

( ) ,

INTERSTATE COUNCIL FOR STANDARDIZATION. METROLOGY AND CERTIFICATION  
(ISC)

**34,12—  
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 . N? 1061-

34.12—2018

1 2019 .

5 34.12—2015

6 28147—89 1 «

»

« », —

« », ( )

« », ,

—

(www.gost.ru)



1	.....	1
2	, .....	1
2.1	.....	1
2.2	.....	2
3	.....	3
4	-128 .....	3
4.1	.....	3
4.2	.....	4
4.3	.....	4
4.4	.....	4
5	- 64 .....	
5.1	.....	5
5.2	.....	
5.3	.....	5
5.4	.....	6
( )	.....	7
	.....	12

/ 10116 (1)

—

/ 18033 [2]. (3).

«

».

Information technology. Cryptographic data security.  
Block ciphers

— 2019—06—01

1

2

2.1

8

2.1.1

(encryption algorithm):

2.1.2

(decryption algorithm):

2.1.3

(basic block cipher):

2.1.4

(block):

2.1.5

(block cipher):

1

2

2.1.6 (encryption): , \*

— / 16033-1 (2).

2.1.7 (round key): ,

2.1.8 (key): ,

1 / 18033-1 (2).

2 ( ).

2.1.9 (plaintext): .

— / 10116 (1J).

2.1.10 (key schedule): .

2.1.11 (decryption): , .

1 / 18033-1 (2).

2

— ,

— ,

— « » « » „ « » ,

»

2.1.12 (symmetric cryptographic technique): -

— ,

— / 18033-1 (2).

2.1.13 (cipher): , -

— / 18033-1 (2).

2.1.14 (ciphertext): ,

— / 10116 (1J).

2.2

V\* —

V, — s. s — : -

t/x iv \_ ( ) U W, , | | = 0):

| | — ( ) V\* ( — ^ |4| |

|| — . Be V\*. .

V|<sub>8|</sub> ;

<\$\$\_{11} — 11 ,

: 2

<8 — 2

Z<sub>21</sub> — 2<sup>1</sup>.

— Z<sub>233</sub>;

F — GF(2)(x)/p(x), p(x)=x<sup>e</sup>+x<sup>7</sup>+x<sup>e</sup>+x + 1eGF(2)(x): F -

2<sub>0</sub> + z,G+-... + 2<sub>7</sub> -9<sup>7</sup>eF -

2 +2 • 2, ...+2<sup>7</sup> • 2<sub>7</sub>. 2, (0.1). /=0.1.....7.

( ). :

$\text{Vec}_s: Z_{2j} \rightarrow V_s$  — ,  $z \in Z_{j4}$   
 $2 = \wedge, +2z, +\dots + 2^s$   $z \in \{0,1\}, / = 0,1,\dots, s-1$   
 $\text{Vec}_s \langle z \rangle \langle z_{\#}, |z_t|z_0 \rangle$   
 $\text{Int}_s: V, -\wedge_2 s$  — ,  $\text{Vec}_s \dots \text{Int}_s a \text{Vec}/:$   
 $: V_8 \rightarrow F$  — » , « » »  $V \&$   
 $F$  :  $z_7$  I kh z.  $\{0,1\}, / = 0.1 \dots 7$   
 $Z_0 + z, 6 + \dots + z_7$   $F$ ;  
 $V: F \rightarrow V_{\&}$  — ,  $\dots ? = 1$ ;  
 $5$  — ,  $5$  ,  $1 =$  .

3

8

- 128 - 64 - 256 .

1 - 128  
 « » («Kuznechik»).  
 2 = 64  
 « » («Magma»).

4

= 128

4.1

4.1.1

$x = \text{Vec}_8 K' \text{Int}_8: V_8 \rightarrow V_8$   $x': Z^{\wedge} \rightarrow Z$  \*  
 $' = ( '( ) \dots \dots \dots \cdot (255))$ :

$' = \{252. 238. 221. 17. 207, 110, 49. 22, 251. 196. 250, 218, 35. 197. 4. 77. 233. 119, 240. 219, 147,$   
 $46. 153. 186, 23. 54. 241. 187, 20. 205, 95, 193, 249. 24. 101, 90. 226, 92. 239. 33, 129, 28. 60. 66.$   
 $139. 1, 142, 79. 5, 132, 2, 174. 227, 106. 143. 160, 6, 11, 237. 152. 127. 212. 211. 31. 235, 52. 44, 81.$   
 $234. 200. 72, 171, 242, 42, 104, 162. 253. 58. 206, 204, 181, 112, 14. 86. 8. 12. 118, 18. 191. 114. 19.$   
 $71. 156. 183. 93, 135, 21, 161, 150. 41, 16. 123, 154. 199. 243. 145. 120. 111, 157, 158, 178, 177, 50.$   
 $117. 25. 61. 255, 53. 138, 126, 109. 84. 198. 128, 195. 189. 13. 87. 223, 245. 36. 169. 62. 168. 67.$   
 $201. 215, 121, 214, 246, 124. 34. 185. 3. 224. 15. 236. 222. 122, 148. 176, 188. 220. 232. 40, 80, 78.$   
 $51. 10. 74. 167, 151. 96. 115, 30. 0. 98. 68. 26. 184, 56. 130. 100, 159. 38. 65. 173, 69. 70. 146, 39.$   
 $94. 85. 47, 140, 163, 165. 125, 105, 213, 149. 59. 7. 88. 179. 64. 134, 172. 29. 247. 48. 55. 107, 228.$   
 $136. 217, 231, 137, 225. 27, 131, 73. 76. 63. 248. 254. 141. 83. 170, 144. 202. 216, 133. 97. 32. 113.$   
 $. 164. 45. 43. 9, 91. 203, 155. 37. 208. 190, 229. 108. 82. 89. 166, 116. 210, 230. 244. 180. 192.$   
 $209. 102, 175. 194. 57. 75. 99, 182).$

4.1.2

$I: V_8 \rightarrow V_8$   
 $:$   

$$\begin{aligned}
 & / ( \text{ }_{16} \dots \wedge ) = 7(148 ( \text{ }_{16} ) + 32 ( \text{ }_{14} ) + 133 ( \text{ }_{13} ) + 16 ( \text{ }_{12} ) + \\
 & + 194 ( \text{ }_{11} ) + 192 ( \text{ }_{10} ) + 1 ( \text{ }_9 ) + 251 - \{ \text{ }_8 \} + 1 ( \text{ }^{\wedge} ) + 192 ( \text{ }_8 ) + \\
 & + 194 ( \text{ }_5 ) + 1 ( \text{ }_4 ) + 133 ( \text{ }_3 ) + 32 ( \text{ }_2 ) + 148 ( \text{ }_1 ) + 1 ( \text{ }^{\wedge} )
 \end{aligned}
 \tag{1}$$

$, V_8, / = 0, 1 \dots 15,$   $F, *$

## 4.2

;

$$[ / 1 ( ) = \quad . \quad (2)$$

$$W - V_{126};$$

 $\wedge_{128} \gg 2$ 

$$S(a)=S(a_{16}|...|^{\wedge})=K(a_{15})|...|x(a_0). \quad (3)$$

$$a = a_{15}|...|a_0eV_{12a}, a,eV_a. \quad ....15:$$

 $\$ : \wedge_{128} \wedge \wedge_{128}$ 

S.

$$S-Xa)-S_{15}|...|_0) = \quad_{15})|...|| \quad ' \{ \quad ). \quad (4)$$

$$a_{15}|...|a_0eV_{12a}, a,eV_a./\ll \quad ...,15.$$

$$-1 - \quad , \quad ;$$

$$/?( \quad ) \quad /?( \quad , \quad 5 \quad || \quad | \quad >- \quad_{15}..... \quad | \quad (5)$$

$$a \gg a_{15}|...|a_0eV_{12a}, a,-eV_8, \ll 0 \quad ....15;$$

 $\wedge_{128} \text{***} \wedge_{128}$ 

$$) -R^{\delta}(a). \quad (6)$$

$$aeV_{t2a}:$$

 $* \quad_2 \quad - \gg \quad_{128}$ 

R,

$$R^{\wedge}a)=R'( \quad_{15}|...|_0)- \quad_{1(1|| \quad_1 \quad |...|_0)/( \quad_{14} \quad_{13}..... \quad_0 \quad_{15}). \quad (7)$$

$$a = a_{15}|...|a_0eV_{12a}, \quad , \quad / . \quad ....15:$$

 $1:\wedge_{12} \text{**} \wedge_{128}$ 

$$\pounds'( \quad ) \quad ( \quad ')| \quad ( \quad ), \quad (8)$$

$$asV_{12a}:$$

 $F[A]: \quad V'_{t2a}xV'_{12a}-$ 

$$, . \quad . (\pounds SXM(a, ) \odot . \quad , ). \quad (9)$$

$$k.a^{\wedge}a^{\wedge}V^{\wedge}.$$

 $,_{28} \quad \wedge_{128}$ 

## 4.3

$$,eV_{t2a} / .1 \quad 2.....32.$$

:

$$C_f \ll \pounds (Vec_{128} \ll / > ), / -12.....32. \quad (10)$$

$$_{12}, =1 \quad 2.....10.$$

 $\text{**}25\$|$  $\wedge_{2se}-$ 

$$0 \quad ...,255.$$

$$*1 \quad \text{"} \quad 25 \quad | \quad -|^{ft} \wedge_{128}:$$

$$2 \quad_{127}|...|_0: \quad (11)$$

$$\langle K2^{\wedge}.K2M2 \rangle = HC_{e|j-|M}^{\wedge}!.. F[C_{8( \quad -1)n} KX_{2l}, K_{2l}).MIZ3.4.$$

## 4.4

## 4.4.1

$$_{28}, / = 12,....10.$$

 $\wedge \quad ,$ 

128

$$, \quad ... \ll_{10}(a)=X(X_{10})\pounds SX[K_9]... \pounds SXIX_2 \pounds SX[K_1](a). \quad (12)$$

 $V'_{128}.$



## 4.4.2

 $D_K^\wedge$  , $V_{528}$ ,  $V_{128} / = 12 \dots 10$ ,.....^ ( )-XIKJS 'L 'XP^I-.S 't 'Xp^IS .-' [ <sub>1(></sub> >.

&lt;«)

 $a_{fe} V_{128}$ 

## 5

- 64

## 5.1

## 5.1.1

.  $\text{Vec}_4 n! \text{Int}_d$ :  $V_4 \rightarrow V_4$ .  $' : 2_2, \rightarrow 2_{|4}$  , / 0.1.... 7.  
- «{ '(0), '(1)..... '(15)),  $i \gg 0.1 \dots 7$ :

£ «(12. 4. 6. 2 10. 5. 11. 9.14. 8.13. 7. 0. 3.15. 1);  
; «(6. 8. 2. 3. 9. 10. 5.12 114. 4. 7. 1 13. 0.15);  
' ( . 5. 8. 2 15. 10.13. 14. 1 7. 4.12. 9. 6. 0);  
<sub>3</sub> =(12. 8. 2. 113. 4.15, 6. 7. 0. 10. 5. 3.14. 9, 11);  
'<sub>4</sub> «(7. 15. 5. 10, 8. 1 6. 13. 0. 9. 3. 14. 4. 2. 12);  
£ »(5. 13. 15. 6. 9. 2. 12. 10. 11 7. 8. 1. 4. 3. 14. 0);  
; «(8. 14. 2 5, 6. 9. 1. 12 15. 4. 11. 0. 12 10. 3. 7);  
; »(1 7. 14. 13. 0. 5. 8. 3, 4.15. 10. 6. 9. 12. 11 2).

## &amp;2 ^

:

 $t: V_{32} \rightarrow V_{32}$  $f(a) = ((\gamma | \cdot |) \gamma (\gamma)^\wedge \cdot | \gamma (0) \cdot$ 

(14)

 $\gamma | \dots | ^\wedge V_{32} \cdot a \cdot V_4 / \otimes 0.1 \dots 7;$  $9[AJ: V_{32} \rightarrow V_{32}$  $[ft] < ) = (f(\text{Vec}_{32}(\text{Int}_{32} ( ) \text{Int}_{32} ( ) \gg) \ll ,$ 

(15)

 $\cdot 32;$  $G[A]: V_{32} V_{32} \rightarrow V_{32} V_{32}$  $G[ , a_0) 8(a^\wedge, . g[AHa_0) \otimes a,).$ 

(16)

 $A. a^\wedge \cdot a, eV_{32};$  $G'[A1: V_{32} \times V_{32} \rightarrow V_m$  $G'[*](a_1, a_0) 8(\text{ff}[Al(a_0) \otimes a_1]) a_0.$ 

(17)

 $A. s(j, a, e V_{32}.$ 

## 5.3

 $32, / = 12 \dots 32$  $s_{25} | \dots | 0_{25} , ; , / 0.1 \dots 255,$ 

:

 $*1 \quad *255 || '1 *224:$  $2 \quad 8 \quad 223 \quad 1 \quad | \quad 192;$  $*3 \quad " *19i | - | *ieo:$  $^4 \quad " *15\$ | - | *125:$  $^5 = *12? \quad 11 *9 :$  $*6 \quad " \quad *95 \quad * \quad 4:$

? “\* || 2:

..... 8;

1 \* (’

“„24- 9.,-1-12..... 8.

5.4

5.4.1

,  $V_{32'}$  / 12..... 32.

$V_M$

$$^EK_{\vartheta} \cdot \chi_{3J}(a) = G^*[K_{32}|G[K_{31}|...G[K_2]GIK_1|](a_1 \cdot a_0). \quad (19)$$

,|  $_0$   $V^{\wedge}.a$ ,  $V_{32}$ .

5.4.2

,  $V_{32'}$  / 12, ...,32.

$D_K \cdot 1', 32$

$V_M$

$$D_{K1'.....K_{32}}(a)=G^*[K_1|G[K_2]...GIK_{31}]GIK_{32}J(a_1 \cdot a_{(>}). \quad (20)$$

,|  $V^{\wedge}. Aj.a$ ,  $V_{32}$ .

( )

**.1**

■

—

$$V^*_{41} = \frac{V^*_{41}}{V^*_{41}} = 1$$

( .... 9. . 6. , d. , 7), / = 0 ...., -1. 4 -  
1 ( . .1). , -  
4 . -

.1 —

	*		*		*		-
0000	0	0100	4	1000	8	1100	
0001	1	0101	5	1001	9	1101	d
0010	2	0110	6	1010		1110	
0011	3	0111	7	1011		1111	f

$$.2 \qquad \qquad \qquad = 128$$

**.2.1** **S**

S(ffeeddcbbbaa99881122334455667700) = b66cd8887d38e8d77765aeaa0c9a7efc.  
S(b66cd8887d38e8d77765aeaa0c9a7efc) = 559d8dd7bd06cbfe7e7b262523280d39.  
S(559d8dd7bd06cbfe7e7b262523280d39) = 0c3322fed531e4630d80e15c5a81 cSOB.  
S(0c33221ed531e4630d80ef5c5a81cSOB)\*23ae6S633f842d29c5d(529c13r5aoda.

### A.2.2

[illegible]

**A.2.3** *L*

L(64aS94000000000000000000000000000000) = d456584dd0e3e84cc3166e4b7fa2890d.  
L(d456584dd0e3e84cc3166e4b7fa2890d) - 79d26221b87b584cd42(bc4ffea5de9a).  
L(79d26221b87b584cd421bc4ffea5de9a)\*0e93691a0cfc60408b7b68f66b513c13.  
L(0e93691a0cfc60408b7b68f66b513c13) = 6 8094( 204 97 44 8580.

### A.2.4

```

=8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.
, = 8899aabbccddeeff0011223344556677.
=fedcba96765432100123456789abcdef.

```

, s6ea276726c487ab85d27bd10dd849401.

$X[C_i](X_i) = e63bdcc9a09594475d369f2399d1f276,$

$SX[C_i](K_i) = 0998ca37a7947aabb78f4a5ae81b748a.$

$LSX^{RX_i} = 3d0940999db75d6a9257071d5e6144a6.$

$HCJK_i, K_2) = (c3d5fa01ebe36f7a9374427ad7ca8949, 8899aabbccddeH0011223344558677).$

$C_2 = (Jc87ece4d890f4b3ba4eb92079cbeb02.$

$F(C_2)F[C_i](K_i, K_2) = (37777748Q56453377d5e262d9O9O3f87. c3d5fa01ebe36f7a9374427ad7ca8949).$

$C_3 = 2259\ 96\ 4\ 88\ 0\ 7690430\ 44\ 7,$

$F(C_3) \dots F[C_i](X_i, X_2) = \{f9eae5f29b2815e31M\ 1ac5d9c29fb01. 37777748e56453377d5e262d90903f87\}.$

$C_4\ s7bcd1b0b73e32ba5b79cb140f2551504,$

$F[C_4] \dots F[C_i](X_i, X_2) = (e98OO89683d00d4be37dd3434699b98f. f9eae5f29b2815e31f11ac5d9c29fbO1).$

$C_5 = 156f6d791fab511deabb0c502(d18105.$

$F[C_5] \dots F[C_i](K_i, K_2) = \{b7bd7Oacea44\&O714f4ebe13e35croO4.098OO89\&83dOOd4be37dd3434699b98f\}.$

$C_6 = a74ar7\&fab73df160dd208608b9efe06.$

$F(C_6) \dots F[C_i](X_i, X_2) = (1a46ea1cf6ccd236467287df93fdf974.b7bd70acea4460714\>4ebe13835cf004).$

$C_j = C9e8819do73ba5ae50f5b570561a6a07.$

$F[C_j] \dots F[C_i](X_i, X_2) = (3d4553d8e9cfec6B15ebadc40a9ffd04.1a46eatcfeccd236467287df93fdf974\>.$

$C_8 = f6593616e6055689adfa18027aa2a08.$

$(X_3, X_j) = F[C_8] \dots F[C_i](K_i, X_2) =$

$(db31485315694343228d6aef\ 8cc78c44.3d4553d8e9cfec6815ebadc40a9ff\ d04).$

$X_i, i = 1.2 \dots 10. :$

$X_i = 8899aabbccddeK0011223344556877,$

$_2 = (edcba98765432100123456789abcdet$

$_3 = db31485315694343228d6aef8cc78c44.$

$_4 = 3d4553d8e9cfec6815ebadc40a9ffd04.$

$X_5 = 57646468c44a5e28d3e59246f429f1ac,$

$X_6 = bd079435165c\<432b532e82834da581b,$

$X_7 = 51e640757e8745de705727265a0098b1.$

$X_8 = 5a7925O17b9fdd3ed72a91a22286f9\&4.$

$X_9 = bb44e25378c73123a5f32f73odb6e517.$

$X_{10} = 72e9dd7416bcf45b755dbaa88e4a4043.$

AJ.5

.2.4.

» , ,  
=1122334455667700feeddccbbaa99&8.

$SXfX, 1(a) = \&87de8b6e87de8b6b6b6b\<b6b6b6b6b6,$

$LSX(X, J(a) - 297\ 686\ 355\ 0\ 1\ 4\ 2\ 9249140830.$

$tSX(X_2)Z.SX(X, Ke) = 285e497a0862d596b36f4258a1c89072.$

LSX[K<sub>j</sub>]...LSX[X<sub>i</sub>](a) = 0187a3a429b567841ad50d29207cc34e,  
 LSX[KJ...LSX[K<sub>i</sub>Xa) = ec9bdba057d4f4d77c5d70619dcad206.  
 LSX[K<sub>s</sub>]...LSX(K<sub>i</sub>Ka) = 1357fd11de9257290c2a1473eb6bcde1.  
 LSX(K<sub>6</sub>J...LSX(K<sub>i</sub>Ks) = 28ae31e7d4c2354261027ef0b32897df.  
 tSX[K<sub>7</sub>]...LSX[K<sub>i</sub>]<a) = 07e223d56002c013d3f5e6f714b86d2d.  
 LSX[KJ...tSX[K<sub>i</sub>]<a) = cd8ef6cd97e0e092a8e4cca61b38bf65.  
 LSX[K<sub>5</sub>3...LSX[X<sub>i</sub>](a) = Od8e4Oe4a8OOdO6b211b370a3790ad8e.

b=X(K<sub>10</sub>]tSX[K<sub>9</sub>]...tSX[K,X3) = 7f679d90bebc24305a468d42b9d4edcd.

&\*

.2.4.

.2.5:

b - 7f679d90bebc24305a468d42b9d4edcd,

XfK, )= 0d8e40e4a800d06b2f1 b37ea379ead8e.  
 L-'XIK^Kb) = 8a6b930a52211b45c5baa43ff8b9l319.  
 S-'Z.'X(K<sub>0</sub>J(b>= 76ca149eef27d1b10d17e3d5d68e5a72.  
 S-'Z.-'X(K<sub>9</sub>]S-'L-'X[K<sub>10</sub>J(ti> - 5d9b06d41b9d1d2d04df7755363e94a9.  
 S VxfKeJ.-.S ' ' ( 10 ) = 79487192aa45709c115559d6e9280f6e.  
 S-i.-'X(K<sub>j</sub>]...S-'t-'X(K<sub>0</sub>K6) = ae506924c8ce331bb9iefc5bdfM95fa.  
 S-'L-'X(X<sub>6</sub>J...S-'t-'X(K<sub>0</sub>Kb)» bbfbbfc8939eaaHafb8e22769e323aa.  
 S-L'X(K<sub>5</sub>]...S-'L-'X(K<sub>10</sub>Kb) = 3cc2f07cc07a8bec0f3ea0ed2ae33e4a.  
 S-'t-'X(K<sub>4</sub>]...S-'i-'X(X<sub>10</sub>Kb) = f36f01291d0b96d591e228b72d011c36,  
 S-'L-'X(K<sub>3</sub>]...S-'t-'XfK<sub>16</sub>]<b) = 1c4b0c1e950182Mce696af5c0bfc5df.  
 S-'L'X(K<sub>2</sub>]...S-'e'X(K<sub>16</sub>Kb) = 99bb99ff99bb99ffffHWffWH.

= X[K,JS- 't-'XtXJ... S 'L-' | 1 \*>° 1122334455667700feeddccbbaa9988.

A.3 = 64

.3.1 t  
 f(fdb97531) = 2a196f34,  
 (<2a196f34) = ebd9f03a,  
 f{ebd9f03a) - b039bb3d,  
 f{b039bb3d) = 68695433.

A.3.2 g  
 g[87654321J(fedcba98) = fdcbc20c.  
 g[fdcbc20c][87654321>= 7e791a4b,  
 g[7e791a4bJ(fdcbc20c) = c76549ec.  
 g[c76549ecj(7e791a4b) = 9791c849.

A.3.3

:

- tfeeddccbbaa99887766554433221100KHH2f3t4f5i6f7f8f9fafWcfdfeH.

., / = 1.2.....32.				:
$X_1 = \text{ffeeddccc.}$	$X_9 - \text{ffeeddccc.}$	$K_{17} = \text{ffeeddccc.}$	$X_{25} = \text{fcfdfeff.}$	
$X_2 = \text{bbaa9988.}$	$X_{10} = \text{bbaa9988.}$	$X_{18} = \text{bbaa9988.}$	$X_{26} = \text{f8f9fafb.}$	
$X_3 = 77665544.$	$X_{11} = 77665544,$	$X_{19} = 77665544.$	$X_{27} = \text{f4f5f6f7.}$	
$X_4 = 33221100,$	$X_{12} = 33221100.$	$K_{20} = 33221100,$	$X_{28} = \text{f0f1f2f3.}$	
$X_5 = \text{fOf1f2f3,}$	$X_{13} = \text{f0f1f2f3.}$	$X_{21} = \text{f0f1f2f3.}$	$X_{29} = 33221100.$	
$X_6 = \text{f4f5f6f7.}$	$X_{14} = \text{f4f5f6f7.}$	$X_{22} = \text{f4f5f6f7.}$	$X_{30} = 77665544.$	
$K_j - \text{f8f9fafb.}$	$X_{15} = \text{f8f9fafb.}$	$X_{23} = \text{f8f9fafb,}$	$X_{31} = \text{bbaa9988.}$	
$X_8 = \text{fcfdfeff,}$	$X_{16} = \text{fcfdfeff.}$	$X_{24} = \text{fcfdfeff.}$	$X_{32} = \text{ffeeddccc.}$	

.3.4

= fedcba9876543210.

( , , « ) = &lt;fedcba98. 76543210).

 $G(X_1)(a_{11} \geq (76543210. 28da3b14).$  $G(X_2)G(X_1)(a_{10}) = (28da3b14. 14337 5).$  $<^{\wedge} ) \dots ( , , at_1 ) = ( 4337 5. 633 7 68).$  $Gp<_4] \dots G(X_1)(a_{11}) = \{633 7 68. 89 2 \},$  $G(K_8] \dots G(K_1Ka_{11}^{\wedge}) - ( 89 02 . 11 fe726d),$  $G(X_6) \dots G(X_1Xa_{11}^{\wedge}) = (11fe726d. ad0310a4),$  $G<K_7J \dots G(K_1Ka_{11}^{\wedge}) = (ad0310a4. 37d97f25).$  $\therefore \wedge , , ) \ll (37d97f25.46324615).$  $G\{K_8] \dots G(K_1He_1^{\wedge}) - (46324615, ce995f2a).$  $GfK^{\wedge}I \dots GIK^{\wedge}a_{11} a_{11}) = (ce995f2a. 93c1(449).$  $GfX_1, ) \dots G[K_1Ka_{11} a_{11}) = (93c1f449. 4811c7ad),$  $G(X_2] \dots G[X_1](a_1 a_0) = (4811c7ad. c4b3edca),$  $G(K_1] \dots G(K_1Ka_{11}^{\wedge}) = (c4b3edca. 44ca5ce1),$  $GfX_4J \dots G(X_1)(a_{11} a_1) = \{44ca5ce1, fef51b68(,$  $G\{K_1] \dots G[K_1Ka_{11} a_{11}) = (fef51b68. 2098od86).$  $GpC, J \dots Gp<, Ka_{11} Sc) = (2098cd86. 4f15bObb),$  $Gp^{\wedge}j \dots Gp^{\wedge}Ka_{11} a^{\wedge}) = (4f15bObb. e32805bc),$  $G\{K_1] \dots G(K_1Xa_{11} a_{11}) = (e32805bc. e7116722).$  $GJX_9] \dots G[X_1Xa_{11}^{\wedge}) = (e7116722.89cadf21),$  $G(X_{20}] \dots G[X_1](a_{11} a_0) \gg (89cadf21. bac8444d).$  $G(X_{21}) \dots G(X_1I(a_{11} \geq (bac8444d. 11263a21).$  $G(X_{22}] \dots GJX_1)(a_{11}^{\wedge}) = (11263a21.625434c3),$  $GJX_{23}] \dots G(X_1)(a_{11} e_{11} > - (625434c3. 8025c0a5).$  $G<X_{24}] \dots G(X_1)(a_{11} e_0) = (8025c0a5. b0d66514).$  $G(X_{25}] \dots G(X_1)(a_1 e_{11}) = (b0d66514, 47b1d5f4).$  $G[X_{26}] \dots GIX_1K^{\wedge} e_{11} = <47Md5f4. c78e6d50).$  $G\{X_{27}] \dots G[X_1](a_{11} e_Q > = <c78e6d50. 60251e99).$  $G\{X_{28}] \dots G(X_1)(a_{11} a_Q > = (80251e99. 2b96eca6).$

$$. GIKJfa, a^j) = (2 \ 96 \ 6. \ 05ef44Q1).$$

$$G(X_{30})...G(X, Ka, fi,) = (05ef4401.239a4577).$$

$$GIX_3, l...G[X_1l(a_1, a_0) = (239a4577. \ c2d8ca3d).$$

$$6=G4K_3JG(K_3,...GfK,)(a,e_0)=4ee901e5c2d8ca3d.$$

**pKUMfcmu**

.3.3.

$$b \ s \ 4ee901e5c2d8ca3d.$$

$$( \ , \ ) = (4 \ 901 \ 5. \ c2d8ca3d).$$

$$G[X_{32}KA- A,) = (c2d8ca3d. \ 239 \ 4577).$$

$$G[X_3,G\{K_{32}\}(A. A) = (239 \ 4577. \ 05ef4401>.$$

$$G[X_{30})...G[X_{32}Kb,, \ 3) = (05ef4401.2 \ 96 \ 6).$$

$$G(X_{2\#})...G(X_{32}XA- \ }) = (2 \ 96 \ 6. \ 80251 \ 99).$$

$$G[X_{2e}]...G(X_{32}XA^* \ })^9 (80251 \ 99. \ c78e6d50).$$

$$G(K,,J...G(K_{32}XA. \ ))^9 (c78e6d50. \ 47b1d5f4).$$

$$G(K_{2<3}...GtK_{3a}JCb_v \ ) = (47b1d5f4. \ b0d66514),$$

$$G[K_2J...G(K_{32}X6,. \ b_0) = (WW66514. \ 8025c0a5).$$

$$G(K_{24}J...G(K_{32}KA- A_j) \ )^e (8025c0a5, \ 625434c3).$$

$$G(K_{2j})...G\{K_{32}KA- A)\}^9 (625434c3. \ 11263a21),$$

$$G(K_{22}J...G[K_{32}Xb,. \ A,) \ )^9 (11263a21. \ bac8444d),$$

$$G(K_2,...G(K_{32}XA- A)) \ )^s (bac8444d. \ 89cadf21).$$

$$G[K_{20}J...GtX_{32}XA. \ A,) = (89cadf21, \ e7116722),$$

$$GIK_{ig}]...G(K_{32})(A. A,) = (87116722. \ e32805bc).$$

$$G|K_uJ...G(K_{32}Kb,. \ b_0) = (e32805bc. \ 4f15b0bb).$$

$$G(K_{7,},...<^AK_{32})(A. A,) \ )^e (4(15b0bb. \ 2098cd86).$$

$$G(X,,,)]...G\{K_{32}\}(A. A_i> \ )^9 (2098cd86. \ fefS1b68).$$

$$G(X_5)]...G(X_{32})(A. A) \ )^9 (to»1b68.44ca5ce1).$$

$$6(X_{14}]...G(X_{32})(A, A) \ )^9 (44ca5ce1. \ c4b3edca).$$

$$G[X_{13}]...G(X_{32})(A. A_j) \ )=<c4b3edca, \ 4811c7ad>.$$

$$G(K_{12})...G(K_{32}J(A. A>) \ )^s(4811c7ad. \ 93c1f449).$$

$$GIK,,)]...G\{X_{32}J(A- A>) \ )^s(93c1f449. \ ce995f2a),$$

$$G(X_e)]...G(X_{32})(A. A,) \ )^9 (ce995f2a. \ 46324615).$$

$$G(X_9J...GX_{32})(A, A_j) \ )^s (46324615. \ 37d97f25).$$

$$G(X_8)]...G(X_{32})(A. At) \ )^9 (37d97125. \ ad0310a4).$$

$$G(X_7)]...G(X_{32}J(A. A)) \ )^9 (ad0310a4. \ 11fe726d).$$

$$G(X_eI...G[X_{32})(A. At> \ )^9 (111e726d. \ ea89c02c),$$

$$G(X_5J...G\{X_{32}\}(A. A,) \ )^9 (ea89c02c. \ 633a7c68),$$

$$G(X_41...G[X_{32})(A. A_j> \ )^9 (633a7c68. \ 4337 \ 5).$$

$$G(X_3].-G(X_{32})(A. \ \&_o) = (M4337a5, \ 28da3b14),$$

$$GIX_2)]...G(X_{32})(A.b_0) = (28da3b14. \ 76543210).$$

$$= G' (X, \ \gg1 \ 2 \ ] \bullet \bullet - G ( \ 32 \ ]( \ . At) \ )^9 fedcba9876543210.$$

	Reference	Standard	Version	Year	Standard Title
[1]	ISO/IEC 10116:2017	Information technology — Security techniques — Modes of operation for an n-bit block cipher	1.0	2017	Information technology — Security techniques — Modes of operation for an n-bit block cipher
[2]	ISO/IEC 18033-1:2015	Security techniques — Encryption algorithms — Part 1: General	1.0	2015	Security techniques — Encryption algorithms — Part 1: General
[3]	ISO/IEC 18033-3:2010	Security techniques — Encryption algorithms — Part 3: Block ciphers	3.0	2010	Security techniques — Encryption algorithms — Part 3: Block ciphers

**681.3.06:006.354**

**35.040**

1—2019/63

OS. 12 2013.

00.01.2019. 6Q » 04'g.

. . . 1.66 - - . 1.49.

« \_\_\_\_\_ », 11S419. \_\_\_\_\_, \_\_\_\_\_. \_\_\_\_\_ .11.  
www.juristzda.ru y.book@mail.nj

« »

117416 . - , .31. .2.  
www.goslinlo.ru into@gostinfb.ru