

The CAST-256 Encryption Algorithm
[draft-adams-cast-256-00.txt](#)

Status of This Memo

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Abstract

There is always a desire in the Internet community for unencumbered encryption algorithms with a range of key sizes that can provide security for a variety of cryptographic applications and protocols.

This document describes an existing algorithm that can be used to satisfy this requirement. Included are a description of the cipher and the key scheduling algorithm, the s-boxes, and a set of test vectors (Appendix A).

Table of Contents

Status of This Memo.....	1
Abstract.....	1
1 . Introduction.....	2
2 . CAST-256 Algorithm Specification.....	2
3 . Cipher Naming.....	8
4 . Cipher Usage.....	8

5. Security Considerations.....	8
6. References.....	8
7. Authors' Addresses.....	8
Appendix A. Test Vectors.....	9

[1. Introduction](#)

This document describes the CAST-256 encryption algorithm, a DES-like Substitution-Permutation Network (SPN) cryptosystem built upon the CAST-128 encryption algorithm [[1](#)] which appears to have good resistance to differential cryptanalysis, linear cryptanalysis, and related-key cryptanalysis. This cipher also possesses a number of other desirable cryptographic properties, including avalanche, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), no complementation property, and an absence of weak and semi-weak keys. It thus appears to be a good candidate for general-purpose use throughout the Internet community wherever a cryptographically-strong, freely-available encryption algorithm is required.

CAST-256 has a block size of 128 bits and a variable key size (128, 160, 192, 224, or 256 bits).

[2. CAST-256 Algorithm Specification](#)

[2.1 CAST-128 Notation](#)

The following notation from CAST-128 [[1](#)] is relevant to CAST-256.

CAST-128 uses a pair of subkeys per round: a 5-bit quantity K_{ri} is used as a "rotation" key for round i and a 32-bit quantity K_{mi} is used as a "masking" key for round i .

Three different round functions are used in CAST-128. The rounds are as follows (where D is the data input to the operation, $I_a - I_d$ are the most significant byte through least significant byte of I , respectively, S_i is the i th s-box (see [Section 1.1.1](#) for s-box contents), and O is the output of the operation). Note that "+" and "-" are addition and subtraction modulo $2^{*}32$, "^" is bitwise eXclusive-OR, and "<<<" is the circular left-shift operation.

Type 1: $I = ((K_{mi} + D) \lll K_{ri})$
 $O = ((S_1[I_a] \wedge S_2[I_b]) - S_3[I_c]) + S_4[I_d]$

Type 2: $I = ((K_{mi} \wedge D) \lll K_{ri})$
 $O = ((S1[Ia] - S2[Ib]) + S3[Ic]) \wedge S4[Id]$

Type 3: $I = ((K_{mi} - D) \lll K_{ri})$
 $O = ((S1[Ia] + S2[Ib]) \wedge S3[Ic]) - S4[Id]$

Let f_1, f_2, f_3 be keyed round function operations of Types 1, 2, and 3 (respectively) above.

CAST-128 uses four round function substitution boxes (s-boxes), $S1 - S4$. These are defined as follows (entries (written in hexadecimal notation) are to be read left-to-right, top-to-bottom).

Adams, Gilchrist

Expires 25 August 1999

[Page 2]

Internet Draft

The CAST-256 Encryption Algorithm

25 February 1999

[2.1.1](#) S-Boxes

S-Box $S1$

30fb40d4	9fa0ff0b	6beccd2f	3f258c7a	1e213f2f	9c004dd3	6003e540	cf9fc949
bfd4af27	88bbdbb5	e2034090	98d09675	6e63a0e0	15c361d2	c2e7661d	22d4ff8e
28683b6f	c07fd059	ff2379c8	775f50e2	43c340d3	df2f8656	887ca41a	a2d2bd2d
a1c9e0d6	346c4819	61b76d87	22540f2f	2abe32e1	aa54166b	22568e3a	a2d341d0
66db40c8	a784392f	004dff2f	2db9d2de	97943fac	4a97c1d8	527644b7	b5f437a7
b82cbaef	d751d159	6ff7f0ed	5a097a1f	827b68d0	90ecf52e	22b0c054	bc8e5935
4b6d2f7f	50bb64a2	d2664910	bee5812d	b7332290	e93b159f	b48ee411	4bfff345d
fd45c240	ad31973f	c4f6d02e	55fc8165	d5b1caad	a1ac2dae	a2d4b76d	c19b0c50
882240f2	0c6e4f38	a4e4bfd7	4f5ba272	564c1d2f	c59c5319	b949e354	b04669fe
b1b6ab8a	c71358dd	6385c545	110f935d	57538ad5	6a390493	e63d37e0	2a54f6b3
3a787d5f	6276a0b5	19a6fcdf	7a42206a	29f9d4d5	f61b1891	bb72275e	aa508167
38901091	c6b505eb	84c7cb8c	2ad75a0f	874a1427	a2d1936b	2ad286af	aa56d291
d7894360	425c750d	93b39e26	187184c9	6c00b32d	73e2bb14	a0becb3c	54623779
64459eab	3f328b82	7718cf82	59a2cea6	04ee002e	89fe78e6	3fab0950	325ff6c2
81383f05	6963c5c8	76cb5ad6	d49974c9	ca180dcf	380782d5	c7fa5cf6	8ac31511
35e79e13	47da91d0	f40f9086	a7e2419e	31366241	051ef495	aa573b04	4a805d8d
548300d0	00322a3c	bf64cddf	ba57a68e	75c6372b	50afd341	a7c13275	915a0bf5
6b54bfab	2b0b1426	ab4cc9d7	449ccd82	f7fbf265	ab85c5f3	1b55db94	aad4e324
cfa4bd3f	2deaa3e2	9e204d02	c8bd25ac	eadf55b3	d5bd9e98	e31231b2	2ad5ad6c
954329de	adbe4528	d8710f69	aa51c90f	aa786bf6	22513f1e	aa51a79b	2ad344cc
7b5a41f0	d37cfbad	1b069505	41ece491	b4c332e6	032268d4	c9600acc	ce387e6d
bf6bb16c	6a70fb78	0d03d9c9	d4df39de	e01063da	4736f464	5ad328d8	b347cc96
75bb0fc3	98511bfb	4ffbcc35	b58bcf6a	e11f0abc	bfc5fe4a	a70aec10	ac39570a
3f04442f	6188b153	e0397a2e	5727cb79	9ceb418f	1cacd68d	2ad37c96	0175cb9d
c69dff09	c75b65f0	d9db40d8	ec0e7779	4744ead4	b11c3274	dd24cb9e	7e1c54bd
f01144f9	d2240eb1	9675b3fd	a3ac3755	d47c27af	51c85f4d	56907596	a5bb15e6
580304f0	ca042cf1	011a37ea	8dbfaadb	35ba3e4a	3526ffa0	c37b4d09	bc306ed9
98a52666	5648f725	ff5e569d	0ced63d0	7c63b2cf	700b45e1	d5ea50f1	85a92872
af1fbda7	d4234870	a7870bf3	2d3b4d79	42e04198	0cd0ede7	26470db8	f881814c

474d6ad7	7c0c5e5c	d1231959	381b7298	f5d2f4db	ab838653	6e2f1e23	83719c9e
bd91e046	9a56456e	dc39200c	20c8c571	962bda1c	e1e696ff	b141ab08	7cca89b9
1a69e783	02cc4843	a2f7c579	429ef47d	427b169c	5ac9f049	dd8f0f00	5c8165bf

S-Box S2

1f201094	ef0ba75b	69e3cf7e	393f4380	fe61cf7a	eec5207a	55889c94	72fc0651
ada7ef79	4e1d7235	d55a63ce	de0436ba	99c430ef	5f0c0794	18dcdb7d	a1d6eff3
a0b52f7b	59e83605	ee15b094	e9ffd909	dc440086	ef944459	ba83ccb3	e0c3cdfb
d1da4181	3b092ab1	f997f1c1	a5e6cf7b	01420ddb	e4e7ef5b	25a1ff41	e180f806
1fc41080	179bee7a	d37ac6a9	fe5830a4	98de8b7f	77e83f4e	79929269	24fa9f7b
e113c85b	acc40083	d7503525	f7ea615f	62143154	0d554b63	5d681121	c866c359
3d63cf73	cee234c0	d4d87e87	5c672b21	071f6181	39f7627f	361e3084	e4eb573b
602f64a4	d63acd9c	1bbc4635	9e81032d	2701f50c	99847ab4	a0e3df79	ba6cf38c
10843094	2537a95e	f46f6ffe	a1ff3b1f	208cfb6a	8f458c74	d9e0a227	4ec73a34
fc884f69	3e4de8df	ef0e0088	3559648d	8a45388c	1d804366	721d9bfd	a58684bb
e8256333	844e8212	128d8098	fed33fb4	ce280ae1	27e19ba5	d5a6c252	e49754bd
c5d655dd	eb667064	77840b4d	a1b6a801	84db26a9	e0b56714	21f043b7	e5d05860
54f03084	066ff472	a31aa153	dad4755	b5625dbf	68561be6	83ca6b94	2d6ed23b
eccc01db	a6d3d0ba	b6803d5c	af77a709	33b4a34c	397bc8d6	5ee22b95	5f0e5304
81ed6f61	20e74364	b45e1378	de18639b	881ca122	b96726d1	8049a7e8	22b7da7b

Adams, Gilchrist

Expires 25 August 1999

[Page 3]

Internet Draft	The CAST-256 Encryption Algorithm	25 February 1999
----------------	-----------------------------------	------------------

5e552d25	5272d237	79d2951c	c60d894c	488cb402	1ba4fe5b	a4b09f6b	1ca815cf
a20c3005	8871df63	b9de2fcb	0cc6c9e9	0beeff53	e3214517	b4542835	9f63293c
ee41e729	6e1d2d7c	50045286	1e6685f3	f33401c6	30a22c95	31a70850	60930f13
73f98417	a1269859	ec645c44	52c877a9	cdff33a6	a02b1741	7cbad9a2	2180036f
50d99c08	cb3f4861	c26bd765	64a3f6ab	80342676	25a75e7b	e4e6d1fc	20c710e6
cdf0b680	17844d3b	31eef84d	7e0824e4	2ccb49eb	846a3bae	8ff77888	ee5d60f6
7af75673	2fdd5cdb	a11631c1	30f66f43	b3faec54	157fd7fa	ef8579cc	d152de58
db2ffd5e	8f32ce19	306af97a	02f03ef8	99319ad5	c242fa0f	a7e3ebb0	c68e4906
b8da230c	80823028	dcdef3c8	d35fb171	088a1bc8	bec0c560	61a3c9e8	bca8f54d
c72feffa	22822e99	82c570b4	d8d94e89	8b1c34bc	301e16e6	273be979	b0fffeaa6
61d9b8c6	00b24869	b7ffce3f	08dc283b	43daf65a	f7e19798	7619b72f	8f1c9ba4
dc8637a0	16a7d3b1	9fc393b7	a7136eeb	c6bcc63e	1a513742	ef6828bc	520365d6
2d6a77ab	3527ed4b	821fd216	095c6e2e	db92f2fb	5eea29cb	145892f5	91584f7f
5483697b	2667a8cc	85196048	8c4bacea	833860d4	0d23e0f9	6c387e8a	0ae6d249
b284600c	d835731d	dcb1c647	ac4c56ea	3ebd81b3	230eabb0	6438bc87	f0b5b1fa
8f5ea2b3	fc184642	0a036b7a	4fb089bd	649da589	a345415e	5c038323	3e5d3bb9
43d79572	7e6dd07c	06dfdf1e	6c6cc4ef	7160a539	73bfbe70	83877605	4523ecf1

S-Box S3

8defc240	25fa5d9f	eb903dbf	e810c907	47607fff	369fe44b	8c1fc644	aececa90
beb1f9bf	eefbcaea	e8cf1950	51df07ae	920e8806	f0ad0548	e13c8d83	927010d5
11107d9f	07647db9	b2e3e4d4	3d4f285e	b9afa820	fade82e0	a067268b	8272792e
553fb2c0	489ae22b	d4ef9794	125e3fbc	21fffcee	825b1bfd	9255c5ed	1257a240
4e1a8302	bae07fff	528246e7	8e57140e	3373f7bf	8c9f8188	a6fc4ee8	c982b5a5

a8c01db7	579fc264	67094f31	f2bd3f5f	40fff7c1	1fb78dfc	8e6bd2c1	437be59b
99b03dbf	b5dbc64b	638dc0e6	55819d99	a197c81c	4a012d6e	c5884a28	ccc36f71
b843c213	6c0743f1	8309893c	0feddd5f	2f7fe850	d7c07f7e	02507fbf	5afb9a04
a747d2d0	1651192e	af70bf3e	58c31380	5f98302e	727cc3c4	0a0fb402	0f7fef82
8c96fdad	5d2c2aae	8ee99a49	50da88b8	8427f4a0	1eac5790	796fb449	8252dc15
efbd7d9b	a672597d	ada840d8	45f54504	fa5d7403	e83ec305	4f91751a	925669c2
23efe941	a903f12e	60270df2	0276e4b6	94fd6574	927985b2	8276dbcb	02778176
f8af918d	4e48f79e	8f616ddf	e29d840e	842f7d83	340ce5c8	96bbb682	93b4b148
ef303cab	984faf28	779faf9b	92dc560d	224d1e20	8437aa88	7d29dc96	2756d3dc
8b907cee	b51fd240	e7c07ce3	e566b4a1	c3e9615e	3cf8209d	6094d1e3	cd9ca341
5c76460e	00ea983b	d4d67881	fd47572c	f76cedd9	bda8229c	127dadaa	438a074e
1f97c090	081bdb8a	93a07ebe	b938ca15	97b03cff	3dc2c0f8	8d1ab2ec	64380e51
68cc7bfb	d90f2788	12490181	5de5ffd4	dd7ef86a	76a2e214	b9a40368	925d958f
4b39ffffa	ba39aee9	a4ffd30b	faf7933b	6d498623	193cbcfa	27627545	825cf47a
61bd8ba0	d11e42d1	cead04f4	127ea392	10428db7	8272a972	9270c4a8	127de50b
285ba1c8	3c62f44f	35c0eaa5	e805d231	428929fb	b4fcdf82	4fb66a53	0e7dc15b
1f081fab	108618ae	fcfd086d	f9ff2889	694bcc11	236a5cae	12deca4d	2c3f8cc5
d2d02dfe	f8ef5896	e4cf52da	95155b67	494a488c	b9b6a80c	5c8f82bc	89d36b45
3a609437	ec00c9a9	44715253	0a874b49	d773bc40	7c34671c	02717ef6	4feb5536
a2d02fff	d2bf60c4	d43f03c0	50b4ef6d	07478cd1	006e1888	a2e53f55	b9e6d4bc
a2048016	97573833	d7207d67	de0f8f3d	72f87b33	abcc4f33	7688c55d	7b00a6b0
947b0001	570075d2	f9bb88f8	8942019e	4264a5ff	856302e0	72dbd92b	ee971b69
6ea22fde	5f08ae2b	af7a616d	e5c98767	cf1feb2d	61efc8c2	f1ac2571	cc8239c2
67214cb8	b1e583d1	b7dc3e62	7f10bdce	f90a5c38	0ff0443d	606e6dc6	60543a49
5727c148	2be98a1d	8ab41738	20e1be24	af96da0f	68458425	99833be5	600d457d
282f9350	8334b362	d91d1120	2b6d8da0	642b1e31	9c305a00	52bce688	1b03588a
f7baefd5	4142ed9c	a4315c11	83323ec5	dfef4636	a133c501	e9d3531c	ee353783

Adams, Gilchrist

Expires 25 August 1999

[Page 4]

Internet Draft	The CAST-256 Encryption Algorithm	25 February 1999
----------------	-----------------------------------	------------------

S-Box S4

9db30420	1fb6e9de	a7be7bef	d273a298	4a4f7bdb	64ad8c57	85510443	fa020ed1
7e287aff	e60fb663	095f35a1	79ebf120	fd059d43	6497b7b1	f3641f63	241e4adf
28147f5f	4fa2b8cd	c9430040	0cc32220	fdd30b30	c0a5374f	1d2d00d9	24147b15
ee4d111a	0fca5167	71ff904c	2d195ffe	1a05645f	0c13fefe	081b08ca	05170121
80530100	e83e5efe	ac9af4f8	7fe72701	d2b8ee5f	06df4261	bb9e9b8a	7293ea25
ce84ffdf	f5718801	3dd64b04	a26f263b	7ed48400	547eebe6	446d4ca0	6cf3d6f5
2649abdf	aea0c7f5	36338cc1	503f7e93	d3772061	11b638e1	72500e03	f80eb2bb
abe0502e	ec8d77de	57971e81	e14f6746	c9335400	6920318f	081dbb99	ffc304a5
4d351805	7f3d5ce3	a6c866c6	5d5bcc9a	daec6fea	9f926f91	9f46222f	3991467d
a5bf6d8e	1143c44f	43958302	d0214eeb	022083b8	3fb6180c	18f8931e	281658e6
26486e3e	8bd78a70	7477e4c1	b506e07c	f32d0a25	79098b02	e4eabb81	28123b23
69dead38	1574ca16	df871b62	211c40b7	a51a9ef9	0014377b	041e8ac8	09114003
bd59e4d2	e3d156d5	4fe876d5	2f91a340	557be8de	00eae4a7	0ce5c2ec	4db4bba6
e756bdf	dd3369ac	ec17b035	06572327	99afc8b0	56c8c391	6b65811c	5e146119
6e85cb75	be07c002	c2325577	893ff4ec	5bbfc92d	d0ec3b25	b7801ab7	8d6d3b24

```

20c763ef c366a5fc 9c382880 0ace3205 aac9548a eca1d7c7 041afa32 1d16625a
6701902c 9b757a54 31d477f7 9126b031 36cc6fdb c70b8b46 d9e66a48 56e55a79
026a4ceb 52437eff 2f8f76b4 0df980a5 8674cde3 edda04eb 17a9be04 2c18f4df
b7747f9d ab2af7b4 efc34d20 2e096b7c 1741a254 e5b6a035 213d42f6 2c1c7c26
61c2f50f 6552daf9 d2c231f8 25130f69 d8167fa2 0418f2c8 001a96a6 0d1526ab
63315c21 5e0a72ec 49bafefd 187908d9 8d0dbd86 311170a7 3e9b640c cc3e10d7
d5cad3b6 0caec388 f73001e1 6c728aff 71eae2a1 1f9af36e cfcabd12f c1de8417
ac07be6b cb44a1d8 8b9b0f56 013988c3 b1c52fca b4be31cd d8782806 12a3a4e2
6f7de532 58fd7eb6 d01ee900 24adffc2 f4990fc5 9711aac5 001d7b95 82e5e7d2
109873f6 00613096 c32d9521 ada121ff 29908415 7fbb977f af9eb3db 29c9ed2a
5ce2a465 a730f32c d0aa3fe8 8a5cc091 d49e2ce7 0ce454a9 d60acd86 015f1919
77079103 dea03af6 78a8565e dee356df 21f05cbe 8b75e387 b3c50651 b8a5c3ef
d8eeb6d2 e523be77 c2154529 2f69efdf afe67afb f470c4b2 f3e0eb5b d6cc9876
39e4460c 1fda8538 1987832f ca007367 a99144f8 296b299e 492fc295 9266beab
b5676e69 9bd3ddda df7e052f db25701c 1b5e51ee f65324e6 6afce36c 0316cc04
8644213e b7dc59d0 7965291f ccd6fd43 41823979 932bcd6f b657c34d 4edfd282
7ae5290c 3cb9536b 851e20fe 9833557e 13ecf0b0 d3ffb372 3f85c5c1 0aef7ed2

```

2.2 CAST-256 Notation

The following notation is employed in the specification of CAST-256.

Let f_1, f_2, f_3 be as defined for CAST-128.

Let $BETA = (ABCD)$ be a 128-bit block where A, B, C and D are each 32 bits in length.

Let " $BETA \leftarrow Qi(BETA)$ " be short-hand notation for the following:

```

C = C ^ f1(D, Kr0_(i), Km0_(i))
B = B ^ f2(C, Kr1_(i), Km1_(i))
A = A ^ f3(B, Kr2_(i), Km2_(i))
D = D ^ f1(A, Kr3_(i), Km3_(i))

```

Let " $BETA \leftarrow QBARI(BETA)$ " be short-hand notation for the following:

```

D = D ^ f1(A, Kr3_(i), Km3_(i))
A = A ^ f3(B, Kr2_(i), Km2_(i))
B = B ^ f2(C, Kr1_(i), Km1_(i))
C = C ^ f1(D, Kr0_(i), Km0_(i))

```

($Q(*)$ is called a "forward quad-round" and $QBAR(*)$ is called a "reverse quad-round".)

Let $Kr_i = \{Kr0_i, Kr1_i, Kr2_i, Kr3_i\}$ be the set of rotation keys for the i th quad-round, where Krj_i is a 5-bit rotation key for $f1$, $f2$, or $f3$ (as specified above).

Let $Km_i = \{Km0_i, Km1_i, Km2_i, Km3_i\}$ be the set of masking keys for the i th quad-round, where Kmj_i is a 32-bit masking key for $f1$, $f2$, or $f3$ (as specified above).

Let $KAPPA = (ABCDEFGH)$ be a 256-bit block where A, B, \dots, H are each 32 bits in length.

Let " $KAPPA \leftarrow Wi(KAPPA)$ " be short-hand notation for the following:

```
G = G ^ f1(H, Tr0_(i), Tm0_(i))
F = F ^ f2(G, Tr1_(i), Tm1_(i))
E = E ^ f3(F, Tr2_(i), Tm2_(i))
D = D ^ f1(E, Tr3_(i), Tm3_(i))
C = C ^ f2(D, Tr4_(i), Tm4_(i))
B = B ^ f3(C, Tr5_(i), Tm5_(i))
A = A ^ f1(B, Tr6_(i), Tm6_(i))
H = H ^ f2(A, Tr7_(i), Tm7_(i))
```

($W(*)$ is called a "forward octave".)

Let " $Kr_i \leftarrow KAPPA$ " be short-hand notation for the following:

```
Kr0_(i) = 5LSB(A), Kr1_(i) = 5LSB(C), Kr2_(i) = 5LSB(E),
Kr3_(i) = 5LSB(G)
```

where $5LSB(x)$ denotes "the five least significant bits of x ".

Let " $Km_i \leftarrow KAPPA$ " be short-hand notation for the following:

```
Km0_(i) = H, Km1_(i) = F, Km2_(i) = D, Km3_(i) = B
```

[2.3](#) The CAST-256 Cipher

BETA = 128bits of plaintext.

```
for (i=0; i<6; i++)
  BETA <- Qi(BETA)
for (i=6; i<12; i++)
  BETA <- QBARi(BETA)
```

128bits of ciphertext = BETA

Round Key Re-Ordering for Decryption

The cipher employs a 256-bit primary key K . Decryption is identical to encryption except that the sets of quad-round keys $Kr_{-}(i)$, $Km_{-}(i)$ derived from K are used in reverse order as follows.

```
for (i=0; i<12; i++)
{
    KrNEW_(i) = Kr_(11-i)
    KmNEW_(i) = Km_(11-i)
}
```

[2.4](#) The CAST-256 Key Schedule

Initialization:

```
Cm = 2**30 * SQRT(2) = 5A827999 (base 16)
Mm = 2**30 * SQRT(3) = 6ED9EBA1 (base 16)
Cr = 19
Mr = 17
```

```
for (i=0; i<24; i++)
{
    for (j=0; j<8; j++)
    {
        Tmj_(i) = Cm
        Cm = (Cm + Mm) mod 2**32
        Trj_(i) = Cr
        Cr = (Cr + Mr) mod 32
    }
}
```

Key Schedule:

$KAPPA = ABCDEFGH = 256$ bit of primary key, K .

```
for (i=0; i<12; i++)
{
    KAPPA <- W2i(KAPPA)
    KAPPA <- W2i+1(KAPPA)
    Kr_(i) <- KAPPA
    Km_(i) <- KAPPA
}
```

Note: $(|K| = 128) \Rightarrow (E = F = G = H = 0)$
 $(|K| = 160) \Rightarrow (F = G = H = 0)$
 $(|K| = 192) \Rightarrow (G = H = 0)$
 $(|K| = 224) \Rightarrow (H = 0)$

Internet Draft The CAST-256 Encryption Algorithm 25 February 1999

[3. Cipher Naming](#)

In order to avoid confusion when variable keysize operation is used, the name CAST-256 is to be considered synonymous with the name CAST6; this allows a keysize to be appended without ambiguity. Thus, for example, CAST-256 with a 192-bit key is to be referred to as CAST6-192; where a 256-bit key is explicitly intended, the name CAST6-256 should be used.

[4. Cipher Usage](#)

The CAST-256 cipher described in this document is available worldwide on a royalty-free and licence-free basis for commercial and non-commercial uses.

[5. Security Considerations](#)

This entire memo is about security since it describes an algorithm which is specifically intended for cryptographic purposes.

[6. References](#)

- [1] C. Adams, The CAST-128 Encryption Algorithm, [RFC 2144](#), May 1997.

[7. Authors' Addresses](#)

Questions about this memo can be directed to:

Carlisle Adams
Entrust Technologies
750 Heron Road, Suite E08
Ottawa, Ontario, Canada
K1V 1A7
phone: 613-247-3180
fax: 613-247-3690
e-mail: carlisle.adams@entrust.com

Jeff Gilchrist
Entrust Technologies
750 Heron Road, Suite E08
Ottawa, Ontario, Canada
K1V 1A7
613-248-3074
613-247-3450
jeff.gilchrist@entrust.com

Internet Draft The CAST-256 Encryption Algorithm 25 February 1999

Appendix A: Test Vectors

Intermediate Values Known Answer Test. The data listed is:

KEYSIZE=the current key length in bits

KEY=the key in hexadecimal format

PT=the plaintext to be encrypted

R=the quad-round number (1 to 12)

ROTK1,ROTK2,ROTK3,ROTK4=the rotation keys for the current quad-round

MASK1,MASK2,MASK3,MASK4=the masking keys for the current quad-round

OUT=the output of the quad-round

CT=the ciphertext corresponding to the given plaintext.

For each key size, an encryption and the corresponding decryption are shown.

KEYSIZE=128

KEY=2342bb9efa38542c0af75647f29f615d

PT=00000000000000000000000000000000

R=1

ROTK1=1c	ROTK2=1d	ROTK3=18	ROTK4=06
MASK1=f364d7f9	MASK2=233500c0	MASK3=83cee501	MASK4=01f857c6
OUT=e2c604af966715811b377f12de19e459			

R=2

ROTK1=1e	ROTK2=18	ROTK3=13	ROTK4=02
MASK1=ae877786	MASK2=ef78852e	MASK3=0aa1c41f	MASK4=a28ec9c4
OUT=5375c3be208f38eed0419d98f50dd9b3			

R=3

ROTK1=02	ROTK2=1d	ROTK3=01	ROTK4=0b
MASK1=a3eedefb	MASK2=ac426ecf	MASK3=2e8220ec	MASK4=cd92c34a
OUT=732e4ec0f205e39afaf407c956d83728			

R=4
ROTK1=0d ROTK2=1d ROTK3=04 ROTK4=12
MASK1=3046827f MASK2=568ab6b9 MASK3=b86e7c10 MASK4=ef290a58
OUT=af23fd837033dc81a60be8a69865c543

R=5
ROTK1=01 ROTK2=14 ROTK3=0c ROTK4=06
MASK1=302e76c3 MASK2=cf429964 MASK3=e9ecad47 MASK4=8850a515
OUT=8b5e011401e1124f731135fa780c59ef

R=6
ROTK1=17 ROTK2=1d ROTK3=0e ROTK4=09
MASK1=bb903fdc MASK2=a9915d2f MASK3=0974e50a MASK4=0c1708f1
OUT=bdea3985cd08c7902096561b76f20944

R=7

Adams, Gilchrist Expires 25 August 1999 [Page 9]

Internet Draft The CAST-256 Encryption Algorithm 25 February 1999

ROTK1=03 ROTK2=13 ROTK3=07 ROTK4=0e
MASK1=13330f06 MASK2=5e1906f5 MASK3=fb2bce75 MASK4=8331aed4
OUT=438053fe465c299bcb35f273b10ea71a

R=8
ROTK1=07 ROTK2=02 ROTK3=14 ROTK4=14
MASK1=a29189c1 MASK2=d1aeff98 MASK3=c9b55ba7 MASK4=c149f70c
OUT=172c3a9a2791509d5939f58b703f2533

R=9
ROTK1=1c ROTK2=08 ROTK3=1f ROTK4=1f
MASK1=5687e118 MASK2=bc4f5d80 MASK3=cca4c042 MASK4=bab3fb68
OUT=79178d5f90187732f8007fd3884cc309

R=10
ROTK1=15 ROTK2=12 ROTK3=04 ROTK4=0f
MASK1=cdb18671 MASK2=f06a3c64 MASK3=0c7031f9 MASK4=7dfbff4e
OUT=e9e2b1f23e82479baec3b3b35fdf890f

R=11
ROTK1=1f ROTK2=1a ROTK3=01 ROTK4=0e
MASK1=317654b5 MASK2=a1433222 MASK3=f6d8c69f MASK4=304dfbeb
OUT=1f3270101b2b38adc4818ca2aa334a

R=12
ROTK1=0b ROTK2=11 ROTK3=0f ROTK4=18
MASK1=9339b14f MASK2=971d14bb MASK3=f3b7ca97 MASK4=2b8a06f9

OUT=c842a08972b43d20836c91d1b7530f6b

CT=c842a08972b43d20836c91d1b7530f6b

R=1

ROTK1=0b	ROTK2=11	ROTK3=0f	ROTK4=18
MASK1=9339b14f	MASK2=971d14bb	MASK3=f3b7ca97	MASK4=2b8a06f9
OUT=1f3270101b2b38adc4818ca2aa fc334a			

R=2

ROTK1=1f	ROTK2=1a	ROTK3=01	ROTK4=0e
MASK1=317654b5	MASK2=a1433222	MASK3=f6d8c69f	MASK4=304dfbeb
OUT=e9e2b1f23e82479baec3b3b35fd f890f			

R=3

ROTK1=15	ROTK2=12	ROTK3=04	ROTK4=0f
MASK1=cdb18671	MASK2=f06a3c64	MASK3=0c7031f9	MASK4=7dfbff4e
OUT=79178d5f90187732f8007fd3884cc309			

R=4

ROTK1=1c	ROTK2=08	ROTK3=1f	ROTK4=1f
MASK1=5687e118	MASK2=bc4f5d80	MASK3=cca4c042	MASK4=bab3fb68
OUT=172c3a9a2791509d5939f58b703f2533			

R=5

Adams, Gilchrist	Expires 25 August 1999	[Page 10]
------------------	------------------------	-----------

Internet Draft	The CAST-256 Encryption Algorithm	25 February 1999
----------------	-----------------------------------	------------------

ROTK1=07	ROTK2=02	ROTK3=14	ROTK4=14
MASK1=a29189c1	MASK2=d1aef f98	MASK3=c9b55ba7	MASK4=c149f70c
OUT=438053fe465c299bcb35f273b10ea71a			

R=6

ROTK1=03	ROTK2=13	ROTK3=07	ROTK4=0e
MASK1=13330f06	MASK2=5e1906f5	MASK3=fb2bce75	MASK4=8331aed4
OUT=bdea3985cd08c7902096561b76f20944			

R=7

ROTK1=17	ROTK2=1d	ROTK3=0e	ROTK4=09
MASK1=bb903fdc	MASK2=a9915d2f	MASK3=0974e50a	MASK4=0c1708f1
OUT=8b5e011401e1124f731135fa780c59ef			

R=8

ROTK1=01	ROTK2=14	ROTK3=0c	ROTK4=06
MASK1=302e76c3	MASK2=cf429964	MASK3=e9ecad47	MASK4=8850a515
OUT=af23fd837033dc81a60be8a69865c543			

R=9
ROTK1=0d ROTK2=1d ROTK3=04 ROTK4=12
MASK1=3046827f MASK2=568ab6b9 MASK3=b86e7c10 MASK4=ef290a58
OUT=732e4ec0f205e39afaf407c956d83728

R=10
ROTK1=02 ROTK2=1d ROTK3=01 ROTK4=0b
MASK1=a3eedefb MASK2=ac426ecf MASK3=2e8220ec MASK4=cd92c34a
OUT=5375c3be208f38eed0419d98f50dd9b3

R=11
ROTK1=1e ROTK2=18 ROTK3=13 ROTK4=02
MASK1=ae877786 MASK2=ef78852e MASK3=0aa1c41f MASK4=a28ec9c4
OUT=e2c604af966715811b377f12de19e459

R=12
ROTK1=1c ROTK2=1d ROTK3=18 ROTK4=06
MASK1=f364d7f9 MASK2=233500c0 MASK3=83cee501 MASK4=01f857c6
OUT=00000000000000000000000000000000

PT=00000000000000000000000000000000

=====

KEYSIZE=192
KEY=2342bb9efa38542cbcd0ac83940ac298bac77a7717942863

PT=00000000000000000000000000000000

R=1
ROTK1=1e ROTK2=1a ROTK3=1b ROTK4=16

Adams, Gilchrist Expires 25 August 1999 [Page 11]

Internet Draft The CAST-256 Encryption Algorithm 25 February 1999

MASK1=21daa501 MASK2=fcdcf612 MASK3=62f629b3 MASK4=9ec93bfa
OUT=4d468c8ca43c1ab66eae0bb9062fe876

R=2
ROTK1=1a ROTK2=1d ROTK3=19 ROTK4=1f
MASK1=d7f04aaf MASK2=76a4b0c2 MASK3=7364327b MASK4=fe0602c3
OUT=1fd808cfd82ac7354728e719a4cc0ebe

R=3
ROTK1=13 ROTK2=19 ROTK3=15 ROTK4=18
MASK1=c5b5a24e MASK2=20577cc0 MASK3=e58b12aa MASK4=a87da0f1

OUT=d3507d51934db5335cebdbb550b774b6

R=4

ROTK1=0f	ROTK2=00	ROTK3=15	ROTK4=08
MASK1=5b1b847c	MASK2=3d700297	MASK3=310383e1	MASK4=a1a19785
OUT=fab3a20243c1c67bf1759f40c4b732e8			

R=5

ROTK1=01	ROTK2=0f	ROTK3=0f	ROTK4=11
MASK1=34422fa1	MASK2=745d0d3c	MASK3=0804535e	MASK4=42de73d8
OUT=cf003a27ba91d2346ddfa8ec76bdf029			

R=6

ROTK1=06	ROTK2=10	ROTK3=06	ROTK4=07
MASK1=ae5e85f6	MASK2=d1f789b0	MASK3=e2113794	MASK4=db8768c0
OUT=b4fb78a74bbaccbfa45c36c23ed997e			

R=7

ROTK1=09	ROTK2=1d	ROTK3=08	ROTK4=1f
MASK1=1a000d83	MASK2=dc6d0e51	MASK3=3b65ccaf	MASK4=b0470998
OUT=1cedb6d94abb223765f0fb9364a8f07f			

R=8

ROTK1=09	ROTK2=0a	ROTK3=01	ROTK4=0d
MASK1=d500ec2c	MASK2=77e23f6f	MASK3=3d1422b2	MASK4=0e4c04aa
OUT=b3289009a03b021d54cec6628712c165			

R=9

ROTK1=1b	ROTK2=0d	ROTK3=0b	ROTK4=14
MASK1=f9b1a192	MASK2=aded6200	MASK3=0fc10d02	MASK4=d8bdb797
OUT=a4d8f6d0abd8613d241fff3c2ba02882			

R=10

ROTK1=17	ROTK2=1d	ROTK3=1c	ROTK4=17
MASK1=a81550e2	MASK2=44e56b22	MASK3=ac97284c	MASK4=e1021ad2
OUT=61a3f74a9a5da18d53a25ce8f3302357			

R=11

ROTK1=19	ROTK2=1e	ROTK3=11	ROTK4=02
MASK1=b09d0346	MASK2=15167c69	MASK3=19990bbd	MASK4=a9258551
OUT=ca5ad45111a662f740c9a94b1d43dfb6			

Adams, Gilchrist

Expires 25 August 1999

[Page 12]

Internet Draft

The CAST-256 Encryption Algorithm

25 February 1999

R=12

ROTK1=10	ROTK2=0d	ROTK3=08	ROTK4=01
----------	----------	----------	----------

MASK1=69d0c348 MASK2=c8a3d81d MASK3=d2714d62 MASK4=8cc3f35a
OUT=1b386c0210dcadcbdd0e41aa08a7a7e8

CT=1b386c0210dcadcbdd0e41aa08a7a7e8

R=1
ROTK1=10 ROTK2=0d ROTK3=08 ROTK4=01
MASK1=69d0c348 MASK2=c8a3d81d MASK3=d2714d62 MASK4=8cc3f35a
OUT=ca5ad45111a662f740c9a94b1d43dfb6

R=2
ROTK1=19 ROTK2=1e ROTK3=11 ROTK4=02
MASK1=b09d0346 MASK2=15167c69 MASK3=19990bbd MASK4=a9258551
OUT=61a3f74a9a5da18d53a25ce8f3302357

R=3
ROTK1=17 ROTK2=1d ROTK3=1c ROTK4=17
MASK1=a81550e2 MASK2=44e56b22 MASK3=ac97284c MASK4=e1021ad2
OUT=a4d8f6d0abd8613d241fff3c2ba02882

R=4
ROTK1=1b ROTK2=0d ROTK3=0b ROTK4=14
MASK1=f9b1a192 MASK2=aded6200 MASK3=0fc10d02 MASK4=d8bdb797
OUT=b3289009a03b021d54cec6628712c165

R=5
ROTK1=09 ROTK2=0a ROTK3=01 ROTK4=0d
MASK1=d500ec2c MASK2=77e23f6f MASK3=3d1422b2 MASK4=0e4c04aa
OUT=1cedb6d94abb223765f0fb9364a8f07f

R=6
ROTK1=09 ROTK2=1d ROTK3=08 ROTK4=1f
MASK1=1a000d83 MASK2=dc6d0e51 MASK3=3b65ccaf MASK4=b0470998
OUT=b4fb78a74bbaccbfa45c36c23ed997e

R=7
ROTK1=06 ROTK2=10 ROTK3=06 ROTK4=07
MASK1=ae5e85f6 MASK2=d1f789b0 MASK3=e2113794 MASK4=db8768c0
OUT=cf003a27ba91d2346ddfa8ec76bdf029

R=8
ROTK1=01 ROTK2=0f ROTK3=0f ROTK4=11
MASK1=34422fa1 MASK2=745d0d3c MASK3=0804535e MASK4=42de73d8
OUT=fab3a20243c1c67bf1759f40c4b732e8

R=9
ROTK1=0f ROTK2=00 ROTK3=15 ROTK4=08
MASK1=5b1b847c MASK2=3d700297 MASK3=310383e1 MASK4=a1a19785
OUT=d3507d51934db5335cebdbb550b774b6

R=10

ROTK1=13	ROTK2=19	ROTK3=15	ROTK4=18
MASK1=c5b5a24e	MASK2=20577cc0	MASK3=e58b12aa	MASK4=a87da0f1
OUT=1fd808cfd82ac7354728e719a4cc0ebe			

R=11

ROTK1=1a	ROTK2=1d	ROTK3=19	ROTK4=1f
MASK1=d7f04aaf	MASK2=76a4b0c2	MASK3=7364327b	MASK4=fe0602c3
OUT=4d468c8ca43c1ab66eae0bb9062fe876			

R=12

ROTK1=1e	ROTK2=1a	ROTK3=1b	ROTK4=16
MASK1=21daa501	MASK2=fcdffc612	MASK3=62f629b3	MASK4=9ec93bfa
OUT=00000000000000000000000000000000			

PT=00000000000000000000000000000000

=====

KEYSIZE=256

KEY=2342bb9efa38542cbcd0ac83940ac2988d7c47ce264908461cc1b5137ae6b604

PT=00000000000000000000000000000000

R=1

ROTK1=08	ROTK2=12	ROTK3=0e	ROTK4=17
MASK1=420b1cef	MASK2=03f07e80	MASK3=cd2ab3ee	MASK4=15371a16
OUT=f6c3b9a6ffd8a31ce04dbcf7772f1536			

R=2

ROTK1=0a	ROTK2=04	ROTK3=01	ROTK4=13
MASK1=bc6025e3	MASK2=d54f5aba	MASK3=17fa667a	MASK4=bb8a840e
OUT=9477ef6fd7d6fce3dcaa27d6132465ee			

R=3

ROTK1=1e	ROTK2=0d	ROTK3=10	ROTK4=01
MASK1=446c0950	MASK2=b4542da0	MASK3=523baa91	MASK4=4a914503
OUT=c056ec5748ecd90f992cf07f3529160f			

R=4

ROTK1=15	ROTK2=0e	ROTK3=0d	ROTK4=09
MASK1=4106d4de	MASK2=9ce441e7	MASK3=2c390c3b	MASK4=52d1b516
OUT=7bcc57d80603b6c7b9ca75eea5cb1c2d			

MASK1=4bd673d3 MASK2=36399d66 MASK3=63385006 MASK4=0579675f
OUT=dd9940f4f2e1786ab6f2bdee519a407e

R=2
ROTK1=1c ROTK2=0b ROTK3=1b ROTK4=1f
MASK1=4fdf26fe MASK2=a4850785 MASK3=615eadd0 MASK4=9b507d47
OUT=57c3a554eafe71dc6a33fe0bda83f566

R=3
ROTK1=1b ROTK2=00 ROTK3=01 ROTK4=01
MASK1=2cf3fd07 MASK2=75580ec1 MASK3=513614b9 MASK4=478097ef
OUT=f4f1322a076d4f5eb2d14dc75815ccf1

Adams, Gilchrist Expires 25 August 1999 [Page 15]

Internet Draft The CAST-256 Encryption Algorithm 25 February 1999

R=4
ROTK1=1a ROTK2=0f ROTK3=09 ROTK4=10
MASK1=4b81b846 MASK2=9f1d941b MASK3=ebb8fe8a MASK4=6616847e
OUT=4265774a393a8a32ed78c5c1571893e4

R=5
ROTK1=0b ROTK2=04 ROTK3=0e ROTK4=19
MASK1=69b1d027 MASK2=e628d930 MASK3=4904b3cd MASK4=51fad71a
OUT=b11d972f22ed26d085189ca3b6c79d36

R=6
ROTK1=1d ROTK2=06 ROTK3=0b ROTK4=1c
MASK1=c0e98900 MASK2=8832532c MASK3=d7403525 MASK4=26ed4609
OUT=1b03a108d6f1878e03a62e72c9c97662

R=7
ROTK1=1f ROTK2=11 ROTK3=17 ROTK4=0a
MASK1=85fcd124 MASK2=c567c5fe MASK3=a4113025 MASK4=ce949239
OUT=d62686a2b01d11837fb6a46c79fc1816

R=8
ROTK1=09 ROTK2=16 ROTK3=08 ROTK4=16
MASK1=2827db72 MASK2=7920623f MASK3=10948a1a MASK4=b639f290
OUT=7bcc57d80603b6c7b9ca75eea5cb1c2d

R=9
ROTK1=15 ROTK2=0e ROTK3=0d ROTK4=09
MASK1=4106d4de MASK2=9ce441e7 MASK3=2c390c3b MASK4=52d1b516
OUT=c056ec5748ecd90f992cf07f3529160f

R=10

ROTK1=1e ROTK2=0d ROTK3=10 ROTK4=01
MASK1=446c0950 MASK2=b4542da0 MASK3=523baa91 MASK4=4a914503
OUT=9477ef6fd7d6fce3dcaa27d6132465ee

R=11
ROTK1=0a ROTK2=04 ROTK3=01 ROTK4=13
MASK1=bc6025e3 MASK2=d54f5aba MASK3=17fa667a MASK4=bb8a840e
OUT=f6c3b9a6ffd8a31ce04dbcf7772f1536

R=12
ROTK1=08 ROTK2=12 ROTK3=0e ROTK4=17
MASK1=420b1cef MASK2=03f07e80 MASK3=cd2ab3ee MASK4=15371a16
OUT=00000000000000000000000000000000

PT=00000000000000000000000000000000

Full Copyright Statement

Copyright (C) The Internet Society (1997). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."