Information Technology
Cryptographic Protection of Information
Hash Function

Official Publication
Russian State Standards
Moscow

Translated from the Russian by Michael Roe

Preface to the English Translation

Firstly, a disclaimer. This English translation has not been approved by GOST or any other standards body. Prospective users of this standard are advised to consult the Russian language version, which is approved by GOST.

This is a first draft of the English translation; I have left out several paragraphs of explanatory text that are present in the Russian text. In the English text, I have indicated these ommissions by ellipsis (. . .).

Foreword

1. ... standards technical committee TK22 (“information technology”) ...
2. ... Russian State Standards on 23.05.94 number 154
3. First Edition

Contents

Introduction

This standard (defines?) an algorithm or procedure (known as?) a hash function, (which takes) sequences of binary symbols ...

... asymmetric cryptographic algorithm GOST R 34.10.

Information Technology
Cryptographic Protection of Information
Hash Function

Date Introduced: 1995-01-01

1 Scope

... ...

2 Normative References

This standard uses the following normative references:

- GOST 28147-89 Information Processing Systems - Cryptographic Protection - Cryptographic Transformation Algorithm

- GOST R 34.10-95 Information Technology - Cryptographic Protection of Information - Produce and check procedures of electronic digital signature based on asymmetric cryptographic algorithm

3 Notation

This standard uses the following notation:

B^*	set of all finite words formed from the alphabet $B = \{0, 1\}$
$\|A\|$	length of a word $A \in B^*$
$V_k(2)$	set of all binary words of length k
$A\|\|B$	concatenation of words $A, B \in B^*$ - word length $\|A\| + \|B\|$, ...
A^k	concatenation of k copies of the word A $(A \in B^*)$
$< N >_k$	a word of length k, containing in binary format the residue $N \pmod{2^k}$ of an integer N
$\hat{A}$	the integer whose binary format representation is A $(A \in B^*)$
$\overline{\oplus}$	bitwise addition modulo 2 of words of equal length
$\oplus'$	addition using the rule $A \oplus' B =< \hat{A} + \hat{B} >_k$ $(k = \|A\| = \|B\|)$
M	sequence of binary symbols which is subject to hashing (in an Electronic Digital Signature communications system) $M \in B^*$
h	hash function which reduces a sequence $M \in B^*$ to a word $h(M) \in V_{256}(2)$
$E_K(A)$	result of enciphering word A with key K using encipherment algorithm GOST 28147 in simple substitution mode (electronic codebook mode) $(K \in V_{256}(2), A \in V_{64}(2))$
H	initial hash vector
$e := g$	assignment of e with the value of g

4 Assumed Relations

... ...

$$h : B^* \to V_{256}(2)$$

... ...

$$\chi : V_{256}(2) \times V_{256}(2) \to V_{256}(2)$$

... ...

5 Steps of the Hash Function

... ...

5.1 Key Generation

Consider $X = (b_{256}, b_{255}, \ldots, b_1) \in V_{256}(2)$

Let

$$X = x_4\|x_3\|x_2\|x_1$$

$$\begin{aligned} &= \eta_{16}\|\eta_{15}\|\ldots\|\eta_1 \\ &= \xi_{32}\|\xi_{31}\|\ldots\|\xi_1 \end{aligned}$$

Where

$$x_i = (b_{i\times 64}, \ldots, b_{(i-1)\times 64+1}) \in V_{64}(2), i = \overline{1,4}$$

$$\eta_j = (b_{j\times 16}, \ldots, b_{(j-1)\times 16+1}) \in V_{16}(2), j = \overline{1,16}$$

$$\xi_k = (b_{k\times 8}, \ldots, b_{(k-1)\times 8+1}) \in V_8(2), k = \overline{1,32}$$

Designate $A(X) = (x_1 \overline{\oplus} x_2)\|x_4\|x_3\|x_2$

Use the transformation $P : V_{256}(2) \rightarrow V_{256}(2)$, which constructs the word $\xi_{32}\|\ldots\|\xi_1$ from the word $\xi_{\varphi(32)}\|\ldots\|\xi_{\varphi(1)}$, where

$$\varphi(i + 1 + 4(k-1)) = 8i + k, i = \overline{0,3}, k = \overline{1,8}$$

...

- words $H, M \in V_{256}(2)$
- parameters: words $C_i (i = 2, 3, 4)$, having the values

$$\begin{aligned} C_2 &= C_4 = 0^{256} \\ C_3 &= 1^8 0^8 1^{16} 0^{24} 1^{16} 0^8 (0^8 1^8)^2 1^8 0^8 (0^8 1^8)^4 (1^8 0^8)^4 \end{aligned}$$

... ...

```
1.    $i := 1, U := H, V := M$
2.    $W = U' \overline{\oplus} V, K_i = P(W)$
3.    $i := i + 1$
4. Check if $i = 5$. If the test succeeds, then go to step 7; otherwise, go to step 5.
5.    $U := A(U) \overline{\oplus} C_i, V := A(A(V)), W := U \overline{\oplus} V, K_i = P(W)$
6. Go to step 3.
7. Stop.
```

5.2 Enciphering Transformation

In this stage, H is enciphered in words of 64 bits using the keys $K_i (i = 1, 2, 3, 4)$.

$$H = h_4 \| h_3 \| h_2 \| h_1, h_i \in V_{64}(2), i = \overline{1, 4}$$

$$s_i = E_{K_i}(h_i), i = 1, 2, 3, 4$$

$$S = s_4 \| s_3 \| s_2 \| s_1$$

5.3 Mixing Transformation

Let $\psi : V_{256}(2) \rightarrow V_{256}(2)$ map the word $\eta_{16} \| \ldots \| \eta_1, \eta_i \in V_{16}(2), i = \overline{1, 16}$ to the word $\eta_1 \overline{\oplus} \eta_2 \overline{\oplus} \eta_3 \overline{\oplus} \eta_4 \overline{\oplus} \eta_{13} \overline{\oplus} \eta_{16} \| \ldots \| \eta_2$

The value resulting from this step of the hash function is $\chi(M, H) = \psi^{61}(H' \overline{\oplus} \psi(M \overline{\oplus} \psi^{12}(S)))$ where ψ^i is the ith power of the transformation ψ.

6 Procedure for Calculating Hash Function

$M \in B^*$	... sequence M ...
$H \in V_{256}(2)$	current value of the hash function
$\Sigma \in V_{256}(2)$	current value of the checksum
$L \in V_{256}(2)$	current value of the length ...

Stage 1

1. $M := M$
2. $H := H$
3. $\Sigma := 0^{256}$
4. $L := O^{256}$
5. Procede to stage 2

Stage 2

1. If $|M| > 256$, then go to stage 3.
2. $L :=< \hat{L} + |M| >_{256}$

3. $M' := 0^{256-|M|}||M$

4. $\Sigma := \Sigma\overline{\oplus}'M'$

5. $H := \chi(M', H)$

6. $H := \chi(L, H)$

7. $H := \chi(\Sigma, H)$

8. This is the end of the algorithm

Stage 3

1. ... $M_s \in V_{256}(2)$ ... $(M = M_p|||Ms)$

2. $H := \chi(M_s, H)$

3. $L :=< L + 256 >_{256}$

4. $\Sigma := \Sigma\overline{\oplus}'M_s$

5. $M := M_p$

6. Go to stage 2.

A Worked Example

...

A.1 Using algorithm GOST 28147

... algorithm GOST 28147 in simple substitution mode ...
... substitution blocks $\pi_1, \pi_2, \ldots \pi_8$:

	8	7	6	5	4	3	2	1
0	1	d	4	6	7	5	e	4
1	f	b	b	c	d	8	b	a
2	d	4	a	7	a	1	4	9
3	0	1	0	1	1	d	c	2
4	5	3	7	5	0	a	6	d
5	7	f	2	f	8	3	d	8
6	a	5	1	d	9	4	f	0
7	4	9	d	8	f	2	a	e
8	9	0	3	4	e	e	2	6
9	2	a	6	a	4	f	3	b
10	3	e	8	9	6	c	8	1
11	e	7	5	e	c	7	1	c
12	6	6	9	0	b	6	0	7
13	b	8	c	3	2	0	7	f
14	8	2	f	b	5	9	5	5
15	c	c	e	2	3	b	9	3

A.2 Representation of vectors

...

A.3 Examples of the hash function

H = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

A.3.1

Text
M = 73657479 62203233 3d687467 6e656c20
2c656761 7373656d 20736920 73696854

Initial Hash Value
H = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

Initial sum of text blocks
Σ = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

Initial text length
L = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

L = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000100

M' = 73657479 62203233 3d687467 6e656c20
2c656761 7373656d 20736920 73696854

Ξ = 73657479 62203233 3d687467 6e656c20
2c656761 7373656d 20736920 73696854

K_1 = 733d2c20 65686573 74746769 79676120
626e7373 20657369 326c6568 33206d54

K_2 = 110c733d 0d166568 130e7474 06417967
1d00626e 161a2065 090d326c 4d393320

K_3 = 80b111f3 730df216 850013f1 c7e1f941
620c1dff 3abae91a 3fa109f2 f513b239

K_4 = a0e2804e ff1b73f2 ece27a00 e7b8c7e1
ee1d620c ac0cc5ba a804c05e a18b0aec

H is enciphered in 64-bit blocks using algorithm GOST 28147.

h_1 = 00000000 00000000
enciphered under key K_1 gives the result
s_1 = 42abbcce 32bc0b1b
h_2 = 00000000 00000000
enciphered under key K_2 gives the result
s_2 = 5203ebc8 5d9bcffd
h_3 = 00000000 00000000
enciphered under key K_3 gives the result
s_3 = 8d345899 00ff0e28
h_4 = 00000000 00000000
enciphered under key K_4 gives the result
s_4 = e7860419 0d2a562d

S = e7860419 0d2a562d 8d345899 00ff0e28
5203ebc8 5d9bcffd 42abbcce 32bc0b1b

Ξ = cf9a8c65 505967a4 68a03b8c 42de7624
d99c4124 883da687 561c7de3 3315c034

K_1 = cf68d956 9aa09c1c 8c3b417d 658c24e3
50428833 59de3d15 6776a6c1 a4248734

K_2 = 8fcf68d9 809aa09c 3c8c3b41 c7658c24
bb504288 2859de3d 666676a6 b3a42487

K_3 = 4e70cf97 3c8065a0 853c8cc4 57389a8c
cabb50bd e3d7a6de d1996788 5cb35b24

K_4 = 584e70cf c53c8065 48853c8c 1657389a
edcabb50 78e3d7a6 eed19867 7f5cb35b

S = 66b70f5e f163f461 468a9528 61d60593
e5ec8a37 3fd42279 3cd1602d dd783e86

Ξ = 2b6ec233 c7bc89e4 2abc2692 5fea7285
dd3848d1 c6ac997a 24f74e2b 09a3aef7

K_1 = 5817f104 0bd45d84 b6522f27 4af5b00b
a531b57a 9c8fdfca bb1efcc6 d7a517a3

K_2 = e82759e0 c278d950 15cc523c fc72ebb6
d2c73da8 19a6cac9 3e8440f5 c0ddb65a

K_3 = 77483ad9 f7c29caa eb06d1d7 841bcad3
fbc3daa0 7cb555f0 d4968080 0a9e56bc

K_4 = a1157965 2d9fbc9c 088c7cc2 46fb3dd2
7684adcb fa4aca06 53eff7d7 c0748708

S = 2aebfa76 a85fb57d 6f164de9 2951a581
c31e7435 4930fd05 1f8a4942 550a582d

Ξ = faff37a6 15a81669 1cff3ef8 b68ca247
e09525f3 9f811983 2eb81975 d366c4b1

The result of the hash function is:

H = faff37a6 15a81669 1cff3ef8 b68ca247
e09525f3 9f811983 2eb81975 d366c4b1

A.3.2

Step 1

H = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

M = 73616820 65676173 73656d20 6c616e69
6769726f 20656874 2065736f 70707553

K_1 = 73736720 61656965 686d7273 20206f6f
656c2070 67616570 616e6875 73697453

K_2 = 14477373 0c0c6165 1f01686d 4f002020
4c50656c 04156761 061d616e 1d277369

K_3 = cbff14b8 6d04f30c 96051ffe dfffb000
35094caf 72f9fb15 7cf006e2 ab1ae227

K_4 = ebaccb00 f7006dfb e5e16905 b0b0dfff
ba1c3509 fd118df9 f61b830f f8c554e5

S = ff41797c eeaadac2 43c9b1df 2e14681c
eddc2210 1ee1adf9 fa67e757 dafe3ad9

Ξ = f0ceea4e 368b5a60 c63d96c1 e5b51cd2
a93befbd 2634f0ad cbbb69ce ed2d5d9a

Step 2

H	=	f0ceea4e 368b5a60 c63d96c1 e5b51cd2 a93befbd 2634f0ad cbbb69ce ed2d5d9a
M'	=	00000000 00000000 00000000 00007365 74796220 3035203d 20687467 6e656c20
K_1	=	f0c6ddeb ce3d42d3 ea968d1d 4ec19da9 36e51683 8bb50148 5a6fd031 60b790ba
K_2	=	16a4c6a9 f9df3d3b e4fc96ef 5309c1bd fb68e526 2cdbb534 fe161c83 6f7dd2c8
K_3	=	c49d846d 1780482c 9086887f c48c9186 9dcb0644 d1e641e5 a02109af 9d52c7cf
K_4	=	bdb0c9f0 756e9131 e1f290ea 50e4cbb1 1cad9536 f4e4b674 99f31e29 70c52afa
S	=	62a07ea5 ef3c3309 2ce1b076 173d48cc 6881eb66 f5c7959f 63fca1f1 d33c31b8
Ξ	=	95bea0be 88d5aa02 fe3c9d45 436ce821 b8287cb6 2cbc135b 3e339efe f6576ca9

Step 3

H = 95bea0be 88d5aa02 fe3c9d45 436ce821
b8287cb6 2cbc135b 3e339efe f6576ca9

L = 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000190

K_1 = 95feb83e be3c2833 a09d7c9e be45b6fe
88432cf6 d56cbc57 aae8136d 02215b39

K_2 = 8695feb8 1bbe3c28 e2a09d7c 48be45b6
da88432c ebd56cbc 7fabe813 f292215b

K_3 = b9799501 141b413c 1ee2a062 0cb74145
6fda88bc d0142a6c fa80aa16 15f2fdb1

K_4 = 94b97995 7d141b41 c21ee2a0 040cb741
346fda88 46d0142a bdfa81aa dc1562fd

S = d42336e0 2a0a6998 6c65478a 3d08a1b9
9fddff20 4808e863 94fd9d6d f776a7ad

Ξ = 47e26afd 3e7278a1 7d473785 06140773
a3d97e7e a744cb43 08aa4c24 3352c745

Step 4

H	=	47e26afd 3e7278a1 7d473785 06140773 a3d97e7e a744cb43 08aa4c24 3352c745
Σ	=	73616820 65676173 73656d20 6c61e1ce dbe2d48f 509a88b1 40cde7d6 ded5e173
K_1	=	340e7848 83223b67 025aaaab dda5f1f2 5b6af7ed 1575de87 19e64326 d2bdf236
K_2	=	03dc0ed0 f4cd26bc 8b595f13 f5a4a55e a8b063cb ed3d7325 6511662a 7963008d
K_3	=	c954ef19 d0779a68 ed37d3fb 7da5addc 4a9d0277 78ef765b c4731191 7ebb21b1
K_4	=	6d12bc47 d9363d19 1e3c696f 28f2dc02 f2137f37 64e4c18b 69ccfbf8 ef72b7e3
S	=	790dd7a1 066544ea 2829563c 3c39d781 25ef9645 ee2c05dd a5ecad92 2511a4d1
Ξ	=	0852f562 3b89dd57 aeb4781f e54df14e eafbc135 0613763a 0d770aa6 57ba1a47

The result of the hash function is:

H	=	0852f562 3b89dd57 aeb4781f e54df14e eafbc135 0613763a 0d770aa6 57ba1a47

UDC 681.3.06:006.354 P85 Inv. No. 5002
Key words: information technology; cryptographic protection of information; electronic digital signature; asymmetric cryptographic algorithm; ???, ???, ???, hash-function, function for hashing

Editor L. V. Athanashenko
Technical Editor N. S. Grischanova
Proof Reader A. S. Chernousova

Submitted for typesetting 24 June 94.

Approved for publication 19 August 94.

0.93 USL. kr-ott 0.93.

Order of the Sign of Honour Printing House, 107076, Moscow,