

( ) ,

INTERSTATE COUNCIL FOR STANDARDIZATION. METROLOGY AND CERTIFICATION  
(ISC)

**34,13—  
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? 1062- 34.13—2018

1 2019 .

5 34.13—2015

6 28147—89 2 « »: 3 «

»: 4 « »: 5 «

»

« », —

« ».

« ».

—

(www.gost.ni)



1	.....	1
2	, .....	1
2.1	.....	1
2.2	.....	3
3	.....	3
4	.....	4
4.1	.....	4
4.2	.....	4
4.3	.....	&
5	.....	5
5.1	.....	
5.2	& .....	6
5.3	.....	(
5.4	.....	9
5.5	.....	11
5.6	.....	13
	(       ) .....	16
	.....	22

«

Information technology. Cryptographic data security.  
Modes of operation for block ciphers

— 2019—06—01

1

2

2.1

2.1.1

(encryption algorithm):

2.1.2

(decryption algorithm):

2.1.3

(basic block cipher):

2.1.4

( ):

2.1.5

(block cipher):

1

2

- 2.1.6 (padding):  
— / 10118-1 [3].
- 2.1.7 (block chaining):  
— / 18033-1 (4).
- 2.1.8 (encryption):  
— / 18033-1 (4).
- 2.1.9 (message authentication code):  
— / 9797-1 [1].
- 2.1.10 (key):  
1 / 18033-1 [4].  
2  
( ).
- 2.1.11 (starting variable):  
— / 10116 (2).
- 2.1.12 (plaintext):  
— / 10116 [2].
- 2.1.13 (decryption):  
1 / 18033-1 (4).  
2  
— , —  
— « », —  
— » « ».  
»
- 2.1.14 (symmetric cryptographic technique):  
— / 16033-1 (4).
- 2.1.15 (initializing value):  
— / 14888-115].
- 2.1.16 (message):  
— / 10118 [2].
- 2.1.17 (counter):  
— / 16033-1 (4).
- 2.1.18 (cipher):  
— / 10116 (2).
- 2.1.19 (ciphertext):  
— / 10116 (2).

## 2.2

6

$$V^*_{-}$$
 $V_s -$ 

11-

$$11 -$$

0' —

---

2^, —

tb —

$$\text{mod/} -$$
$$\text{MSB}_s \cdot V \backslash (JV \leftrightarrow V_s -$$

5-1 2 милл. - 17 мс V. » 0.1 ... -1;

 $V_s -$ 

-  $2_s, |l^{\wedge}.z.eV, \cdot / \ll 0.1....m-1;$

« —

$A_{\ll r, \{LSB', -(A, ]^{o'}]_{ecmir} < s <$

**Poty<sub>s</sub>: -> GF(2)[x] —**

**S-1**  
**Poly<sub>s</sub>(z)»£z,x';**  
**-0**

$$V_{to}, z_2 \rightarrow v_s -$$
$$z \cdot \wedge) + 2z_2 + \dots + 2^{s-1} z_{s-1} \quad z_i \in \{0,1\}, i \in \overline{1, s-1},$$
$$\text{Vec}_e(2) \ll 2_{a+1} | [.. | 2_1 | 2_0 :$$
$$\text{int/Vj-tZ?} \text{, — } \text{Vec}_s, \dots \text{Int}_s \ll \text{Vec}_e';$$

---

---

$$: V_n \quad V^* \rightarrow V_n \text{ —}$$
$$: - \gg V_n -$$
$$d_K: V_n \rightarrow V_n$$
$$\dots d_K = e_x.$$

**3**

« ( . . Electronic Codebook);

- (CTR. . Counter):

- (OFB. . Output Feedback);

« ( . . . **Cipher Block Chaining**);

- (CFB. . Cipher Feedback);

- ( . Message Authentication Code algorithm).

## 4

## 4.1

### 4.1.1

$$\left( \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \right) \quad \left( \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \right)$$

***I.***

 $V^*$ 

4.1.2 1

$$r^*|P| \bmod \ell.$$

**0,**

P's | 0'

$$P_v \quad |pJ= / < J -1$$
$$q. \quad {}_2 P_t \parallel 0$$

**4.1.3 2**

$$z \ll |P| \bmod /.$$

||1|0- ' \

***I.***

**4.1.4** **3**

 $\ll |P| \bmod \ell$ 
$$\begin{aligned} & \vdots \\ & \text{"} \sim, \end{aligned}$$

- $\quad =$
- $\quad < l,$

**2.**

**1** (5.1—5.5).

**(5.6)**

2

## 4.2

/

*m*

 $\gg V_m$ 

**IV.**

***IV***

( )::

2' < :



\* , , . ;

\* ( ), .

#### 4.3

8

*s.ssn.c* -

$I_s - MSB_s, \dots$

#### 5

##### 5.1

##### 5.1.1

, , -

( ) ( - )

##### 5.1.2

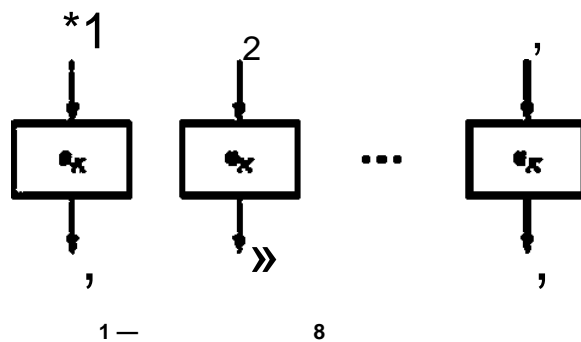
$Pt_{(} \mid \mid \gg q.$  :

**p-p.hi** . / 12.....*q*.

, = $e_K(P,)/ = tZ$  )

:  
- ,  $\mid 2 \mid \dots \mid \gg$ ,

1.



##### 5.1.3

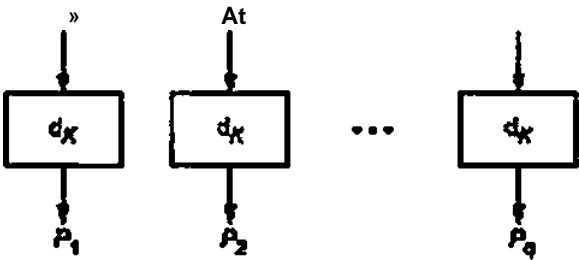
: - ,  $\mid 2 \mid \dots \mid \gg$  .  $V_{n,i} - 1.2 \dots q.$

:  
 $p_e d_K(C,)/ \ll 1.2 \dots q. \quad (2)$

( ) :

=  $\mid 1 \mid \mid 2 \mid \dots \mid \gg$  ,

2.



2—

5.2

5.2.1

, 0 < \*• s . -

( ) -

$$IV \quad V_n' \\ 2$$

CTR, 6 V, i = 1.2.....

$$CTR_y \cdot 1 ( / ) = / ||02.$$

Add: V\_n — :

$$\text{AddtCTR}_i) \gg \text{Vec}_n(\text{Int}_{JJ}(\text{CTR}_i) \text{ffi}_i 1). \tag{3}$$

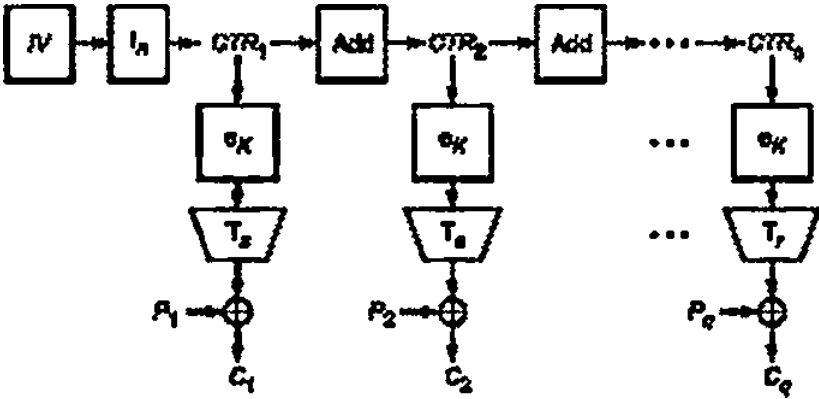
5.2.2

$$V^* \quad | \quad 2 | - | ^\wedge . \quad / \quad t_2, \dots, q - IP_q e V'_r, r Ss. :$$

$$(C_j. ^\wedge \odot T_5(e_K(C7-RJ). / - IZ, \dots, Q - I$$

:

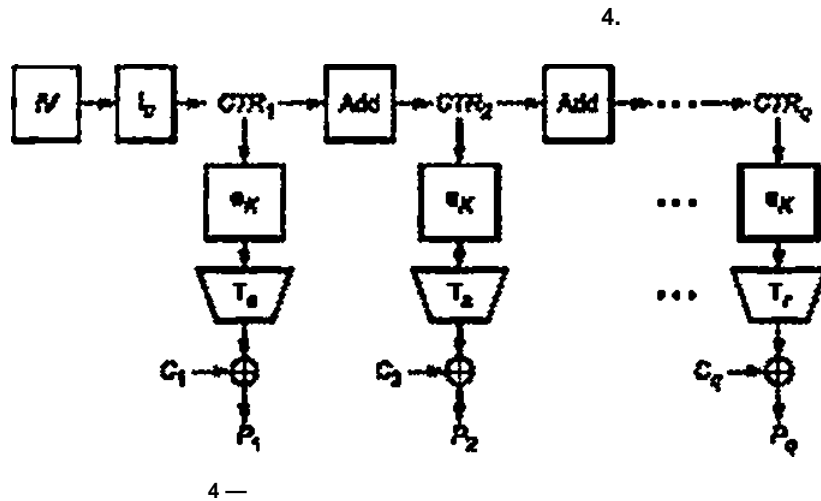
3.



3—

5.2.3

$$\begin{aligned}
 &: C_t \parallel 1 \cdot |', \quad V_s, / \ll 1, 2, \dots, g-1 \quad C_Q e V_s, \quad \varepsilon s. \\
 &= ( \quad 5( \quad ? \rangle, l, t \dots < j-t \\
 &P'.C'QT^{\wedge}CTR')). \quad (5) \\
 &: \\
 &p'p.hLjp, '
 \end{aligned}$$



5.3

5.3.1

\$ m. Q<sin, m\* - , 21 —

R

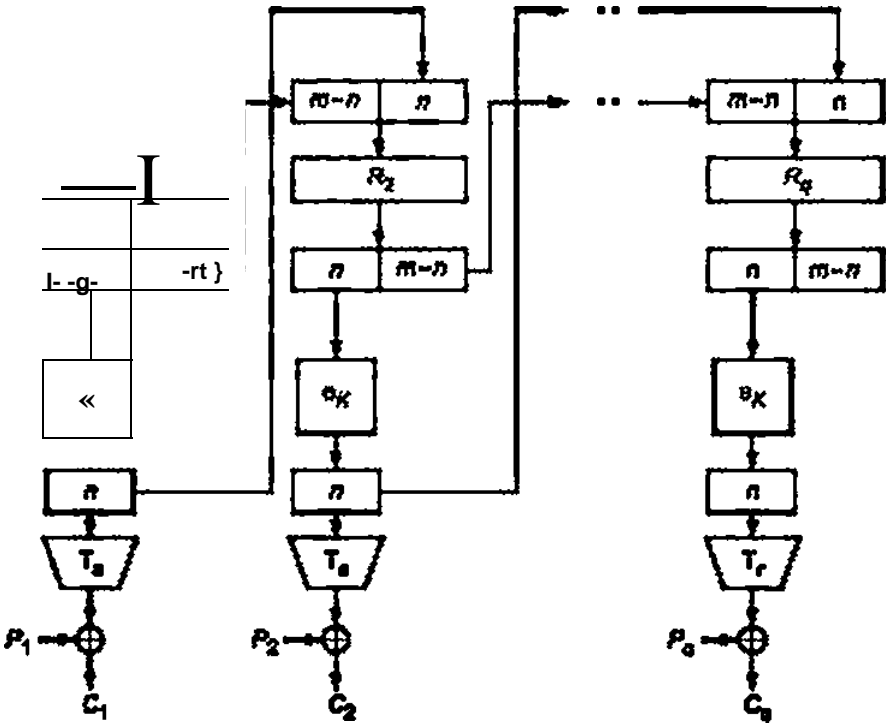
IV.

5.3.2

$$\begin{aligned}
 V^* &: 1 \mid - P, bV_s, -12, \dots, Q-1, P_q bV_q r^* s. \\
 &, = IV, \\
 &V, Be_K(MS8_n(RJ)). \\
 &\rangle, >. , ( \quad /-1, \dots, <7-1 \quad (6) \\
 &R_{i+1} = \text{LSB}_{m-n}(R_i) \parallel Y_i \\
 &Y_q = e_K(\text{MSB}_n(R_q)). \\
 &C_q = P_q \oplus T_r(Y_q).
 \end{aligned}$$

:

5.



5 —

5.3.3

:        ^        . |C<sub>Q</sub>. C-<=V<sub>s</sub>/«12.....Q-1,  
:

R, - /V.

^~e<sub>K</sub>(MSB<sub>„</sub>{R.)).

Ve<sub>K</sub><MSB<sub>„</sub>(R<sub>q</sub>)),

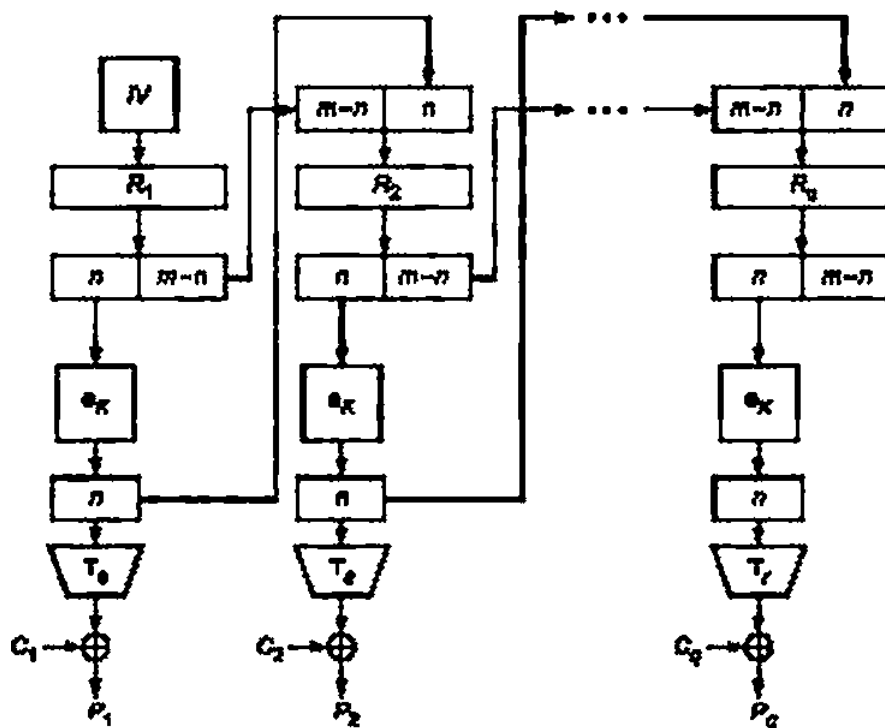
^~c,eT<sub>r</sub>(y<sub>g</sub>).

TMSCT

!

p=p,hi h

6.



6 —

5.4

5.4.1

-2.2 £ 1 —

( )  $I \vee V_m$ 

R

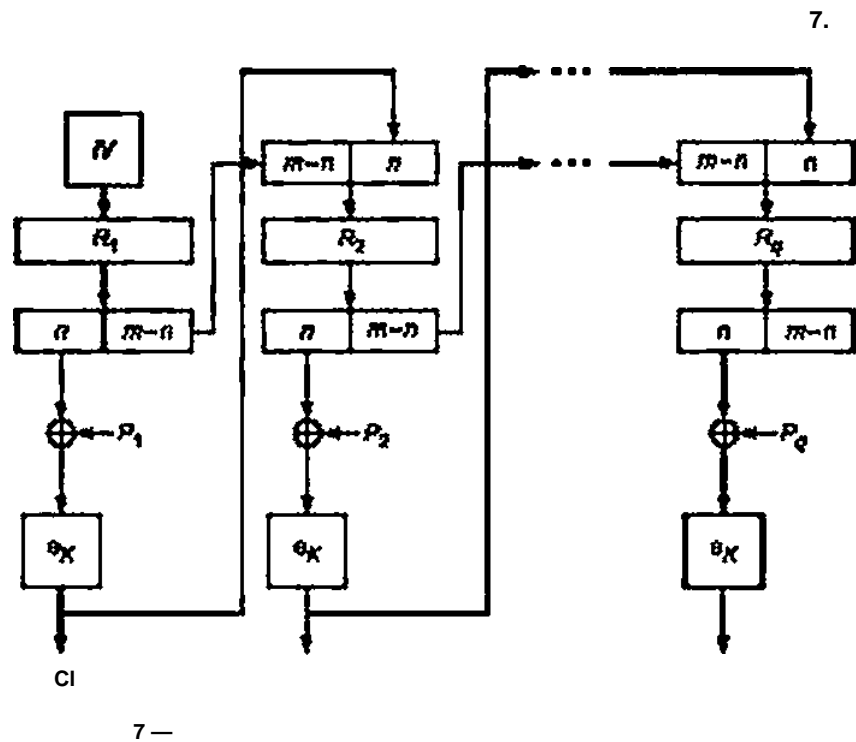
IV

5.4.2

 $PbV^* \cdot | | q.$  $, - P^{\wedge} V_n / \ll 12 \dots \dots q.$ 

, - IV.

 $C, ^e_{e_K}(P_t \odot MSBJR,)).$  $/ \ll 1, Z \dots \dots < j-t$  $c_9 \ll M^p_9 \odot^{MSB}, W > -$



5.4.3

$C_j C^{A_i} \mid g, \dots, m \quad (i = 1, 2, \dots, q)$

:

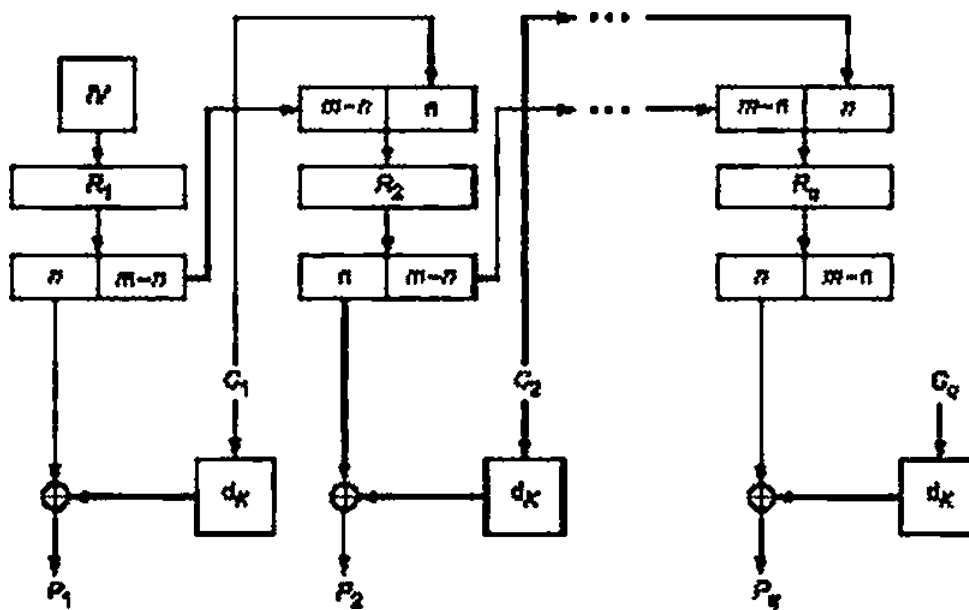
, - IV,

$K, n\text{-LSB}_{m-n}(R_1)(C, \dots, f-1, \dots, q-1)$

(                      )                      :

p-p,hi h

8.



8 —

\*!

5.5

5.5.1

$s$ ,  $0 < s \leq s$ ,  $s$ .

8

$| | s \cdot q$ .

. 8

( )  $IV V_m$

$R$

IV.

\$

5.5.2

$V^*$  »  $|_2 |$  » ;  $V^* / 12 \dots Q-1$  ^ r ss.

$R_i = IV$ .

$C, \langle P_{\geq} \odot T, (e_K \langle \text{MSB}_{\geq} \langle R_i \rangle) \rangle$ ,

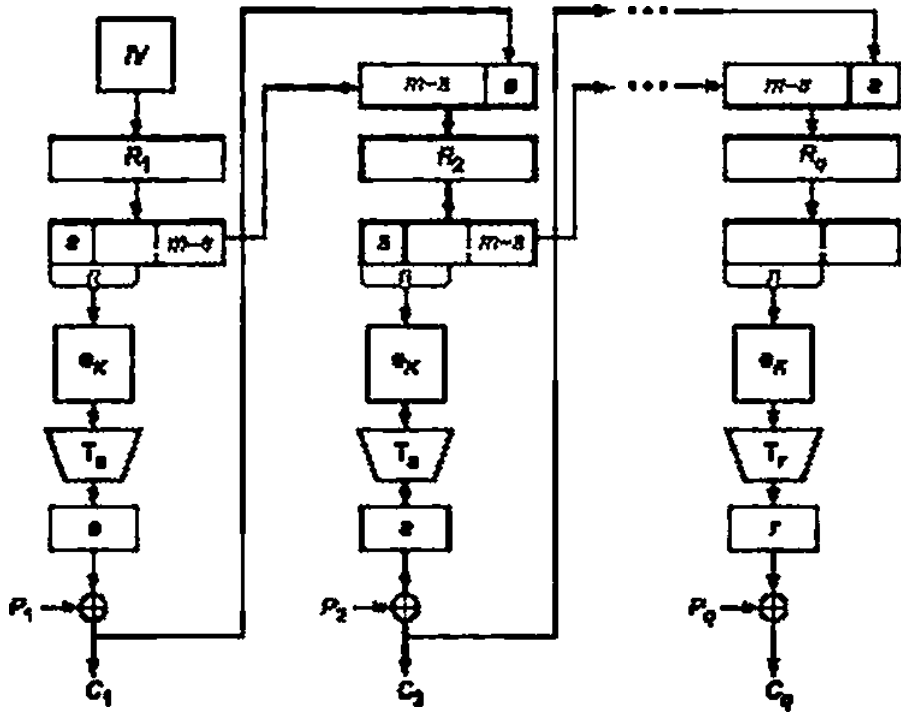
$/ \gg 1.2 \dots -1$

( )

$a_{\text{LSB}_\geq}$

$C^{\wedge} e T J e^{\wedge} \text{MSBJR}_i \rangle$ .

9.



9 —

5.5.3

: , | 2|...| , C, £V<sub>S</sub>, /«1,2,... -t „ V,, s s.

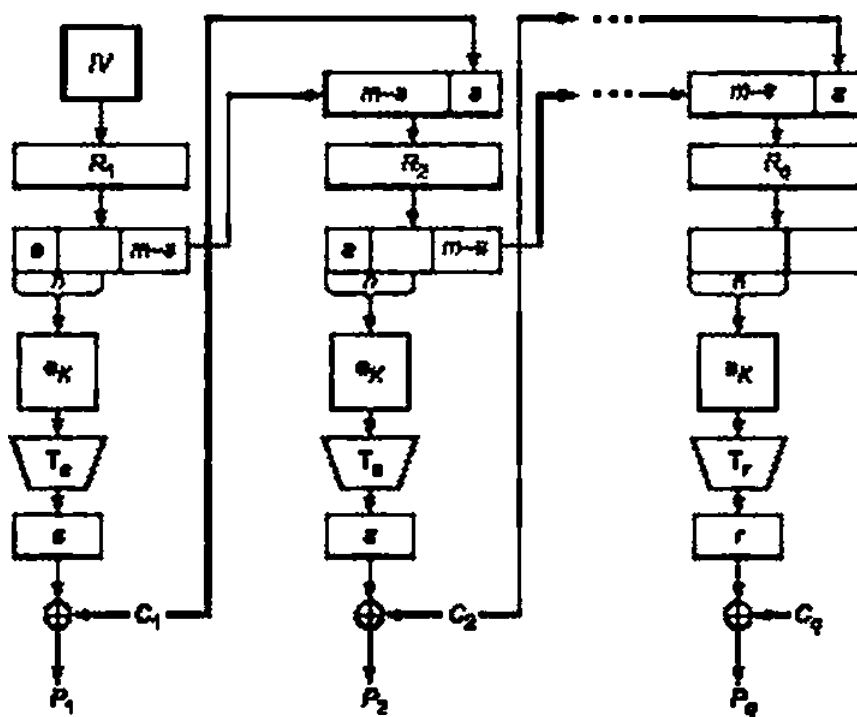
$$, = IV,$$
$$, \ll , @T_e(e_K(\text{MSB}_n(R_i))), \quad i \gg 12.....<?-1,$$
$$\ll \dots = \text{LSB}_n, \gg \ll , \bullet$$
$$P_Q \gg C_9 @T_e(e_K(\text{MSB}_n(R_4))).$$

(11)

$$p=p,hi-ip \ll -$$



10.



10 —

5.6

5.6.1

1 (

ISO

[1]).

( )  $0 < s \leq \varepsilon$  .

5.6.2

$R \ll e_K < 0''$ );

$MSB_i(R) = 0,$

$1^* \lfloor (/? \ll 1) \ 8_{,,}$  ;

$MSB_i(K_1) \gg 0,$

$*2 \ " \ \{( \ , < 1) \odot 0_{,,}$  .

$4 \ll 0 \ | 11011. \quad 12 \ \ll 0^{120} | 10000111.$

64    128.

GF(2)

$f_{,,}(x)$

(2)  $\lceil \mathcal{V}(\cdot) \rceil$ ,  
:  
⑧.  
1 2

$$\begin{aligned} & \text{^oly^PolyJPISx),} \\ & \text{rPoly^Poly^PJSx^2).} \end{aligned} \tag{12}$$

— , .  
R

5.6.3

0":  
:  
MAC  
V\*.

$$p=p.hi\ h$$

$P_j^{\wedge}V_n, z' = \{Z....g-1\} P_q e V, rin.$

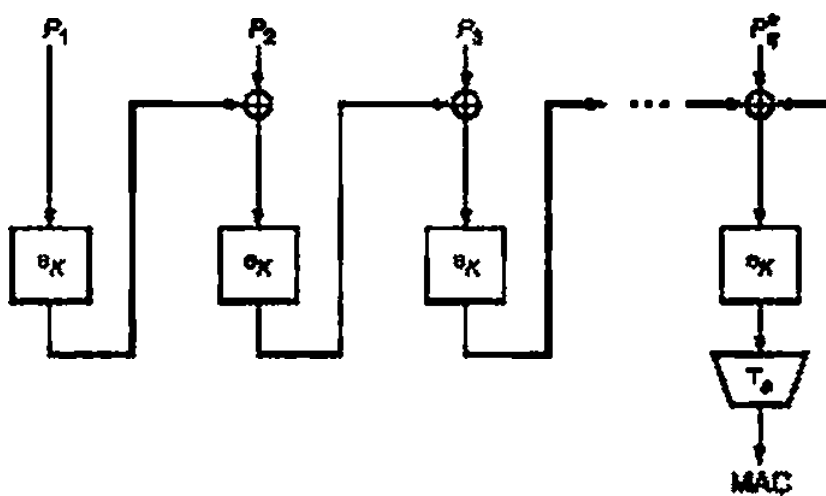
$$\begin{aligned} & 0 \text{ "}. \\ & .... g-l \\ & MAC = T_s(e_K(P_i; \odot C_{(f-1)} \odot K' \rangle). \end{aligned} \tag{13}$$

$$\begin{aligned} & \text{,, } |\ddot{P}_q| \rangle \text{ .} \\ & 2' \text{ ,} \end{aligned}$$

$$P_q' \text{ — 3. , -}$$

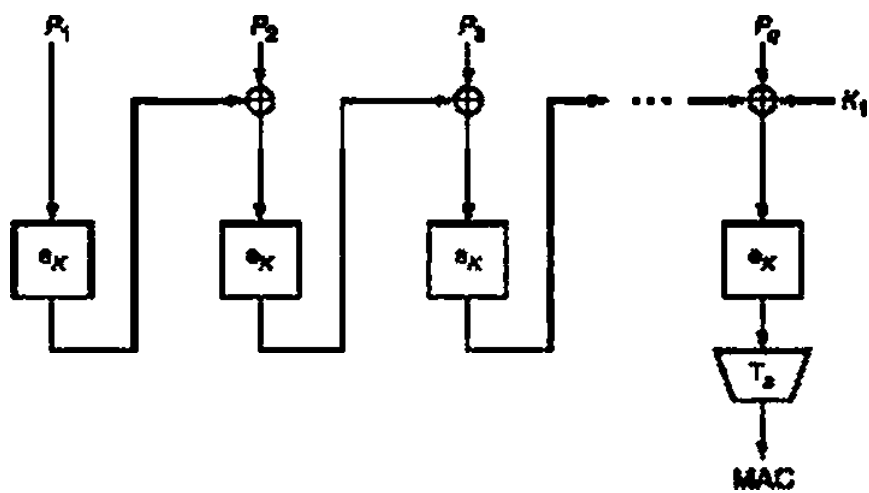
5.1—5.5.

11—13.



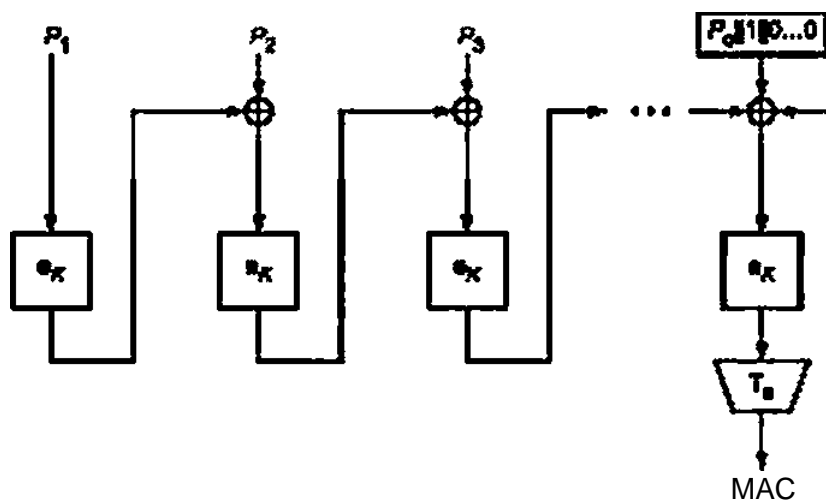
11 —

—



12 —

—



13 —

«

—

8

( )

.1

.

s

V\*.

4.

(\*)

{0.1.....9, a. b. c.d.e.f}. i 0.1 ...,r-1.

.2

= 128 (« »),

- 64 (« »).

.2

= 128

AJ.1

:

= 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcde(.

— 128-

, = 1122334455667700feeddccbbaa9988.

2 - 00112233445566778899 abbcceeff0a,

- - 11223344556677&899 ( 00.

4 = 2233445566778899aabbccceeff0a0011.

.2.2

.1 —

1122334455667 700feeddccbbaa9988	71679d90bec24305a468d42b9d4edod
00112233445566778899	b429912c6e0032f9285452d76718d08b
112233445566778899	(0ca33549d247ceef3f5a5313bd4b157
2233445566778899aabbccceeff0a0011	d0b09ccde830b9eb3a02c4c5aa8ada98

.2.3

.2.3.1

s-n- 128.

IV- 1234567890abcef.

.2 —

1	1	2
p,	11223344556677OOf feeddec 9988	00112233445566778899aabbccceeff0a
	1234567890 »000000000000000000	1234567890abcefO O O O O O O O O O O O O O O O I
	e0b7ebfa9468a6db2a95826efb173830	85fTc500b2f4582a7ba54e08f0ab21
,	1195d8bec10ed1dbd57b5fa240bda1b8	85eee733f6a13e5df33ce4b33c45dee4

.2

<i>t</i>	3	4
,	112233445566778899 0 00	2233445566778899aabbccceff0a0011
	1234567890 00 000000000000002	1234567890abcef00000000000000003
	Mc8dbcfb353195b4c42cc3ddb9ba9a5	e9a2bee4947b32217b7d1db6dfb7ba62
,	a5eae88be6356ed3d5e877f 13564	cb91 faM f20cbab6d 1 c6d15820bdba73

.2. .2

. IV

,, %. 3. +.

.2.4

.2.4.1

s = n=128, = 2 = 256.

IV = 12345 7890 1 2 4 5 011223344556677889901213141516171819.

. —

<i>r</i>	1	2
<i>p&gt;</i>	1122334455667700Reedddccbbaa9988	00112233445566778899aabbccceR0a
	1234567890abcef0a1b2c3d4e5f00112	23344556677889901213141516171819
	90a2391de4e25c2400f1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
,	81800a59b1842b24R1f795e897abd95	ed5b47a7048cfab48fb521369d9326bf

.

<i>i</i>	3	4
<i>P,</i>	112233445566778899aabbccceR0a00	2233445566778899aabbccceR0aOO11
	90a2391de4e25c2400f1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
	778064e869c6cf3951 a55c30fed78013	020dff9500640ef90a92eead099a3141
,	66a257ac3ca0b8b1c80fe7fc10288a13	203ebbc066138660a0292243f6903150

.2.4.2

. IV

,, 2. 3. +.

.2.5

.2.5.1

= 2 = 256,

IV = 1234567890abcef0a1b2c3d4e5f0011223344556677889901213141516171819.

.4 —

<i>r</i>	1	2
<i>p,</i>	1122334455667700Reedddccbbaa9988	00112233445566778899aabbccceR0a
	0316653cc5cdb9f05e5c1e185e5a989a	23256765232defe79a8abeaedaf9e713
	689972d4a085fa4d90e52e3d6d7doc27	2826e661 b4 78eca6af 1 e8e448d5ea5ac
,	689972d4a085fa4d90e52e3d6d7dcc27	2826e661 b4 78eca6af 1 e8e448d5ea5ac

. 4

<i>i</i>	3	4
<i>P</i> ,	112233445566778899aabbccceeff0a00	2233445566778899aabbccceeff0a0011
	79bb419015e38dc5 094f95f18382c627	0a16a234d20f643f05a542aa7254a5bd
	fe7babf 1e91999e85640e8b«49d90d0	167688065a895c631 a2d9a1560b63970
,	1e7babf1e91999e85640e8b0f49d90d0	167688065aB95c631a2d9a1560b63970

.2.5.2

, IV

*P*<sub>v</sub> 2' 3' 4'

.2.6

.2.6.1

5 = 128. m = 2 =256,

IV- 1234567890abcef0a1b2c3d4e5f0011223344556677889901213141516171819.

.5 —

<i>i</i>	1	2
<i>P</i> ,	1122334455667700feed dec bbaa9988	00112233445566778899aabbccceeff0a
	1234567890abcef0a1b2c3d4e5f00112	23344556677889901213141516171819
	90a2391de4e25c2400f 1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
,	81800a59M842b241T1f795e897abd95	ed5b47a7O48cfab481b521369d9326bf

.5

<i>i</i>	3	4
<i>P</i> .	112233445566778899aabbccceeff0a00	2233445566778899aabbccceeff0a0011
	81800a59M842b241T1f795e897abd95	ed5b47a7O48cfab48fb521369d9326W
	68d09baf09a0fab01 d879d82795d32b5	6dcdfa9828e5a57(6de01533bbf 114c0
,	79f2a8eb5cc68d38842d264e97a238b5	4ffebeod4e922de6c75bd9dd441bf4d1

.2.6.2

. IV

' 2' 2' '

.2

.2.7.1

R-94bec15e269cf1e506f02b994c0a8ea0.

MSB<sub>i</sub>(R)=t

, »R<ieS<sub>A</sub>

= 297d82bc4d39e3ca0de0573298151dc7.

MSB<sub>i</sub>(K<sub>i</sub>) = 0,

K<sub>2</sub> = K<sub>1</sub> «1 = 297d82bc4d39e3ca0de0573298151dc <1 = 52fb05789a73c7941bc0ae65302a3b8e.

|P<sub>i</sub>| = n. K' = K<sub>r</sub>

A.2.7.2

s = 64.

.6—

<i>i</i>	1	2
,	1122334455667700feeddccbbaa9988	00112233445566778899aabbccceeff0a
	1122334455667700feeddccbbaa9988	7f76Wa3fae94247d2df2719753a12c7
	7f679d90t»bc24305a468d42b9d4edcd	1ac9d976f83636f55ae9ef305e7c90d2

.6

<i>r</i>	3	4
<i>p</i> ,	112233445566778899aabbccceeff0a00	2233445566778899aabbccceeff0aOO11
	0beba32ad50417dc34354fcb0839ad2	1 e2a9c1 d8cc03bfa0cb340971252fe24
	15645af4a78e50a9abe8db4b754de3f2	33614d296059fbe34ddeb35b37749c67

MAC - 336f4d2960591be3.

. = 64

.3.1

:

K=feeddccbbaa9988776655443322110CM0f1f2f3f4f5{6f7f8f9fafbfc1dfefl.

— 64- :

, = 92def06b3c130a59.

 $P_2 = \text{db54c704(8189d20.}$  $_3 = 4a98fb2e67a8024c.$  $_4 = 8912409 \ 17 \ 57 \ 41.$ 

.3.2

.7 —

92def06b3c130a59	2b073f0494f372a0
db54c704IB189d20	6e70e715d3556e48
4a98fb2e67a8024c	11 d8d9e9eacfbfc1 e
8912409b17b57e41	7c68260996c67efb

.3.3

. .3.1

S = - 64.

IV- 12345678.

.8—

<i>r</i>	1	2
<i>p</i> ,	92def06b3c130a59	db54c704f8189d20
	1234567800000000	1234567800000001
	dc46e167aba4b365	e571ca972ef0c049
,	4 98110 97 7 93	3e250d93d6e85d69

. 8

<i>i</i>		4
'	4a98fb2e67a8024c	8912409 7 57 41
	1234567800000002	1234567800000003
	59fS7da6601ad9a3	d(9cf61bbce7df6c
,	136d868807b2dbef	568eb6B0ab52a12d

.3.3.2

. fV

” 2’ \$, .

.3.4

.3.4.1

s = n = 64, = 2 = 128.

IV - 1234567890abcdef234567890abcdef1.

.9 —

>		2
'	92def06b3c130a59	db54c704f8189d20
	1234567890abcdef	234567890abcdef1
	49e910895a8336da	d612a348e78295bc
,	<Jb37e0e266903c83	0d46644c1f9a089c

.9

<i>i</i>	3	4
<i>P'</i>	4 98< 2 67 8024	8912409 7 57 41
	49e910895a8336da	d612a348e78295bc
	60 4 24 63032	4136af23aafaa544
,	a0f83062430e327e	c824e(b8bd4fdb05

.3.4.2

. IV

3’ \$, .

A.3.S

.3.5.1

= 3 =192,

IV = 1234567890abcdef234567890abcde(134567890abcdef 12.

.10 —

>		2
'	92def06b3c130a59	db54c704f8189d20
	80 61 8 7 6	f811a08df2a443d1
	96d1b05eea683919	«76129 937 9
,	96d1b05eea683919	76129 937 9

. 10

<i>i</i>	3	4
<i>P<sub>t</sub></i>	4 98< 2 67 8024	8912409 7 57 41
	7ece83beoc65ed5e	1fc3f0c5fddd4758
	5058b4a1c4bc0019	20b78b1a7od7e667
,	5058b4a1c4bc0019	20b78b1a7od7e667



.3.5.2

, IV

, 2. \$.

.3.6

.3.6.1

s = 64, = 2 = 128.

IV = 1234567890abcdef234567890abcdeFt

.11 —

<i>i</i>	1	2
,	92def06b3c130a59	db54c704fS189020
	1234567890abcdef	234567890abcdef1
	49e910895a8336da	d612a348e78295bc
,	db37e0e266903c83	0646644c1f9a089c

.11

<i>i</i>	3	4
<i>P</i> >	4a98fb2e67a8024c	8912409 7 57 41
	db37e0e266903c83	0d46644c1f9a089c
	6e25292d34bdd1c7	35d2728f36b22b44
,	24bdd2035315d38b	bcc0321421075505

.3.6.2

. IV

, % 3 4

.3.7

.3.7.1

P = 2fa2cd99a1290a12.

MSB,(«) « 0. X, = R &lt; 1 = 51459b3342521424,

MSB,(K<sub>n</sub>) = 0. K<sub>2</sub> = , < 1 = 8 366684 42848.| . ' = K<sub>t</sub>.

.3.7.2

s-32.

.12—

<i>t</i>	1	2
<i>p</i> ,	92def06b3c130a59	db54c70418189d20
	92def06b3c130a59	1053f8006cebef80
	2b073f0494f372a0	c89ed814fd5e18e9

.12

<i>r</i>	3	4
<i>p</i> ,	4a98fb2e67a8024c	8912409 17 57 41
	8206233a9af61aa5	216e6a2561cff165
	1739M8d34289b00	154e72102030c5bb

MAC - 154 7210.

- (11) / 9797-1:2011  
(ISO/IEC 9797-1:2011) (MAC). 1. (Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher)
- (2J) / 10116:2017  
(ISO/IEC 10116:2017) (Information technology — Security techniques — Modes of operation for an -bit block cipher)
- [3] / 10118-1:2016  
(ISO/IEC 10118-1:2016) 1. (Information technology— Security techniques — Hash-functions — Part 1: General)
- [4] / 18033-1:2015  
(ISO/IEC 18033-1:2005) 1. (Information technology— Security techniques — Encryption algorithms — Part 1: General)
- [5] / 14888-1:2008  
(ISO/IEC 14888-1:2008) 1. (Information technology — Security techniques — Digital signatures with appendix — Part 1: General)

681.3.06:006.354

35.040

⋮  
, , , , , \*

1—2019/64

«  
»  
»  
»  
»  
»

05.12.2018.

01.2019. 60 » ^/g.  
3.26 - . 2.95.  
»

« », 115419. , . 11.  
[www.jurietzdal.ru](http://www.jurietzdal.ru) y-book@mailnj

« »

117416 . - , . 31. . 2.  
[www.postinfo.ru](http://www.postinfo.ru) info@gostinfo.ru