ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

Издание официальное

Тексты ГОСТ 34.311-95 и ГОСТ Р 34.11-94 идентичны между собой.

БЗ 3-94/131

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Главным управлением безопасности связи Федерального агентства правительственной связи и информации ir Всероссийским научно-исследовательским институтом стандартизации

ВНЕСЁН **Техническим комитетом по стандартизации ТК 22 «Информационная технология» и Федеральным агентством правительственной связи и информации**

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 23.05.94 № 154

3 ВВЕДЕН ВПЕРВЫЕ

i t

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Расширяющееся применение информационных технологий при создании, обработке, передаче и хранении документов требует в определенных случаях сохранения конфиденциальности их содержания, обеспечения полноты и достоверности.

Одним из эффективных направлений защиты информации является криптография (криптографическая защита), широко применяемая в различных сферах деятельности в государственных и коммерческих структурах.

Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

Настоящий стандарт определяет процедуру вычисления хэш-функции для любой последовательности двоичных символов.

Функция хэширования заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины, что позволяет использовать эту функцию в процедурах электронной цифровой подписи для сокращения времени подписывания и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

Information technology.
Cryptographic Data Security-
Hashing function

Дата введения 1995—01—01

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур электронной цифровой подписи (ЭЦП) при передаче, обработке и хранении информации в автоматизированных системах.

Определенная в настоящем стандарте функция хэшировании используется при реализации систем электронной цифровой подписи на базе асимметричного криптографического алгоритма по ГОСТ Р 34.10.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы ссылки на сле^}ющие стандарты:

ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

ГОСТ Р 34.10—94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

3 ОБОЗНАЧЕНИЯ

В настоящем стандарте используются следующие обозначения:

Издание официальное

В —множество всех конечных слов в алфавите В = {0,1}. Чтение с нов и нумерация знаков алфавита (символов) осуществляются справа налево (номер правого символа в слове равен единице, второго справа — двум и т. д.).

|А| — длина слова Af*B*.

Vk(2) —множество всех бинарных слов длины к.

А||В — конкатенация слов А, В 6 В* — слово длины |А| + |В|, в котором левые |А| символов образуют слово А» а правые |В| символов образуют слово В. Можно также использовать обозначение АЦВ-АВ.

А ^{к}~~ конкатенация к экземпляров слова А (At В*),

— слово длины к, содержащее двоичную запись вычета N(mod 2^{K}) неотрицательного целого числа N.

А — неотрицательное целое число, имеющее двоичную запись А (At В*).

ф — побитовое сложение слов одинаковой длины по модулю 2.

0 ' — сложение по правилу А Ф'В = <А+В>$_{к}$, (к = |А|—|В|).

М -- последовательность двоичных символов, подлежащая хэшированию Сообщение в системах ЭЦП), М б В*.

h — хли-ф>нкция, отображающая последовательность Мб В* в слово Р (М> б V256 (2) .

$E_{к}$(А) рез>льтат зашифрования слова А на ключе К с использованием алгоритма шифрования по ГОСТ 28147 в режиме простой замены (K6V_{255}(2), Аб V_{6}4(2)).

Н - стартовый вектор хэширования.

е ~g— присвоение параметру е значения g.

4 ОБЩИЕ ПОЛОЖЕНИЯ

Под хэш-функцией h понимается зависящее от параметра гартового вектора хэширования Н, являющегося словом из 56(2)) отображение

⎩ С ^25Г,(2).

Для определения хэш-функции необходимы:

— алгоритм вычисления шаговой функции хэширования и, т. е. отображения

x: V,$_{3С}$<2) x\\Д2> Vre<2);

— описание итеративном процедуры вычисления значения хэш-функции h.

б ШАГОВАЯ ФУНКЦИЯ ХЭШИРОВАНИЯ

Алгоритм вычисления шаговой функции хэширования включает в себя три части, реализующие последовательно:

— генерацию ключей — слов длины 256 битов;

— шифрующее преобразование — зашифрование 64-битных подслов слова Н на ключах Ki (i=l, 2, 3, 4) с использованием алгоритма по ГОСТ 28147 в режиме простой замены;

— перемешивающее преобразование результата шифрования.

5.1 Генерация ключей.

РассмотримX=(Ь$_{356}$, Ь$_{255}$» • • b^eVa^).

Пусть X = x_4||xз||x_2||x_1 =

^lelfaibll- ■ -hi =

= ^32ll^3t|| • • • |Rl,

где X_3=(bix64 ,. .., b(i-nx64+i)6V_{e4}(2), i=l,4;

^{7}J)=(Wxie, .. ., b<j-1)$_X$i&-fl)6V,$_6$(2), j = 1,16;

6$_k$=(bnx8,..., b$_{(k}$_i,x«4a)ev$_a$(2), k = П35.

Обозначают A(X)=(x, © x_2)]x JxJxg.

Используют преобразование P: V_{26G}(2)---------- ^V_{266}(2)

слова £$_{39}$jj... |R, в слово^32)1- • •!$?i>,

где <p(i + l+4(k—l))=8l+k, 1=0н~3, k=l-*-8.

Для генерации ключей необходимо использовать следующие исходные данные;

— слова Н, M6$V_2$5e(2);

— параметры: слова Q (i = 2, 3, 4), имеющие значения

C_2=c_4 = 0^{206} и C_s=lWl^{1}4)*l‘^04^e)4^0^{8}l^8)^4(l^{8}0^s)^4.

При вычислении ключей реализуется следующий алгоритм -

1 Присвоить значения

J: — 1, U: = H, V: = M.

2 Выполнить вычисление

W = U ® V , K, = P(W).

3 Присвоить i: —H-1.

4 Проверить условие i=5.

При положительном исходе перейти к шагу 7. При отрицательном — перейти к шагу 5.

5 Выполнить вычисление

U:=A(U)®q, V: = A(A(V))$_f$ W: = U,®V, K,= P(W).

6 Перейти к шагу 3.
7 Конец работы алгоритма.

5.2 Шифрующее преобразование

На данном этапе осуществляется зашифрование 64-битных подслов слова Н на ключах Ki (i — 1, 2, 3, 4).

Для шифрующего преобразования необходимо использовать следующие исходные данные:

H-hJhelhdht, $h_1 6V_{G4}(2)$, i = M

и набор ключей Кь Кг, Кз, К*.

Реализуют алгоритм зашифрования и получают слова

Si —$Ек_г$(Н]), где 1=1, 2} 3, 4.

В результате данного этапа образуется последовательность

S^sJsJIsJs,.

5 3 Перемешивающее преобразование

г а д< ином этапе осуществляется перемешивание полученной дослещ вательности с примененьем регистра сдвига.

Исходными данными являются:

слоьа Н, Мс $V_2$56(2) и слово S6 Уг5в(2).

Пусть отображение

.....“^V_2se(2)

преобразует слово

V! • ■ -llv,, r/»6V_{i4}(2), J=ГГ 16

ь слово

rH<$r/2&y3®rl$_i$e4i3&Viellrhell-■ -1Мг-

Тогда в качестве значения шаговой функции хэширования принимается слово

x(M, H)=фn|(H·Фф(МФ((»12(5))),

где ф1 - i-я степень преобразования ф.

6 ПРОЦЕДУРА ВЫЧИСЛЕНИЯ ХЭШ-ФУНКЦИИ

Исходными данными для процедуры вычисления значения функции h является подлежащая хэшированию последовательность Mf< B*. Параметром является стартовый вектор хэширования Н — произвольное фиксированное слово из V_2se (2).

Процедура вычисления функции h на каждой итерации использует следующие величины:

Мб В* — часть последовательности М, не Прошедшая процедуры хэширования на предыдущих итерациях;

$HeV_{2M}(2)$ —текущее значение хэш-функции;

2 6 V256(2) —текущее значение контрольной суммы;

L6 $У_2$5б(2) — текущее значение длины обработанной на предыдущих итерациях части последовательности М.

Алгоритм вычисления функции h включает в себя этапы:

Этап 1

Присвоить начальные значения текущих величин

1.1 M:=M
1.2 H: = H
1.3 E: = (P«
1.4 L: = O^{260}
1.5 Переход к этапу 2

Этап 2

2.1 Проверить условие)M|>256.

При положительном исходе перейти к этапу 3.

В противном случае выполнить последовательность вычислений:

2.2 L:= $<L+|M|>_{256}$
2.3 M/:=*0??$^{6''}$,м^ ||M
2.4 2; = £®'M'
2.5 H:-*(M', H)
2.6 H:=*(L, H)
27 H:—x(2, H)
2.8 Конец работы алгоритма

Этап 3

3.1 Вычислить подслово $M_3$6 $V_{256}(2)$ слова М ($M=M_P||M_S$). Далее выполнить последовательность вычислений:

3.2 H:~x(M_S, H)
3.3 **L:=** <jL"j“25b>256
3.4
3.5 M: =M_P
3.6 Перейти к этапу 2.

Значение величины Н, полученное на шаге 2.7, является значением функции хэширования h (М).

Проверочные примеры для вышеизложенной процедуры вычисления хэш-функции приведены в приложении А.

ПРИЛОЖЕНИЕ А
(справочное)

ПРОВЕРОЧНЫЕ ПРИМЕРЫ

Заполнение узлов замены Яь . ., Яз и значение стартового вектора хэширования Н, указанные в данном приложении, рекомендуется использовать только в проверочных примерах для настоящего стандарта

А1 Использование алгоритма ГОСТ 28147

В качестве шифрующего преобразования в приводимых ниже примерах используется алгоритм ГОСТ 28147 з режиме простой замены

При этом заполнение узлов замены щ, лэ, . .,ла блока подстановки л следующее.

	8	7	6	5	4	3	9	1
0	1	D	4	6	7	5	E	4
1	F	B	B	C	D	8	B	A
2	D	4	A	*l*	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	O	*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	I
И	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	в	5	9	5	5
15	C	C	E	2	3	B	9	3

В столбце с номером j, j^=l,8, в строке с номером i, i=0,15, приведено значение ttj(i) в шестнадцатеричной системе счисления

А2 Представление векторов

Последовательности двоичных символов будем записывать как строки шестнадцатеричных цифр, в которых каждая цифра соответствует четырем знакам ее двоичного представления

А3 Примеры вычисления значения хэ ш-функции

В качестве стартового вектора хэширования принимают, например, нулевой вектор

н = 00000000 ooooooоо 00000000 OOGOOOOO
00000000 00000000 00000000 00000000

А3 1 Пусть необходимо выполнить хэширование сообщения

M= 73657479 62203233 3D687467 6E656C20
2C656761 7373656D 20736920 73696854

Выполняют присвоение начальных значений:
текста
M —73657479 ^203233 3D687467 6E656C20
9C656761 70.C356D 20736920 73696854

хэш-функции

H-OOOGOOOO 00000000 00000000 00000000
ooooooоо ooooooоо 00000000 OQOOOOOO

суммы блоков текста

***Z*-00000000 00000000 00000000 00000000**
00000000 00000000 000C0000 00000000

длины текста

L —00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

Так как длина сообщения, подлежащего хэшированию, равна 256 битам (32 байтам),

L — OC000000 OOOOOOOO OOOOOOOO OOOOOOOO
OOOOOOOO OOOOOOOO OOOOOOOO 00000100

M'-M- 73657479 62203233 3D687167 6E656C20
2C656761 7373656D 20736920 73696854, то

нет необходимости дописывать текущий блок нулями,

£=~M'=« 73657479 62203233 3D687467 6E656C20
2C556761 7373656D 20736920 73696854

Переходят к вычислению значения шаговой функции хэширования x (M, H). Вырабатывают ключи

Ki =	733D2C20	65686573	74746769	79676120
	626E7373	20657369	326C6568	33206D54
	1I0C733D	0D166568	130E7474	06417967
	! D0C626E	I6IA2065	090D326C	4D393320
Кз-	8ЭВ1ИРЗ	730DF2I6	850013F1	C7EIF941
	620C1DFF	3ABAE9IA	3FA109F2	F513B239
K* =	A0E2804E	FFSB73F2	ECE27AOO	E7B8C7E1
	EEJD620C	AC0CC5BA	A804C05E	A18B0AEC

Осуществляют зашифрование 64-битных подслов блока H с помощью алгоритма по ГОСТ 28147.

Блок hi — OOOOOOOO 00000000 зашифровывают на ключе Ki и получают si-* = 42ABBCCE 32BC0B1B.

Блок 1*2 = 00000000 00000000 зашифровывают на ключе K_2 и получают S_2 = -5203EBC8 5D9BCFFD.

блок ha-=00200000 00000000 зашифровывают на ключе Кз и получают s_3 = «8D345899 OOFFOE28.

Блок 1*4 = 00000000 00000000 зашифровывают на ключе Кл и получают s_4== -E7860419 0D2A562D.

Получают

S- E7860419 0D2A562D 8D345899 O3FF0E28
5203EBC8 5D9BCFFD 42ABBCCE 32BC0B1B

Выполняют перемешивающее преобразование с применением регистра сдви~га и получают

E-x(M, H)« CF9A8C65 E')5967A4			68A03E8C	42DE7624
	D99C4I24	883DA687	561C7DE3	3315C034

Полагают H — E, вычисляют *к* (L, H).

Ki—	CF68D956 50428833	9ЛА09С1С 59DE3D 15	8С3В417D 6776А6С1	658С24Е3 А4248734
$к_2$-	8FCF68D9 BB504288	609 W9C 2859DE3D	3Г8С3В41 666676А 5	С7658С24 В3 4 42487
Кз-	4С70CF97 CABB50BD	3С8С65А0 Е3D7A6DE	853С8СС4 D19Э6788	5738948С 6СВ35В24
	584E70CF EDCABB50	С53С8065 78E3D7A6	48853С8С EED19867	1657389А 7F5CB35B
S-	66B70F5E E5EC8A37	F163F461 3FD42279	468А9528 3CD1602D	61D60593 DD783E86
E =	2B6EC233 DD3848D1	С7ВС89Е4 С6АС997А	2ABC2692 24F74E2B	5FEA7285 09A3AEF7

Вновь полагают H — S и вычисляют x (2, H)

К1 —	58I7FI04 А531В57А	0BD45D84 9С8FDFCA	В6522F27 BB1EFCC6	4AF5BOOB D7A517A3
$К_2$=	Е82759Е0 D2C73DA8	С278D950 I9A6CAC9	15СС523С 3Е8440F5	FC72EBB6 С0DDB65А
Кз =	77483А D9 FBC3DAA0	F7C29CAA 7CB555F0	FB06D1D7 D4968080	841BCAD3 ОАЭЕ56ВС
к*=	АП 57965 7684ADCB	2D9FBC9C F A4A CA06	D88C7CC2 53EFF7D7	46FB3DD2 С0748708
S-	2AEBFA76 С31Е7435	А85FB57D 4930FD05	6F164DE9 1F8A4942	2951А581 550А582D
s =	FAFF37A6 F09525F3	I5A81669 9F811983	ICFF3EF8 2EB81975	B68CA247 D366C4B1

Таким образом, результат хэширования есть

H =	FAFF37A6 E09525F3	15A81669 9F811983	1CFF3EF8 2EB81975	B68CA247 D366C4B1

А32 Пусть необходимо выполнить хэширование сообщения

M- 7365 74796220 3035203D 20687457 6E656C20 73616820 65676173
73656D20 6C616E69 6769726F 20656874 2065736F 70707553

Так как длина сообщения, подлежащего хэшированию, равна 400 битам (50 байтам), то разбивают сообщение на два блока и второй (старший) блок дописывают нулями В процессе вычислений получают-

ШАГ I

H-00000000 00000000 00003000 00000000
00000000 00000000 ОСИ[1] **00000 00000000**

M =	73616820 6769726F	65676173 20656874	73656D20 2065736F	6С616Е69 70707553
к,=	73736720 656С2070	61656%5 67616570	6С6D7273 616Е6875	20206F6F 73697453

	14477373 4C50656C	0C0C6I65 04156761	1F01686D 061D616E	4F002020 1D277369
Кз-	CBFF14B8 *шт^к?*	6D04F30C *TiY-Wb\b*	96051FFE 7 СЕйШЕА	DFFFBOO0
К4**-**	EBACCBOO BA1C3509	F7006DFB FD118DF9	E5E16905 F61B830F	BOBODFFF F8C554E5
S“	FF41797C EDDC2210	EEAADAC2 1EE1ADF9	43C9B1DF FA67E757	2E14681C DAFE3AD9
E =	F0CEEA4E A93BEFBD	368B5A60 2634 F0AD	C63D96CI CBBB69CE	E5B51CD2 ED2D5D9A

ШАГ 2

н-	F0CEEA4E A93BEFBD	368B5A60 2634F OAO	C63D96C1 CBBB69CE	E5B51CD2 ED2D5D9A
м'—	00000000 00000000 00000000 00C07365 74796220 3035203D 20687467 6E656C20			
	F0C6DDEB 36E5I683	CE3D42D3 8BB50148	EA968D1D 5A6FD031	4EC19DA9 60B790BA
	16A4C6A9 FB68E526	F9DF3D3B 2CDBB534	E4FC96EF FE161C83	53C9C1BD 6F7DD2C8
	C49D845D 9DCB0644	1780482C DIE641E5	9086887F A02109AF	C48C9186 9D52C7CF
	BDB0C9FO 1CAD9536	756E9I31 F4E4B674	E1F290EA 99F31E29	50E4CBBi 70C52AFA
	62A07EA5 688IEB66	EF3C3309 F5C7959F	2CE1B076 63FCAIFI	173D48CC D33C3IB8
E^=	95BEA0BE B8287CB6	88D5AA02 2CBC135B	FE3C9D45 3E339EFE	436CE821 F6576CA9

ШАГ 3

	95BEA0BE B8287CB6	8SD5AA02 2CBC135B	*FE3C9D45* 3E339EFE	436CE821 F6576CA9
	oooooooo oooooooo oooooooo oooooooo 00000000 00000000 OOOOOOOO 00000190			
*i=	‘йЗЕЕВЛ&Е 88432CF6	вдасаш D56CBC57	Атшсад. AAE8136D	WEAtfiWE 02215B39
Кз=	8695FEB8 DA88432C	1BBE3C28 EBD56CBC	E2A09D7C 7FABE813	48ВБ45В6 F292215B
	B9799501 6FDA88BC	141B413C D0J42A6C	1EE2A062 FA80AA16	0CB74U5 15F2FDB1
Kd=	94B97995 346FDA88	7Г>] 41 B4] 46D0142A	C21EE2A0 BDFA81AA	040CB741 DC1562FD
S»	D42336E0 9FDDFF20	2A0A6998 48CSL853	6C65478A 911 D9D6D	3D08A1B9 F776A7AD

E —	47E26AFD A3D97E7E	3E7278A1 A744CB43	7D473785 08AA4C24	06140773 3352C745

ШАГ 4

H =	47E26AFD A3D97E7E	3E7278A1 A744CB43	7D473785 08AA4C24	06140773 3352C745
2 =	73616820 DBE2D48F	65676173 509A88B1	73656D20 40CDE7D6	6C6IE1CE DED5E173
Ki«	340E7848 5B6AF7ED	83223B67 1575DE87	025AAAAB 19E64326	DDA5F1F2 D2BDF236
K*-	03DC0ED0 A8B063CB	F4CD26BC ED3D7325	8B595F13 6511662A	F5A4A55E 7963008D
Кз-	C954EF19 4A9D0277	D0779A68 78EF765B	ED37D3FB C473I191	7DA5ADDC 7EBB21B1
K4 =	6D12BC47 F2137F37	D9363D19 64E4C18B	1E3C696F 69CCFBF8	28F2DC02 EF72B7E3
S —	790DD7A1 25EF9645	066544E A EE2C05DD	2829563C A5ECAD92	3C39D781 2511A4D1
в-	0852F562 EAFBC135	3B89DD57 0613763A	AEB4781F OD770AA6	E54DF14E 57BAIA47

Таким образом, результат хэширования есть

0852F562 EAFBC135	3B89DD57 0613763A	AEB4781F 0D770AA6	E54DF14E 57BA1A47

УДК 681.3.06:006.354 **П85** **ОКСТУ 5002**

Ключевые слова: информационная технология, криптографическая защита информации, электронная цифровая подпись, асимметричный криптографический алгоритм, системы обработки информации, защита сообщений, подтверждение подписи, хэш-функция, функция хэширования

Редактор **Л.** В. **Афанасенко**
Технический редактор **Н.** С. **Гришанова**
Корректор **А.** *С.* **Черноусова**

Сдано **В** наб 24 06 94 Подп в печ 19 08 94 Уел п л 0 93 Уел кр.*отт В,9|.
Уч-изд л 0,84 Тираж 300 экз С 1585

Ордена «Знак Почета» Издательство стандартов, 107076, Москва, Колодезный пер.. 14
Тнп «Московский печатник» Москва, Лялин пер , 6 Зак 208