

() ,

INTERSTATE COUNCIL FOR STANDARDIZATION. METROLOGY AND CERTIFICATION
(ISC)

**34,11 —
2018**



2018

*,

1.0—2015 «

» 1.2—2015 «

»

1

(« »)

2 26 «

3

(29 2018 . 54)

:

{ 31) 004-97	< 31) 004-97	
	AM KG RU TJ	

4 4

2018 . N9 1060-

34.11—2018

1 2019 .

5 34.11—2012

6

« », —

« ».

« ».

()

—

(www.gost.ru)



1	1
2	1
3	1
3.1	1
3.2	2
4	3
5	3
5.1	3
5.2	3
5.3	3
5.4	3
5.5	4
6	
7	5
8	
8.1	1.....	5
8.2	2.....	6
8.3	3.....	6
	{)	7
	17

-
,
,
*
*
- ,
34.10.
/ 9796 (2), (3), / 14888
2382 [1].
(4J—16J / 10118 [7 -
—
« ».

Information technology. Cryptographic data security. Hash-function

— 2019—06—01

1

—
,
,
(),
.

34.10.

,
.

2

34.10—2018

:
.
—
—
« », « 1 », (),
) 8 ,
,

3

3.1

3.1.1 (padding):

— / 10116-1 (7).

3.1.2 (initializing value): ,

— / 10118-1 [7].

3.1.3 (message): .

— / 14888-1 [4].

3.1.4 (round function): , L_2 , L_2^* -

1 / 10118-1 [7].
2 « L » « - L^*

3.1.5 (hash-code): - .

— / 10118-1 [7].

3.1.6 (collision-resistant hash-function): ,

1) , -
;
2) ,
:
3) - , .

1 / 10118-1 [7].
2 -
, , « - », « -
- », « » « »

3.1.7 ([(signature); :

1 / 14888-1 (4).
2 -
, , « , » ,
« » « »

3.2

V^* — : (—), -
;
| | — () V^* (— , | | = 0):
 V_n — , — ;

\$ — 2
;
||8 — , V^* . . . $V_p, t) |>$ $V|_A$,
" — ;
 2^A — 2 :
09 — 2_{jn} ;

Vec,,: $Z_2^n \rightarrow V_n$ —

2^{\wedge}

$z, (0, 1), / - 0, \dots, - 1,$
 $Vec_n(z) = z^{\wedge}, ||\dots||z_5||z_0;$

Int_n: $V_n \rightarrow Z_2$ —

Vec,,. a. Int_n Vec¹;

MSB,,: —

$z_{(1>,||\dots||z_1||z_0} \text{ kin.}$

b —
 , —

;

—

$t V^* | | < 2^{512};$

: '» —

IV —

() (-) ();
 . IV $V_{2^{\wedge}}$

4

$V' \rightarrow V_n$

- 256 = 512 .

5

5.1

IV

IV

- 512 -
 - 2S6

5^{12}

(00000001)⁶⁴.

5.2

V_e

VecgX'IntgiV'g-» V_e .

(1)

$n': Z_2 \rightarrow Z_{28}$.

' («'(0), '(1)..... '(255)):

'=(252.238, 221, 17.207,110.49.22.251, 196.250.218, 35. 197. 4.77.233.119.240.219.147.

46.153.186. 23. 54. 241, 187. 20. 205. 95. 193. 249. 24, 101. 90. 226. 92. 239. 33, 129. 28. 60. 66, 139, 1. 142.79.5,132. 2. 174.227,106.143. 160,6,11.237, 152. 127.212,211,31,235. 52,44.81.234. 200, 72. 171,242.42,104.162.253,58, 206.204,181.112.14.86.8.12.118.18.191.114,19, 71.156.183.93.135. 21.161,150,41.16,123,154,199.243.145,120.111,157,158.178,177,50.117.25.61.255,53.138,126. 109,84.198, 128.195.189. 13.87.223. 245. 36.169. 62.168.67. 201. 215,121,214. 246. 124, 34,185, 3. 224. 15. 236, 222. 122, 148, 176, 188, 220. 232. 40. 80. 78. 51.10, 74. 167. 151, 96. 115. 30. 0. 98. 68. 26, 184.56,130. 100,159.38. 65.173.69. 70.146. 39. 94.85, 47.140.163,165.125,105.213,149, 59.7, 88. 179, 64.134. 172, 29. 247. 48, 55.107. 228,136. 217. 231, 137, 225. 27.131. 73. 76. 63. 248. 254.141, 83. 170, 144, 202, 216, 133. 97. 32. 113. . 164, 45, 43. 9, 91. 203.155. 37. 208.190. 229.108. 82. 89.166, 116, 210.230, 244. 180.192.209. 102,175.194. 57, 75, 99,182).

5.3

S_M

= ({0}, {1}..... {63}):

= (0. 8.16. 24. 32. 40. 48. 56,1. 9. 17. 25. 33. 41, 49. 57. 2.10, 18. 26. 34. 42. 50. 58. 3. 11. 19. 27.

35. 43. 51. 59. 4.12. 20. 28. 36. 44. 52. 60. 5.13, 21. 29. 37. 45. 53, 61, 6.14. 22. 30, 38. 46. 54. 62. 7.15. 23.31. 39.47. 55.63).

5.4

/

GF(2).

$\text{Vec}_4(a_{y_{15}}) || \dots || \text{Vec}_4(a_{i_0})$ $/, / = 0 \dots 63$ $_{15} \dots 0$ $- Z_{16}, i=0 \dots 15$

8e20faa72ba0b470	47107ddd9b505a38	ad08b0e0c3282d1c	d8045870ef14980e
6c022c38f90a4c07	3601161cf205268d	1b8e0b0e798c13c8	83478b07b2468764
a011d380818e8f40	5086e740ce47c920	2843fd2067adea10	14aff010bdd87508
0ad97808d06cb404	05e23c0468365a02	8c711e02341b2d01	46b60f011a83988e
90dab52a387ae76f	486dd4151c3dfdb9	24b86a840e90f0d2	125C354207487869
092e94218d243cba	8a174a9ec8121e5d	4585254f64090fa0	accc9ca9328a8950
9d4df05d5f661451	c0a878a0a1330aa6	60543c50de970553	302a1e286fc58ca7
18150f14b9ec46dd	0c84890ad27623e0	0642ca05693b9f70	0321658cba93c138
86275df09ce8aaa8	439da0784e745554	afc0503c273aa42a	d96O281e9d1d5215
e230140fc0802984	71180a8960409a42	b60c05ca30204d21	5b068c651810a89e
456c34887a3805b9	ac361a443d1c8cd2	561b0d22900e4669	2b838811460723ba
9bcf4486248d9f5d	c3e9224312c8c1a0	effa11af0964ee50	f97d86d98a327728
O4fa2054a80b329c	727d102a548b194e	39b008152acb8227	9258048415eb419d
492c024284fbaec0	aa16012142f35760	S50b6e9e21f7a530	a48b474f9ef5dc18
70a6a56e2440S98e	3853dc371220a247	1ca76e95091051ad	0eddd37c46a08a6d8
07e095624504536c	8d70c431ac02a736	c83862965601dd1b	641c314b2b8ee083

$/=0 \dots 15$.

$4/ \quad / . j - 0 \dots$

$(\quad) :$

$4/+0.4/ + 1.4 / \quad 2.4 / + 3$.

$b - \quad _{63} \dots b_0 \quad \mathbb{E} \quad V_{e4}$

$\mathbb{E} \quad _{64} :$

$= b_{e3}(\text{Vec}_4(a_0 \quad 1 \quad s) | \bullet \quad " || \text{Vec}^{\wedge} a_0 . o)) \quad \textcircled{\bullet} \quad \dots \quad \textcircled{\bullet} \quad ^o(\text{Vec}_4(a^{\wedge} 315)11 \dots || \text{Vec}_4(a^{\wedge} 3o)), \quad (2)$

$\mathbb{E}_{>}, (\text{Vec}_4(e_{e3 \rightarrow 15})) || \dots || \text{Vec}_4(a_{e3 \rightarrow 0}) > = \quad 0^4, \quad \text{to. } \ll 0.$
 $(\text{Vec}_4(a_{e3 \rightarrow 15}) J \dots | \text{Vec}_4(a_{e3 \rightarrow 15})). \quad , \quad \ll$

$/ = 0 \dots 63$.

5.5

$_{127} \dots 0$ $/=0 \dots 127$ $\text{Vec}_4(a_{i_{27}}) || \dots || \text{Vec}_4(a_0) :$

$, = b1085bda1ecadae9ebcb2f81c0657df2f6a76432e45d016714eb88d7585c4fc$
 $4b7ce09192676901a2422a08a460d31505767436cc744d23dd806559f2a64507;$
 $_2 = 6fa3b58aa99d2f1a4fe39d460f70b5d7f3feea720a232b9861d55e0f16b50131$
 $9ab5176b12d699585cb561c2dbOaa7ca55dda21bd7cbcd56e679047021M9bb7;$
 $_3 = f574dcac2bce2fc70a39fc286a3d843506f15eSf529c1f8bf2ea7514M297b7b$
 $d3e20fe490359eMc1c93a376062db09c2b6f443867adb31991e96f50aba0ab2;$
 $C_4 = ef1fdfb3e81566d2f946e1a05d71e4dd488e857e335c3c7d9d721cad685e353f$
 $a9d72c82ed03d675d8b71333935203be3453eaa193e837f1220cbebc84e3d12e;$
 $C_5 = 4bea6bacad4747999a3f410c6ca923637H51c1f1686104a359e35d7800ffbfd$
 $bfgcd1747253af5a3dfff00b723271a167a56a27ea9ea63f5601758fd7c6cfe57;$
 $C_e = ae4faeae1d3ad3d96fa4c33b7a3039c02d66c4f95142a46c187f9ab49af08ec6$
 $Cffa6b71c9ab7b40af21f66c2bec6b6bf71c57236904f35fa68407a46647d6e;$
 $C_7 = f4c70e16eeaac5ec51ac86febf240954399ec6c7e6bf87c9d3473e33197a93c9$
 $0992abc52d822c3706476983284a05043517454ca23c4af38886564d3a14d493;$
 $C_e = 9Mf5b424d93c9a703e7aa020c6e41414eb7f8719c36de1e89b4443b4ddbc49a$
 $f4892bcb929b069069d18d2bd1a5c42f36acc2355951a8d9a47f0dd4bf02e71e;$

$c_d = 378f5a541631229b944c9ad8ec165fde3a7d3a1b258942243cd955b7e00d0984$
 $800a440bdbb2ceb17b2b8a9aa6079c540e38dc92cMf2a607261445183235adb:$
 $C_{10} = abbedea680056f52382aeS48b2e4f3f38941e71cff8a78db1ffe18a1b336103$
 $9fe76702af69334b7a\ 1\ e6c303b7652f43698fad\ 11\ 53bb6c374b4c7fb984S9ced;$
 $C_n = 7bcd9ed0efc889fb3002c6cd635afe94d8fa6bbbebab07612001802114846679$
 $8a1d71efea48b9caeft>acd1d7d476e98dea2594ac06fd85d6bcaa4cd81f32d1b:$
 $C_{j2} = 378ee767f11631bad21380b00449b17acda43c32bcdf1d77f82012d430219f9b$
 $5d80ef9d1891cc86e71da4aa88e12852faf417d5d9b21b9948bc924af11bd720.$

6

- () V^* :

$$|*|^{\wedge 512} - *^{\vee si2} - * = \odot \cdot k a_e V_{512};$$

$$S:V_{512} \text{ " } ^{\wedge 512} - \circ S(e63 | \quad \quad \quad *^{\wedge} \quad (4)$$

«*₃ | |*₃ | |*

«⁶V_a«

$$P:V_{H2} \text{ " } *V_{1S2}' \quad \quad \quad - 0) \text{ " } ^{\wedge ti63} | | j|^{\wedge t}\{0\}' \quad (5)$$

> | | 3 ^{^512'}, ⁶) * 0« ->-< 63:

$$^{\wedge \wedge 512} - *^{\wedge 512}. \quad) \ll \quad _7 | | \dots | \quad _0) / (\quad _7) | | \dots | \quad _7), \quad (6)$$

8^ |---||^ ⁶ V₅₁₂ • » ⁶ 0..... 7.

7

- MtV^* .

$$9 \ll :^{\wedge 512} \quad ^{\wedge 512} \wedge \quad ^{\wedge 512}' \quad N \quad ^{\wedge 5J2} >$$

$$g_w(rt, m) = \mathbb{E}(LPS\{/?\odot N\},/n)\odot/?\odot iTi, \quad (8)$$

(.) = $Xp_{<_{13}}[tPSXIK_{12}]... tPSXI^{\wedge}tPSXI^{\wedge}Km).$

$$U_{512}', / = 1..... 13 \quad :$$

$$\quad \quad \quad ^{\wedge} \quad _{\cdot} \quad (9)$$

$$K_j-LPS(K^{\wedge \wedge}C^{\wedge}).i-2, ...,13.$$

8

-

$$V^* \quad IV \in \quad _{6'2} \text{ —} \quad \quad \quad - \quad (\quad) \quad \quad \quad -$$

8.1 1

:

$$\begin{array}{ll}
 1.1 \text{ —} & / \gg := IV: \\
 1.2 \text{ —} & N := 0^{S12} \quad V_{512}:
 \end{array}$$

- 1.3 — $\mathbf{E} \leftarrow \mathbf{V}_{512}^{512}$;
- 1.4 — 2.
- 8.2 2
- 2.1 — $|\mathbf{E}| < 512$.
- 3.
- 2.2 — \mathbf{V}_{512} : - 2.2—27;
- 2.3 — $hg_M(h, \mathbf{E})$;
- 2.4 — $NVec_{512}(Int_{512}(W)m512)$;
- 2.5 — $\mathbf{E} := Vec_{512}(Int_{512}\{\mathbf{E}\}BInt_{512}\{m\})$;
- 2.6 — $:=$ ';
- 2.7 — 2.1.
- 8.3 3
- 3.1 — $0^{511} \ll ||1||$;
- 3.2 — bg^Ah, \mathbf{E}):
- 3.3 — $NVec_{512}(Int_{512}(W)ffl|A4|)$;
- 3.4 — $\mathbf{E} := Vec_{512}\{1, \dots, 2\}(\mathbf{E}) \cup Intern\}$;
- 3.5 — bg^Ah, N);
- gAh, \mathbf{E}).
- $MSB_{256}\{g_0(rt, \mathbf{E})\}$, - 512 .
- 256 ;
- 37 — h . 3.6, ().

()

.1

$$\mathbf{V}'' = \mathbf{V}_{4n} \mathbf{a}_{n1} \dots \mathbf{e}_Q$$

.2 1

.2.1

- 32313039383736353433323130393837363534333231303938373635343332
3130393837363534333231303938373635343332313039383736353433323130.

.2.2 - 512

□

***h-sfV-ffi*¹²;**

N:- 512.

2:- *2

IM,! = 504 < 512.

:= 0132313039383736353433323130393837363534333231303938373635343332

3130393837363534333231303938 73635343 323130 9383736353433323130.

$$:= LPS\{h \text{ @ } N\} = LPS(0^{s_{12}}).$$

5:

**S(A W) = fddddddddddddddcfdddcfcfddcfdddc
fdddddcfdddddccfcfdddddcccccfddddc.**

P:

**PSih © N) = fdddddccccfddddddddddddddddccfc
fddddddddddddddddccccfdddddddc.**

L

:« LPS(h W) - b383(c2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574
b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574.

$E(\text{ . m})$:

1

, - b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574
b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574.

XIK,Xm) = b2Mcd1ef7ec924286b7d1dfe49c4c84b5c91afde694448abbcM8fbe09646
82b3c516f9e2904080b1od1ef7ec924286b7cf1cRe49c4c84b5c91afde69444.

SXIX.J(m) = 4645d95fc0beec2c43218914b62d4efd3e5e37f14b097aead67de417c220b048
2492ac996667e0ebdf45d95fc0beec2c43218914b62d4e(d3e5e37ri4b097aea.

FSXJKJf/n) = 46433ed624d1433e452f5e7d92452(5ed98937e4acd989375f14f117995f14f1
C0b64bc266c0b64bbe2d092067be2d09ec4e7ab0e0ec4e7a2cfdea48eb2ddea.

LPSXVqKm) = e60059d4d8e0758024c73f6f3183653f56579189602ae4c21e7953ebc0e212a0
Ce78a8df475c2(d4fc43fc4b71c01e35be465fb20dad2d690cdf65028121bb9.

, Cy - 028ba7f4d01e7f9d5848d3af0eb1d96b9ce98a6de0917562c2cd44a3bb516188
f8 ff 1 c bcf 5cb3cc7511 c 1 d6266ab47661 615881802a0e8576e0399773c72e073.

S(K, C₁) - ddf644e6e15c5733bff24941044553614e9bd69e20013596b3d9ea737d70a1d7d1b6143b9c928835775Bf8er78278aa15514d717dda7cM2b211e87e7f19203d.

PS(K, C₁) = ddbf4eb3d17755b26f6d9bd9b65814114449d6ea14f8d7e8e6419e733bef177e
e104207d9c78dd7f5f450f709227a719575335a1888acb20336f96d735a1123d.

LPS_fKy CJ - d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c186be14f0b2da27973569od2ba051301036f728bd1d7eec3314d18af70c46d1e.

2

„ = d0b00807642fd78f13f2c3ebc774e80de0©902d23aef2ee9a73d010807dae9c1
88be14f0b2da27973569cd2ba051301036(728bd1d7eec33f4d18af70c46cf1e.

LPSXV^ILPSXIK^m) - 18e77571e703d19648075c574ce5e50e0480c9c5b9f21d45611ab86cf32e352a
d91854ea7dF8f863d46333673f62ff2d3efae1cd966f8e2a74ce499O2799aad4.

3

- 9d4475c7899f2d0bb0e8b7dac6ef6e6b44ec 6716d3a0f16681105e2d13712a
1a9387ecc257930e2d61014a1b5c9fc9e24e7d636eb1607e816dbaf927b8fca9.

LPSX|X;j... tPS^KJCM) = 03dc0a9c&4d42&43ocdb62960dS8c17e0bSb805d08a07406ece679d5f82b70(e
a22a7ea56e21814619e8749b308214575489d4d465539852cd4b0cd3629bef39.

4

= 5c283daba5ec1f233b8c833c48e1c670dae2e40cc4c3219c73e58856bd96a72f
df9f8055ffe3c004c8cde3b6bf7ef9sf3370d0a3d6194ac5782487defd83ca0f.

LPSXIKJ ... LPSXIK^Km} = dbec312ea7301b0d6d13e43855e85db81608c780c43675bc93cfd82c1b4933b3
&98a35b 13e1878abe119e4dff9d©4889738ca74d064cd9eb732078c1 fb25eO4.

5

X₆ = 109F33282731f9bd569cbc9317baa5S1d4d29&4fa18d42c41fab4e37225292ec
2fd97d7493784779046388469ae195c436fa7cba93f8239ceb5ffc818826470c.

LPSXIXj]... LPSXIKJH) - 7fb3f15718d90e889f9fb7c38fS27bec861c298arb9186934a93c9d96ade20df
109379bb9c1a1ffd0ad81fce7b45ccd54501e7d127e32874b5d7927b032de7a1.

6

X₅ = b32c9b02667911cf6(Ba0877be9a170757e2S026ccf41e c6b5da7(X)1b87474
3e1135cfbefe244237555c676c153d99459bc382573aee2d85d30d99f286c5e7.

LPSX|XJ ... LPSW^Rm) = 95efa4e104f235824bae5030fe2d0f170a38de3c9b8fc6d8fa1a9adc2945c413
389a121501fa71a65067916bOc06f6b87ce18de1a2a9BeOa64670985M7d73f1.

7

, - 8a13c1b195fd0886ac49989e7d84b08bc7bOOe4Df62765ace6050fcbabdc234
6c8207594714e8e9c9c7aad694edc922d6b01e17285eb7e61502e634559e32f1.

LPSXIX?]... LPSXIX,](m) = 7ea4385f7e5e40103bto25c67e404c7524eec43e33b1d065574e9c6049854304
32b43d941b77ffd476103338e9bd5145d9c1e18b1f262b58a81dcefff6fc6535.

8

K₆ = 52cec3b11448bb8617d0ddfb9c926f2e88730cb9179d6decea5acbfdd323ec376
4c47f7a9e13bMdb56c342034773023d617fF01oc546728e7ldff8de5d128cac.

LPSXtKf] - LPSXtXJfm) = b2426da0e58d5cfe898c36e797993f902531579d8eoc59f8dd8a&0802241a456
1f290cf992eb398894424bf681&36968c167e870967b1dd9047293331956daba.

9

X_g = f38c5b7947e7736d502007a05ea64a4eb9c243cb82154aa138b963bbb7f28e74
d4d710445389671291d70103f48fd4d4c01fc415e3fb7dc61c6088afa1a1e735.

LPSXJXg]... LPSXIXJfm) = 5e0c9978670b25912dd1ede5bdd1cf18ed094d14c6d973b731d50570d0a9bca2
15415a15031fd20ddefb5bc61b96671d6902f49df4d2fd346ceebda9431cb075.

10

X₁₀ = 0740b3(aa03ed39b257dd6e3db7c1bf56b6e18e40cdaabd30617cecbadd618e
a5e€1bb46&4S99S81dd30c24c1ab877ad0687948286cfefaa7eef99l6068b315.

LPSXIXfJ ... LPSXIXJf/n) - Clddd840fe491393a5d460440e03w451794e792c0c629e49ab0c1001782dd37
691cb6896f3e00b877f1d37a584c35b9cd8789fad55a46887e5b60e124b51a61.

11

X_„ = 1&5811cf3c2633aec8cfdfcae9dbb29347011bf92b95910a3ad71e5fca678e45
e374f088f2e5c29496e9695ce6957837107bb3aaS6441af11a82164893313116.

LPSXJXnJ... LPSA|X,|<m) = 3f75beaf2911c35d575088e30542b689c85b6M607f8b8004Q5941f5ab704284
7b9b08b58b4ibdd6154ed7b366fd3ee778ce647726ddb3c7d48c8ce8866a8435.

12

**K₁₂^s 9d46bf66234a7ed06c3b2120d2a3115e0fedd87189b75b3od21206906b5ee00d
c9a1eab80db8cc5760b251f4db5cde14270521a345613fd076451901279ee4c.**

LPSX|K₁₂1... LPSXIKJH) Sf35b0d889eadfcff73b6b17f33413a97417d9610c4cc9d30cda8ebb7dod5d1b0
61e620bec75b367370605f474ddc006003bec4c4d7ce59a73fbe766934c55a2.

13

```
,= 0179104026b900d8d768b6e223484c9761e3c585b3a405a6d2d8565ada926c31
7782e1127cd6b98290bt612558b4b60aa3cbc281d94f95460d76b621cb45be70.
```

XIK₁₃]... LPSXIK,Km) = 1c221dc8b814fc27a4de079d10097600209e5375776898961170bde0647bd81
1664cfa8bb8d8ff 1 e0df3e621 568b66aa075064b0e81 oce 132c8d 1475809ebd2.

g^{fi-1}):

h = fd102cf8812ccb1191ea34a12139413817a86641445aa9a626488adb33738ebd2754f6908cbbbac5d3ed01522c50815c954135793fb11Sd905fee4736b3bdae2.

***N* £:**

N - 00
00118,
I= 0123213039383736353433323130393837363534333231303930373635343332
3130393837363534333231303938 73635343332313039383736353433323130.

g^h, N):

***h* - 5c881fd924695cf196c2e4fec20d14b642026f2a0b1716ebaabb7067d4d597523d2db69d6d3794622147a14119a66e719037e1d662d34501a8901a5de7771d7c.**

$g^h.l$):

**b^s 486 4c1917879417fef082b3381a4e211c3241074654c38823a7b76f830ad00
fa11bae42b1285c0352f227524bc9ab16254288dd6863dccc5b9>54a1ad0541b.**

—

;

H(M₁)-486164c1917879417fe1082b3381a4e211c324f074654c38823a7b76f83OadO0
ra11bae42b1285c0352f227524bc9ab16254288dd6863dccc5b9f54a1ad0541b.

.2.3

- 256

•

•

h:= (00000001)*•;

$$W := 0^{S12};$$

2: «0*

 $|4| = 504 < 512.$

=

:=0132313039383736353433323130393837363534333231303938373635343332
0393837363534333231303938373635343332313039383736353433323130.

$LPS\{h < N\}^s LPS(\{000000001J^{\otimes 4}\})$.

S:

$S(h \text{ \$})N =$ ^^^BWWW ^ 9^^ WWw WVWW ^49 WVWW ^49 BwveVWf ^^7^49 wVv.

P:

|w| > «|* **/

^^BWW ^49^49 ^49 ^49 W WV ^49 ^^BWW ^49 wwwvVWrWJ vwsWe ^49 «WWW ^49 ^49 WV.

L'

LPS(h @N)= 23c5ee40b07b5f1523c5ee40b07b511523c5ee40b07b511523c5ee40b07b5f15
23c5ee40b07b511523c5ee40b07b511523c5ee40b07b5f1523c5ee40b07b5115.

 $E(K.m):$

1

- 23c5ee40b07b511523c5ee40b07b511523c5ee40b07bS11523 5 40 07 5115
23c5ee40b07bS11523c5ee40b07b511523c5ee40b07b5f1523c5ee40b07b5115.

1 ,|/) = 22f7df708943682316f1dd72814b662d14f3db7483496e251afdd976854f6c27
12(5d778874d6a2110f7df708943682316f1dd72814b662d14f3db7483496e25.
SXIK,(m) = 65c061327951f35e99a6d819f5a29a0193d290ffa92ab25cf14b538aa8oc9d21
f0l4fe6dc93a7818©9c061327951f35a99a6d819f5a29a0193d290ffa92ab25c.
PS-Xp^ftm) = 659993f1f0e99993c0a6d24b14c0a6d261d89053fe61d8903219ff8a6d3219ff
79f5a9a8c979f5a951a22acc3a51a22af39ab29d78f39ab25a015c21185a015c.
LPSXIK^nr) = e549368917aOa2611d5e08c9c2Fd5b3c563f18cOf68c410d84ae9d5fbdfb9340
55650121b7aa6d7b3e7d09d46ac4358adaa6ae44fa3b0402c4166d2c3eb2ef02.
, C, - 92cdb59aaeb185Fcc80ac1c1701e230aOcaf98039e3e8f03528bS6cdc5fa9be9
68b90ed1221c36148187c448141b8c0026b39a767c0f1236fe458b1942dd1a12.
S(K., C,> = ecd95e282645a83930045858325f5afa2341dc110ad303110ef676d9ac&3509b
13a3041b65148f93(5c986f293bb7cfcef92288ac34df08f63c8f6362cd8f1f0.
PSJK, C,) = ec30230ef3f5ef63d90441f6a3c992c85e58dc76048628f6285811d91bf28a36
26320aac6593c32c455ld36314bb4dd8a85a03508f7cf0f 139fa 11 9b93c8ff0.
LPS(K, ,) = 18ee8f3176b2e6a3bd6cb8233694cea349769df88be26bM51cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9.
2
Kg - 18ee8f3176b2e6a3bd6cb8233694cea349769df88be26W451cfab6a9O4a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9.
LPSXIKJtPSXIK,(m) = c502dab7e79eb94013fcd1ba64def3b916f18b63855d43d22b77fca1452f9866
C2b45089c62e9d82edf1ef45230db9a23c9e1c521113376628a5f6a5dbc041b2.
3
K.^ - aaa4cf31a265959157aec8ce91e7fd46W27dee21164c5e3940bba1a519e9d1f
Ce0913f1253e7757915000cd674be12cc7f68e73ba26fb00fd74af4101805f2d.
tPSXp<y... LPSXIKJf(n) = 8e5a4fe41fc790af29944f027aa2f10105d65cf60a66e442832bb9ab5020dc54
772e36b03d4b9aa471037212cde9337S226S52392ef4d83010a007e1117a07b5.
4
K₄ = 61fe0a65cc177af50235e2afadded326a5329a2236747bf&a54228aaca9c4585
Cd801ea9dd743a0d98d01ef0602b0e332067fb5ddd6ac1568200311920839286.
LPSXtKJ... LPSXtKJcM) sdee0b40df69997afef726f03bdc13cb6ba9287698201296f2(d8284f06d33ea4
a850a0ff48026dd47c1e88ec813ed2eb1186059d&42d8d17f0Wa259e56655M.
5
= 998368514fd3636f1fd5abb751bf26a8e2934314aa2ecb3ee4693c86c06c7d4e
169bd540al75e1610a546acd63d960bad595394cc199bf6999a5d5309fe73d5a.
LPSXIKg)... LPSXp^Km) = 675ea894d326432e1af7b201bc369f8ab021 fa58da09678ffc08ef30db43a3
7f1f7347cb77da0 ba30c85848896c3bac240ab14144283518b89a33d0ca<07.
6
K_e = f05772ae2ce7f025156c9a7fbcc6b8fdf1e735d613946e32922994e52820ffea
62615d907eb0551ad170990a86602088af98c83c22cdb0e2be297c 13c0f7a 156.
LPSXIK_q] ... LPSXIKJpn) = 1bc204bf9506ee9b86bbcf82d254a112aea6910b6db3805e399cb718d1b33199
64459516967cee4e648e8cfbr81(56dc8da6811c469O91be5123e6a1d5e28c73.
7
= 5ad144c362546e4e46b3e7688829fbb77453e9c3211974330b2b8d0e6be2b5ac
c89eb6b35167M59b7b005a43e5959a651a9M8cfc8e4098fcf03d9b81crbb8d.
tPSXpt,... LPSXI^Km) - f30d791ed78bdee819022a3d78182242124efcdd54e203f23fb2dc7f94338ff9
55a5afc15Kef03165263c4fdb36933aa982016471fbac9419f892551e9e568b.
8
K_q = 6a6cec9a1ba20a8db64fa840b934352b518c638ad530122a&3332fe0b8efdac9
018287a5a9f509c78d6c746adcd5426<b0a0ad5790d<b73(c1(191a539016daa.
LPSX|K&J... LPSX^Km) = 1fc20f1e91a1801a4293d3f3aa9e91560fcc3810bb15f3ee9741c9b87452519f
67cb9145519884a24de6db736a5cb1430da7458e5e51b80ba5204ba5b2600177.

9

, = 99217036737aa9b38a8d66431705bd51f351531f94810fc5e35fa351ee9dd8bd6b4c9d580a224e9cd82e0e2069fc49ed367d5194374435382b8fb6a815dd0409.

LFSX[Kg]... LPSXIKJf/n) = 1a52f09d1e81515a36171e0b1a2809c50359bed9012e78cbd89b7d4afa6d046655c96bdae6ee97055cc7e857267c2cc126c8f5dd95ed58a9a66c12663bb28967.

10

X_{1y} - 906763c0fc89fa1ae69288d8ec9e9dda9a7630e8bfd6c3fed703c35d2e62aeaf
10b35d80a7317a7176f83022f2526791ca81df678fcb337bd741e5393ccb05d2.

LPSX[X₁₀]... LPSX[K_j](m) - 764043744a0a93687e65aba8cfc25ec8714fb8e1bdc9ae2271e7205eaaa577c1
83 7325 50 19bd2d56b061 b5de39235c9c9fd95e071 a 1 a291 a5(24e8c774.

11

X,, - 88ce996c63618e6404a5c8e03ee433854e2ae3eee68991bbbf3c29d38dad6e
d6a1dae9a6dc6ddf52ce34af272f96d3159c8c624c3fe6e13d695c0bfc89add5.

LPSXIX₁₁... LPSXIX₁}(m) = 9Mce8tt26b445cb288c0aeeccf84658eea91dbdf14828br7011Qa5c9bd146cd9
646350cff4e90e7b63c5oc325e9b441081935f282d4648d9584171860538103b.

12

X₁₂ = 3e0a281ea9bd46063eec55010057613a506aa16&cf82915776b9781ccaa32138b55130c79982ca45628e8365d8798477e75a49c68199112a1d7b5a01765512db.

LFSXIK₁₂... tPS^AK^Am) - 133aeecede251eb81914b8ba48dcbcb08a6tc63a292cc49043c3d3346b310829
a9cb71ec1T25ed2a91bdc18f649907c110cb76ff2e43100cdd4ba8a147a57215.

13

X₁₃ = K)b273409eb31aeb432fbae1867212262c84&422b6a92f93f6cbab54ed18b83
14b21cffc51e3la319R433e76ef6a(»Oe19t5e03c9071a11cf9eca06500W03.

Z.PSXIX, J ... LPSXIX,J(m) = e3889d8e409604531d26431450bb9d29e8a78e78024656697ca1698125ee83aa
bd796d133a3bd28988428cM12766d1a1e32831112d361ad21b2440122a5cdf6.

$g^h, m)$:

**$h = \text{e3bbadb178a13264c9137127608aa510de90ba4d30756658449651b611dbb199}$
 $8d48552a0c0ce6bcb71bc802a415b2d2a07M2c22e25794178570341096fdc7$.**

***N* i:**

[illegible]

£ - 0132313039383736353433323130393837363534333231303938373635343332
3130393837363534333231303938373635343332313039383736353433323130.

$g_v\{h, N\}$:

$h = 70f22bada4c1e18a6a56ec4b3f328cd40db8e1b18a9d5f711d5e1ab11191279d715aab7648d07eddW87dc79c80516e6Rcbc15678bOac29ea001a85c8173cc6.$

 $g_v(h, l):$

h - 00557be5e5841d52a449b16b0251d05d27f94ab76cbaa6da890b59d8e11e159d2068e482e2acf564eOe9795a51e4dd261f3f6679&5a21cc40ac8631faca1709a.

—

 M_y

—

) - 00557be5e5841d52a449b16b0251d05d27f94ab76cbaa6da890b59d8e11e159d.

.3.1

2

```

- 1be2e5f0eee3c820bba1aebef20ffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120ff10eeec201
  20fa121ee5e2202ce8f6f 3ede220e8e6eee 1 e81012d1202ce8f0f2e5e220e5d 1.

```

A.3.2

- 512

•

•

$$b = N = 0 \Rightarrow^2.$$
$$W := 5, 2,$$
$$i := 0^{512}$$

$|z_2| = 576 < 512.$

```
:= fbeafaebef20ffbf0e1e0f0f520e0ed20e8ece0ebe5f0f2f120ff10eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.
```

$$LPS(b, W) = LPS(5, 2).$$

\$:

**S[b N) = fddddcfdddddcccccfddddcfWdddddcccccf
fcdddddcccccccccccccfdfcfddddddcccccc.**

2

**$PS(h \otimes N) = f d d d d c f d d d d c f d c f d d d d d c f d d c f d d d d d d d c$
 $f d d d d d d d d d d d d c f d d d d d d d d d d d d d d c f d d d d c.$**

L:

**LPS(h W) = b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574
b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574.**

(.):

1

$\gamma_1 = \text{b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574}$
 $\text{b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574b383fc2eced4a574}.$

**^K,](fn) = 486906c521f45a8f43621cde3bf44599936b10c®253155B642a303de203885B5
93790ed02b3685585b750fc32cf44d925d6214de3c0585585b730ecb2d440a5.**

- f29131ac18e613035196148598e6c8e8de6fe9e75c840c432c731185f906a8a8
de5404e1428fa8W47354d408be63aecb79693857f6ea8bf473d04e48be6eb00.

PSXIKJf(n) = 1251de2cde47b74791966f735435963d3114e911044d9304ac85e785e140&5e4
18985d9428b7f8be6e684068fe66ee613c80ca8a83aa8eb03e843a8bfecbf00.

LPSXIK,_I(m) = 909aa733e1f52321a2fe35bib8f67e92fbc70e(544709d5739d8faaca4ad126e83e273745c25b7b8f4a83a7436f6353753cbbbe492262cd3a868eace0104af1.

K₁@C, s028ba714d01e7f9d584Bd3af0eb1d96b9ce98a6de0917562c2cd44a3bb516188
f8ff 1 cbf5cb3cc7511 c1 d6266ab47661 615881802a0e8576e0399773c72e073.

**S(K, ®C,) = dd1644e6e15f5733bff249410445536f4e9bd69e200l3596b3d9ea737d70a1d7
d1b6143b9c9288357758f8ef78278aa155f4d717dda7cM2b211e87e7f19203d.**

PS(K, C₁) = ddbf4eb3d17755b2f6f29bd9b&58f4114449d6ea14f8d7e8e6419e733bef177ee104207d9c78dd7f5f450f709227a719575335a1888acb20336f96d735a1123d.

LPSifii C₉) = d0b00807642fd76f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c188be14f0b2da27973569cd2ba051301036T728bd1d7eec33f4d18af70c46d1e.

2

K_s=d0b00807642fd78f13f2c3ebc774e80de0e902d23aef2ee9a73d010807dae9c188be14f0b2da27973569cd2ba051301036f728bd1d7eec33f4d18af70c46d1e.

LPSXIK₂]LPSXIK₁](m) = 301aadd761d13df0b473055b14a2f74a45f408022aecadd4d5f19cab8228883a021ac0b62600a495950c628354ffce1161c68b7be7e0c58af090ce6b45e49f16.

3

K₃ = 9d4475c7899f2d0bb0e8b7dac6ef6e6b44ed66716d3a0f16681105e2d13712a1a9387ecc257930e2d61014a1b5c9fc9e24e7d636eb1607e816dbaf927b8fca9.

LPSX|K,J ... LPSXI^Km) = 9b83492b9860a93cbca1c0d8e0ce59db04e10500a6ac85d4103304974e78d32259ceff03fbb353147a9c948786582df78a34c9bde3l72b3ca41b9179c2coeef3.

4

K_t - 5c283daba5ecH233b8c833c48e1c670dae2e40cc4c3219c73e58856bd96a72(df9f8055ffe3c004c8cde3b6bf7B(95f3370d0a3d6194ac57&2487defd83ca0l.

LPSXJKJ ... LPSXIK,Km) = e^{e36e0a1677cdea107ec3402170698a4038450dab44ac7a447e10155aa33ef1bdaf8f49da7b66f3e05815045fbd39c991cb0dc536e09505fd62d3c2cd00b0f57.}

5

**K_b -109f33262731f9bd569cbc9317baa551d4d2964fa18d42c41fab4e37225292ec
2fd97d7493784779046388469ae195c436fa7cba93f8239ceb5ffc818826470c.**

LPSAIKj!... XPSXy^Km)= 1c7c8e19b2bf443eb3adc0c787a52a173821a97bc5a58feaf58fb8b2786182916
dd5ff9c97865e08c1 66147392 578 21266e323a0aacedeec3ef0314 f517c6.

« = b32c9b02667911c1818a0877be9a170757e25026ocf41e67c6b5da70b1b87474
3e113Sdbefe244237555c676c1S3d99459bc382573aee2d8Sd30d99f286c5e7.

LPSXJKJ ... LPSXIK,Km) = 48fedc5b3eb77998fb39bfcccd128cd42fccb714221be1e675a1c6fdde7e31198b318622412af7e999a3ef145e6d61609af72ae5c2ff1ab7H3b37be7011ba2.

7

$K_v = 8a13c1M95fd0886ac49989e7d84b08bc7b0Oe4f3162765ece6050fcbabdc2346c8207594714e8e9c9c7aad694edc922d6b01e17285eb7e61502e634559e32f1.$

LPSXIK₇]... LPSXIK_l(m) = a48f8d781c2c5be417ae644cc2e15a9f01fcead3232e5bd53f18a5ab875cce1b8a1a400c/48521c7ce27fb1e944521b54de23118153b364ee633170a621Sa8a9.

8

= 52cec3MI44&bb8617d0ddfb926f2e88730cb9179d6decea5acbff323ec3764c47f7a9e13bb1db56c342034773023d617fT01cc&46728e71dff8deSd128cac.

LPSXtKeJ... LPSXtKJtm) = e8a31b2e34bd2ae21b0ecf29cc437c75c4d11d9b82852517515c23e81e906a451672779c 3087141f1a15ab57f96d7da &c7ee38ecJ25befbdef631216356ff59c.

9

Kq = 138 5 7947 7736 502007 05 64 4 9 243 82154 138 963 7128 74
d4d710445389671291d70103f48fd4d4c01fc415e3fb7dc61c6088afa1a1e735.

LPSXIKg]... LPSXIK^m) = 34392ed32ea3756e32979cb0a2247c3918e0b38d645Sca88183356bf8eS877e&
5d542278a696523a8036af011c2902e9cbcb585de803ee4d26649c9e1f00bda31.

10

K₁ = 0740b3faa03ed39b257dd6e3db7c1W56b6e18©40cdaabd30617cecbadd618e
a5e61bb4654599581dd30c24c1ab877ad0687948286c(efaa7eef99f6068b315.

LPSX1KJ ... LPSXIK,Xm)= 6a8243695O177fsa74cce6d5O7a5a64e54&8a318145&e3bdfbdbcb618Oc9707de
7ccb676dd809e7cb1eb2c9ebd016561570801a4e9ce17a438b&521214409bb5e.

11

K₁₁ = 185811cf3c2633aec8cfdcae9dbb29347011bf92b95910a3ad71e5fca678e45e374f088f2e5c29496e9695ce8957837107bb3aa56441at11a82164893313116.

LPSXIK,,]... LPSX[K,](zn) - 7b97603135e2842189b0c9667596e96b70472ccbc73ae89da7d1599c72860c285f5771088111b0f943d949f22f1413c991eafb51ab8e5ad8644770037765aec.

12

- 9d46b(66234a7ed06c3b2120d2a3f 15e0fedd87189b75b3cd21206906b5ee00d
C9a1eab8001b8cc5760b251f4db5cdef4270521a345613fd076451901279ee4c.

LPSX[K₁₂] - LPSXIK,Krn) - 39ec8a88db635b460a4321adf41fd9527a39a67f6d7510db5044f05e1af721db5cf976a726ef33dc4d1cda94033e741a463770861a5b25fefcb07281eed629c0e.

13

K₁₃ = 0f79104026b900d8d768b6e223484c9761e3c585b3a405a6d2d8565ada926c3f7782ef127cd6b98290b1612558b4b60aa3cbpc281d94f95460d76b621cb45be70.

X[K₁₃]... tPSXtK_J(m) = 36959ac8fdda5b9e135aac3d62b5d9b0c279a27364f50813d69753b575e0718a
b8158560122584464f72c8656b5317aec0bccaae7cfdcaa9c6719e312627227e.

 $gf/h, l$):

/ s Cd7 023121aa465e3bb4ocd9795395de2914e938f10(8e127b7ac459b0c517b
98ef779ef7c7a46aa7843b8889731f482e5d221e8e2cea852e816cdac407c7af.

***N* £:**

[illegible]

X = fbeafa«)ef20ffbf0e1e0f0520e0ed20e8ece0ebe5f012f120fff0eeec2011
20faf2fee5e2202ce8f6f 3ede220e8e6eee 1 e8f0f2d1202ce8f0f2e5e220e5d 1.

512.

[illegible]
$$)=$$

b - C544ae6efdf14404f089c72d5faf8dc6aca1db5e28577fc07818095f1df70661e8b64d0706811cf92dffbf8f96e61493dc382795c6ed7a17b64685902cbdc878e.

***N* X:**

IV =

[illegible]

£ = fbeafaebef20ffbf0e1e0f0f520e0ed20e8ece0ebe510f2f120ff0eeec20f1
201 af2fee5e2202ce8f6f3ede220e8e6eee 1 e810f2d 1202ee4d3d8d6d 104adf 1.

w):

h - 4deb6649fla5ca14163d9d3f9967fbbd6eb3da68f916b6a09M112518b81292b703dc5d74e1ace5bcd3458a143bb456e83732608812b5df14b183997a0b1ad8d.

$$_0\{ \cdot, X\}:$$

1?
7613966de4ee00531 ae6013b5a4718dae06915d512f 194996lcabi2622e6881 e.

□ □

**mtty - 28fbc9bada033b1460642bdcddb90c3fb3e5&c497ccd0f62b8a2ad4935e85K)3
7613966de4ee00531ae6013b5a4718dae06915d51211949961cabf2622e6681e.**

A.3.3

- 256

• •

$$h:=N=(00000001J^{64};$$
$$W := 0^{s'2}:$$

X := 512.

$$= 576 > 512.$$

```
:= fbeafaebef20fRbfOe1eOH)f52OeOed20e8eceOebe5fOf2ri2OfffOeeec2Of1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f012d1202ce8f0f2e5e220e5d1.
```

$$:= LPS(h \textcircled{R} N) = LPS \{ \{000000001 \text{ J}^{64}\}.$$

S:

S{ft © W) -

P

$$PS(h, N) =$$

L:

**LPS(h © N) = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5I1523c5ee40b07b5115
23c5ee40b07b5f1523c5ee40b07bSf1523c5ee40b07b5(1523c5ee40b07b5f15.**

$E(K.m)$:

1

X, = 23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15
23c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f1523c5ee40b07b5f15.

X|K₁|l(m)=d82f14ab5f5baOeed3240eb0455bWF8032d02a05b9eafe7d2e511b05e977fe4
03311cbe55997f39cb331dad525bb713cd2406b042aa7139cb351ca5525bbac4.

SXIK,J(m) = 8d4f93828747a7&c49e204adc8473bd11101dda7470a415b832b77ad5dbc572d
111 f14950ce8570be4aecd9f0e472fd2d9e231 ad2c38570be46a14000e47a586.

PSXIXfMm) = 8d49118311e4d9e44fe2012b1faee26a9304dd7714cd311482ada7ad959fad00
87c8475d0c0e2c0e47470abce&473847a73b4157572f57a56cd15b2d0bd20b86.

LPSXIXfXm) = a3a72a2e01b5e6f8126&12221ec037b0db972086a395a387a6084508cae13093
aa71d352dcbce288e9a39718a727f61d4c5da5d0bc10fac3707ood1271e45475.

- , © , = 92cdb59aaeM85fcc80ec1c1701e230aOcaf98039&3e8f03528b56cdc5fe9be9
68b90ed1221c36148187c448141b8c0026b39a767c0f1236fe458b1942dd1a12.
- $S(K, \odot)$ = ecd95e282645a83930045858325f5afa2341dc110ad303110ef676d9ac63509b
f3a3041b65148f93f5c986f293bb7cfcef92288ac34df08f63c8f6362cd8f1f0.
- $PS(K, \odot)$ = ec30230ef3f5ef63d90441f6a3c992c85e58dc76048628f6285811d91bf28a36
26320aac6593c32c455fd36314bb4dd8a85a03508f7cf0f139fa119b93fc8ff0.
- $LPS\{K_j \odot\}$ = 18e&8f3176b2ebea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19c7e6b5eea633511e611d68c8401bfcd0c7d0cc39d4a5eb9.
- 2
- K_2 - 18ee8f3176b2etoea3bd6cb8233694cea349769df88be26bf451cfab6a904a549
da22de93a66a66b19 7 6 5 633511 11068c8401bfcd0c7d0cc39d4a5eb9.
- $LPSXpyLPSX[K_1](m)$ = 9f50697Md9ce23680db1f4d35629778864c55780727aa79eb7bb7d648829cba
8674afdac5c62ca352d77556145ca7bc758679fbe1fbd32313ca8268a4a603f1.
- 3
- K_g = aaa4cf31a265959157aecfice91e7fd46bf27dee21164c5e3940bba1a519e9d1f
ce0913f1253e775791500Qcd674be12cc7f68e73ba26fbOOfd74af4101805f2d.
- $tPSXIKg]... LPSXIKJcM)$ = 4183027975b257e9bc239b75c977ecc52ddad82c091e694243c9143a945b4d85
3116eae14fd81b14bb47f2c06fd283cb6c5e61924edfaf971b78d771858d5310.
- 4
- K_4 = 61fe0a65cc177afS0235e2afadded326a5329a2236747bf8a54228aeca9c4585
cd801 ea9dd743a0d98d01 ef0602b0e3320<7<b5ddd6ac1568200311920839286.
- $LPSXIKJ \dots LPSXp<,](n)$ = 0368c884fcee489207b5b97a133oe39a1ebfe5a3ae3cccb3241de1e7ad72857e
76811d324f01fd7a75e0b669e8a22a4d056ce6af3e876453a9c3c47c767e5712.
- 5
- K_o = 9983685f4fd3636f1fd5abb75fW26a8e2934314aa2ecb3ee4693c86c06c7d4e
169bd540af75e1610a546acd63d960bad595394cc199bf6999a5d5309fe73d5a.
- $LPSXIKg]... LPSXIKJfm)$ = c31433ceb8061e46440!44e65553976512e5a9806ac9a2c771d5932d5f6508c5
b78e406c4efab98ac5529be0021 b4d58fa26fO1621 eb 10b4 3de4c4c47b63 15.
- 6
- K_e = f05772ae2ce7f025156c9a7fbcc6b8fdf1e735d613946e32922994e52820ffea
62615d907eb0551ad170990a86602088af98c83c22cdb0e2be297c13c0f7a156,
- $tPS^{\wedge}Ke] \dots LPSXIK,Xm>$ = 5d0ae97f252ad04534503fe5152e9bd07f483ee3b3d206beadc6e736c6e754bb
713f97ea7339927893eacf2b474a482cadd9ac2e58f09bcb440d36c2d14a9b6.
- 7
- K_7 = 5ad144c362546e4e46b3e7688829ft)b77453e9c3211974330b2b8d0e6be2b5ac
c89eb6b35167f159b7b005a43e5959a651a9b18cfc8e4098fcf03d9b81cfbb8d.
- $tPSX[K_7] \dots LPSXIK^{\wedge}m)$ = 859aa21e6ad3e330deedb9ab9912205c355b1c479fdfd89a7696d7de66fbf7d3
cec25879f7f 1 a8cca4c793d5f2888407aebc188bda375eae5B6a8cfd0245c317.
- 8
- K_8 - 6a6cec9a1ba20a8db64fa840b934352b518c638ed530122a83332fe0b8efdac9
018287e5a9I509c78d6c746adcd5426fb0a0ad5790dfb73fc1f191a539016daa.
- $LPSXIKJ \dots LPSXIKJf(n)$ = 9903145a39d5a8c83d28f70fa1fbd88f31b82dc7cfe17b54b50e276cb2c4ac68
2b4434163f214cf7ce6164a75731bcea5819e6a6a6fea99da9222951d2a28e01.
- 9
- K_g = 99217036737aa9b38a8d6643f705bd51f351531f948f0fc5e35fa35fee9dd8bd
bb4c9d580a224e9cd82e0e2069fc49ed367d5194374435382b8fb6a8I5dd0409.
- $LPSXIKg]... LPSXIK,KmJ$ = 330e6cMd04961826aa263f2328f15b4f3370175a6a9fd6505b286efed2d8505
f71823337eF71513e57a700eb1672a665578e45dad298ee2223d4cb3fda8262f.
- 10
- K_{tu} = 906763c0fc89fa1ae69288d8ec9e9dda9a7630e8bfd6c3fed703c35d2e62aeaf
f0b35d80a7317a7r76f83022f2526791ca8fdf678fcb337bd74fe5393ccb05d2.

tPSXIK₁₀... LPSXpqKm) = ad347608443ab9c9bbb64 33a5749ab85c45d4174bfd78f6bc79fc4f4ce9ad1
dd71cb2195b1cfab8dcaaf6f3a65c8bb0079847a0800e4427d3a0a815f40a644.

11

K_u - 88ce996c63618e6404a5c8e03ee433854e2ee3eee68991bbbf3c29d38dad6e
d6a1 dae9a6dc6ddf52ce34a(272196d3159c8c624c3fe6e13d695c0Wc89add5.

LPSXIK,,|... LPSXIK^m) a065c55e2168c31576a756c7ecc1a9129cd3d207f8M3073076c30e111fd5f11
9095ca396e91b78a2bf4781c44e845e447b8fc7Sb788284aae27S82212ec23ee.

12

**K₁₂ - 3e0a281ea9bd46063eec550100576f3a506aa168cf82915776b978fccaa32f38
b5Sf30c79982ca45628e8365d8798477e75a49c68199112a1d7bSa0f765Sf2db.**

LPSXIX₁₂J... LPSXIK₁(m) = 2a6549f7a5cd2eb4a271a7c71762c8683e7a3a90698Sd60f8fc86f64e35908b2
9f83b1 fe3c704f3c 116bdf660704f3b9c8a 1 d0531 baaffaa3940ae9090a33ab.

13

**K₁₃ = 10b273409eb31aebe432fbae1867212262c848422b6a92f93f6cbab54ed18b83
14b21cffc51e3fa319ff433e76ef6adbOef9f5e03c907fa1fcf9eca06500WQ3.**

X[K₁₃]... LPSXtM^m) s dad73ab73b7e345f46435c690f05e94a5cto272d242ef44f6b0a4d5d1ad8883318b31ad01f96e709f08949cd8169f25e09273e8e50d2ad05b5f6de6496c0a8ca8.

$g^h.m$):

**h - 203cc15dd55fcaa5b7a3bd98fb2406a67d5b9f33a80bb50540852b204265a2c1
aacaSefe1d8dS1b2e1636e34f5becc077d930114fefaf176b69c15ad8f2b6878.**

***N* l:**

[illegible]

X = R) eafae b ef20mbKle1e0f0t520e0ed20e8ece0ebe&roF2f120fff0eeec20f1
20faf2fee5e2202ce8f6f3ede220e8e6eee1e8f0f2d1202ce8f0f2e5e220e5d1.

512,

[illegible]

$g, /h, \):$

= a69049e7bd076ab775bc2873af26f098c538b17e39a5c027d532f0a2b3b56426
C96b285fa297b9d39ae6afd8b9001d97bb718a65fcc53c41b4ebf4991a617227.

***N* l:**

[illegible]

X = fbeafaebef20ffibf0e1e0(0f520e0ed20e8ece0ebe5f0f2H20fff0eeec20f1
20faf2fee5e2202ce6f6f3ede220e8e6eee1 e8f0f2d1202ee4d3d8d6d104adf 1.

(, N):

***h* - aee3bd55ea6f387bcf28c6dcdbdWb3ddacc67dcc13dbd8d548c6bf808111d4b75b8e74d2afae960&3&ae6a5f03575S59c9fd839783ffcdScf99bd61566b4818.**

£):

**h - 508f7e553c06501d749a66fc28c6cac0b005746d97537fa85d9e40904efed29d
C345e53d7f84875d5068e4eb743f0793d673f09741f9578471fb2598cb35c230.**

- **Mj** :

$H(\wedge) = 508f7e553c06501\ d749a66fc28c6cac0b005746d97537fa85d9e40904efed29d.$

- | | | | | | | |
|------|------------------------|--------------|---|---|---|---|
| | { | — | * | , | / | . |
| (1) | 2382:2015 | | | | | {Information technology — Vocabulary} |
| | (ISO 2382:2015) | | | | | |
| (2) | / | 9796-2:2010 | | | | 2. |
| | (ISO/IEC 9796-2:2010) | | | | | (Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms) |
| (3) | / | 9796-3:2006 | | | | 3. |
| | (ISO/IEC 9796-3:2006) | | | | | (Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms) |
| (4) | / | 14888-1:2008 | | | | 1. |
| | (ISO/IEC 14886-1:2008) | | | | | (Information technology — Security techniques — Digital signatures with appendix — Part 1: General) |
| (5) | / | 14888-2:2008 | | | | 2. |
| | (ISO/IEC 14688-2:2008) | | | | | (Information technology — Security techniques — Digital signatures with appendix — Part 2: integer factorization based mechanisms) |
| (6) | / | 14888-3:2016 | | | | 3. |
| | (ISO/IEC 14888-3:2016) | | | | | (Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms) |
| (7) | / | 10118-1:2016 | | | | 1. |
| | (ISO/IEC 10118-1:2016) | | | | | (Information technology — Security techniques — Hash-functions — Part 1: General) |
| (8) | / | 10118-2:2010 | | | | 2. |
| | (ISO/IEC 10118-2:2010) | | | | | (Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher) |
| (9) | / | 10118-3:2004 | | | | 3. |
| | (ISO/IEC 10118-3:2004) | | | | | (Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions) |
| (10) | / | 10118-4:1998 | | | | 4. |
| | (ISO/IEC 10118-4:1998) | | | | | (Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic) |

1—2019/65

«
»
»
»
»
»

05.12.201 . 09.01.2019. 60 « 84¹/g.
» . 2.79. .- . 2.24.
»

« » , 115419. , . . 11.
www.4ur1sizdal.ru y-book@mail.ru

« »

117418 . - , . 31. . 2.
www.90sbnfo.ru mfo@gosbnfo.ru

$\backslash A^v$