bb aa 99 88 77 66 55 44 33 22 11 00
Plaintext : 00 11 22 33 44 55 66 77
Ciphertext : 23 ce 9f 72 e5 43 e6 d8

Sub Key	Value	Sub Key	Value
$SK_3 \| SK_2 \| SK_1 \| SK_0$	4e587e5a	$SK_{67} \| SK_{66} \| SK_{65} \| SK_{64}$	be74727f
$SK_7 \| SK_6 \| SK_5 \| SK_4$	b8695b51	$SK_{71} \| SK_{70} \| SK_{69} \| SK_{68}$	af9a8263
$SK_{11} \| SK_{10} \| SK_9 \| SK_8$	07c2c9e8	$SK_{75} \| SK_{74} \| SK_{73} \| SK_{72}$	1e2d5c4a
$SK_{15} \| SK_{14} \| SK_{13} \| SK_{12}$	2b471032	$SK_{79} \| SK_{78} \| SK_{77} \| SK_{76}$	1ceda097
$SK_{19} \| SK_{18} \| SK_{17} \| SK_{16}$	6c262bcd	$SK_{83} \| SK_{82} \| SK_{81} \| SK_{80}$	d4b17ca3
$SK_{23} \| SK_{22} \| SK_{21} \| SK_{20}$	828eb698	$SK_{87} \| SK_{86} \| SK_{85} \| SK_{84}$	404e7bee
$SK_{27} \| SK_{26} \| SK_{25} \| SK_{24}$	230cef4d	$SK_{91} \| SK_{90} \| SK_{89} \| SK_{88}$	5730f30a
$SK_{31} \| SK_{30} \| SK_{29} \| SK_{28}$	254c2af7	$SK_{95} \| SK_{94} \| SK_{93} \| SK_{92}$	d0e6a233
$SK_{35} \| SK_{34} \| SK_{33} \| SK_{32}$	1c16a4c1	$SK_{99} \| SK_{98} \| SK_{97} \| SK_{96}$	67687c35
$SK_{39} \| SK_{38} \| SK_{37} \| SK_{36}$	a5657527	$SK_{103} \| SK_{102} \| SK_{101} \| SK_{100}$	12027b6f
$SK_{43} \| SK_{42} \| SK_{41} \| SK_{40}$	eeb25316	$SK_{107} \| SK_{106} \| SK_{105} \| SK_{104}$	e5dcdbea
$SK_{47} \| SK_{46} \| SK_{45} \| SK_{44}$	5a463014	$SK_{111} \| SK_{110} \| SK_{109} \| SK_{108}$	e1992132
$SK_{51} \| SK_{50} \| SK_{49} \| SK_{48}$	17a6c593	$SK_{115} \| SK_{114} \| SK_{113} \| SK_{112}$	504c5475
$SK_{55} \| SK_{54} \| SK_{53} \| SK_{52}$	6d85475c	$SK_{119} \| SK_{118} \| SK_{117} \| SK_{116}$	68c8899b
$SK_{59} \| SK_{58} \| SK_{57} \| SK_{56}$	ea44f8f1	$SK_{123} \| SK_{122} \| SK_{121} \| SK_{120}$	fa18e40d
$SK_{63} \| SK_{62} \| SK_{61} \| SK_{60}$	422702ca	$SK_{127} \| SK_{126} \| SK_{125} \| SK_{124}$	e2345934

Round	Value	Round	Value
Initial	00ee222144886643	Round 17	db63ca6b6e9dfaaf
Round 1	ee2d21b1880a435f	Round 18	63776b6b9d09af72
Round 2	2db4b11c0acc5fde	Round 19	77856b93091172c5
Round 3	b4951c9fcca3dec5	Round 20	851793871106c58c
Round 4	95c19fe4a30fc556	Round 21	17a7878206f18c48
Round 5	c115e4730f545645	Round 22	a7598251f1c64855
Round 6	15e27386540d45b7	Round 23	597d5119c6e85575
Round 7	e26486c30dabb777	Round 24	7d4a196ee8e775d8
Round 8	6424c35bab9d7772	Round 25	4a7f6ef7e7bdd882
Round 9	24725b8c9d607282	Round 26	7fadf729bdcb8284
Round 10	72458c7b602d829d	Round 27	ad442985cb29845f
Round 11	458c7bab2dc69d59	Round 28	44b58548296e5f31
Round 12	8cc6ab08c6ba5982	Round 29	b51d488f6e0231f3
Round 13	c60f0841ba688280	Round 30	1df78ff802f8f39d
Round 14	0fd3413668f280d4	Round 31	f7fdf850f8529dd8
Round 15	d35c3627f2afd4e4	Round 32	23fd9f50e552e6d8
Round 16	5cdb27caaf6ee4fa	Final	23ce9f72e543e6d8

3. Test vectors 3

Key : 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
Plaintext : 01 23 45 67 89 ab cd ef
Ciphertext : 7a 6f b2 a2 8d 23 f4 66

Sub Key	Value	Sub Key	Value
$SK_3 \| SK_2 \| SK_1 \| SK_0$	27437b69	$SK_{67} \| SK_{66} \| SK_{65} \| SK_{64}$	4f172746
$SK_7 \| SK_6 \| SK_5 \| SK_4$	490c1018	$SK_{71} \| SK_{70} \| SK_{69} \| SK_{68}$	88857f72
$SK_{11} \| SK_{10} \| SK_9 \| SK_8$	501d3667	$SK_{75} \| SK_{74} \| SK_{73} \| SK_{72}$	1f408181
$SK_{15} \| SK_{14} \| SK_{13} \| SK_{12}$	2c5a3569	$SK_{79} \| SK_{78} \| SK_{77} \| SK_{76}$	65480d16
$SK_{19} \| SK_{18} \| SK_{17} \| SK_{16}$	57233a5e	$SK_{83} \| SK_{82} \| SK_{81} \| SK_{80}$	7766437c
$SK_{23} \| SK_{22} \| SK_{21} \| SK_{20}$	25437d71	$SK_{87} \| SK_{86} \| SK_{85} \| SK_{84}$	2b4b8a7f
$SK_{27} \| SK_{26} \| SK_{25} \| SK_{24}$	7e796e4e	$SK_{91} \| SK_{90} \| SK_{89} \| SK_{88}$	6a552a53
$SK_{31} \| SK_{30} \| SK_{29} \| SK_{28}$	38716140	$SK_{95} \| SK_{94} \| SK_{93} \| SK_{92}$	2b532134
$SK_{35} \| SK_{34} \| SK_{33} \| SK_{32}$	19253564	$SK_{99} \| SK_{98} \| SK_{97} \| SK_{96}$	1c2f5520
$SK_{39} \| SK_{38} \| SK_{37} \| SK_{36}$	5a2c4e12	$SK_{103} \| SK_{102} \| SK_{101} \| SK_{100}$	0f110c12
$SK_{43} \| SK_{42} \| SK_{41} \| SK_{40}$	5b315429	$SK_{107} \| SK_{106} \| SK_{105} \| SK_{104}$	0a132445
$SK_{47} \| SK_{46} \| SK_{45} \| SK_{44}$	7f7d796f	$SK_{111} \| SK_{110} \| SK_{109} \| SK_{108}$	4e182245
$SK_{51} \| SK_{50} \| SK_{49} \| SK_{48}$	26376848	$SK_{115} \| SK_{114} \| SK_{113} \| SK_{112}$	17253f72
$SK_{55} \| SK_{54} \| SK_{53} \| SK_{52}$	345e3259	$SK_{119} \| SK_{118} \| SK_{117} \| SK_{116}$	77592c50
$SK_{59} \| SK_{58} \| SK_{57} \| SK_{56}$	69450b16	$SK_{123} \| SK_{122} \| SK_{121} \| SK_{120}$	31613f7a
$SK_{63} \| SK_{62} \| SK_{61} \| SK_{60}$	79705d37	$SK_{127} \| SK_{126} \| SK_{125} \| SK_{124}$	61356c59

Round	Value	Round	Value
Initial	0123456889a9cdf2	Round 17	4f316376b71aad6d
Round 1	23e16815a93af283	Round 18	312f76671a416d89
Round 2	e11815383ace83de	Round 19	2f4a67b241a489a5
Round 3	186638cdce4ede4d	Round 20	4ac1b2d7a491a5d2
Round 4	66d3cd794e624d8a	Round 21	c102d7549118d291
Round 5	d3ee79f8624d8a3e	Round 22	0290547186091f9
Round 6	eeaef8e44d763ee5	Round 23	90987783600ef997
Round 7	ae21e4317684e5c0	Round 24	980e83240e0d97da
Round 8	218b31cc845fc020	Round 25	0ec824f30d84daa7
Round 9	8bedcc255f2f2034	Round 26	c871f3688496a7eb
Round 10	edea259c2f1d347f	Round 27	71bf68e49605eb61
Round 11	ea609c3b1d2e7f8b	Round 28	bfb0e42805eb61dd
Round 12	60753b712ee88b1a	Round 29	b0d028c9eb97ddad
Round 13	75327140e84a1acb	Round 30	d021c90d9769adb1
Round 14	32b940224a63cb9c	Round 31	21630d95692db157
Round 15	b93e224f63e79c80	Round 32	7a63b2958d2df457
Round 16	3e4f4f63e7b780ad	Final	7a6fb2a28d23f466

4. Test vectors 4

Key : 28 db c3 bc 49 ff d8 7d cf a5 09 b1 1d 42 2b e7
Plaintext : b4 1e 6b e2 eb a8 4a 14
Ciphertext : cc 04 7a 75 20 9c 1f c6

Sub Key	Value	Sub Key	Value
$SK_3 \| SK_2 \| SK_1 \| SK_0$	38789841	$SK_{67} \| SK_{66} \| SK_{65} \| SK_{64}$	16b326ec
$SK_7 \| SK_6 \| SK_5 \| SK_4$	10a80fbe	$SK_{71} \| SK_{70} \| SK_{69} \| SK_{68}$	99ba9c4a
$SK_{11} \| SK_{10} \| SK_9 \| SK_8$	951708dd	$SK_{75} \| SK_{74} \| SK_{73} \| SK_{72}$	471a423a
$SK_{15} \| SK_{14} \| SK_{13} \| SK_{12}$	5434f622	$SK_{79} \| SK_{78} \| SK_{77} \| SK_{76}$	aa42df8c
$SK_{19} \| SK_{18} \| SK_{17} \| SK_{16}$	8c401225	$SK_{83} \| SK_{82} \| SK_{81} \| SK_{80}$	1365e98d
$SK_{23} \| SK_{22} \| SK_{21} \| SK_{20}$	c1422382	$SK_{87} \| SK_{86} \| SK_{85} \| SK_{84}$	60686246
$SK_{27} \| SK_{26} \| SK_{25} \| SK_{24}$	784be476	$SK_{91} \| SK_{90} \| SK_{89} \| SK_{88}$	4416e398
$SK_{31} \| SK_{30} \| SK_{29} \| SK_{28}$	12321a85	$SK_{95} \| SK_{94} \| SK_{93} \| SK_{92}$	2525975c
$SK_{35} \| SK_{34} \| SK_{33} \| SK_{32}$	36fdfc00	$SK_{99} \| SK_{98} \| SK_{97} \| SK_{96}$	1bd56655
$SK_{39} \| SK_{38} \| SK_{37} \| SK_{36}$	59d25f47	$SK_{103} \| SK_{102} \| SK_{101} \| SK_{100}$	2ce9d3ae
$SK_{43} \| SK_{42} \| SK_{41} \| SK_{40}$	2da77c03	$SK_{107} \| SK_{106} \| SK_{105} \| SK_{104}$	cbcc693f
$SK_{47} \| SK_{46} \| SK_{45} \| SK_{44}$	4036be69	$SK_{111} \| SK_{110} \| SK_{109} \| SK_{108}$	208e4a1f
$SK_{51} \| SK_{50} \| SK_{49} \| SK_{48}$	fefe0447	$SK_{115} \| SK_{114} \| SK_{113} \| SK_{112}$	bd36748f
$SK_{55} \| SK_{54} \| SK_{53} \| SK_{52}$	da6f6776	$SK_{119} \| SK_{118} \| SK_{117} \| SK_{116}$	4f20c84f
$SK_{59} \| SK_{58} \| SK_{57} \| SK_{56}$	df6de5d7	$SK_{123} \| SK_{122} \| SK_{121} \| SK_{120}$	eaa6394c
$SK_{63} \| SK_{62} \| SK_{61} \| SK_{60}$	32b55709	$SK_{127} \| SK_{126} \| SK_{125} \| SK_{124}$	d75d461a

Round	Value	Round	Value
Initial	b4366bbdeb6b4ad0	Round 17	90517aee395c438b
Round 1	368cbd8d6b48d053	Round 18	5112eeba5c8f8b78
Round 2	8c3c8dcf4895534b	Round 19	12b8ba748feb78fd
Round 3	3cf3cff795344ba7	Round 20	b87574e3eb3bfd6b
Round 4	f3d8f70d34d7a719	Round 21	7530e31b3bb76b20
Round 5	d8b20d19d7e119b9	Round 22	30aa1bf7b7b8206d
Round 6	b26a1900e1d3b96f	Round 23	aa46f705b89e6dde
Round 7	6a640004d3d96f72	Round 24	461305279e5dde71
Round 8	64530481d91c7217	Round 25	135c27595d7371b8
Round 9	538d819b1c7e171c	Round 26	5c075938733fb800
Round 10	8dd29b857e781c17	Round 27	07d938f53ff70000
Round 11	d24d85d7782b1739	Round 28	d93bf52af71f005f
Round 12	4d85d7552b94399b	Round 29	3b442ab61f575f1d
Round 13	852b551e94fd9b90	Round 30	447db63f57901d31
Round 14	2b4e1ecdfd7a90cc	Round 31	7d193f3390b731df
Round 15	4ecacdf87adecc4a	Round 32	cc197a3320b71fdf
Round 16	ca90f87ade394a43	Final	cc047a75209c1fc6