International Journal of Hybrid Information Technology
Vol.2, No.4, October, 2009

Cryptographic Protection of the Information and Algorithms of Enciphering

[1]Sattarova Feruza Y., [2]Tadjibayev Furkhat A., and [1]Seung-Hwan Jeon

[1]Hannam University, Daejeon, S.Korea
[2]Lindenwood University, St. Charles, MO, USA
mymail6585@gmail.com

Abstract

In order to organize informational security the juridical documents, technical means and cryptographically algorithms, systematic, apparatus-systematic or apparatus-technical means are widely used. And with the advent of high-speed digital lines of information transfer requirements for cryptographic means of enciphering is growing more and more. In cryptosystem based on stream ciphers the entering information is not late in cryptosystem and it allows developing high-speed cryptographic hardware. Besides generated pseudo-casual and truly casual sequences it is widely used in cryptosystems for generation of initial values of confidential parameters and the secret key in the electronic digital signature.

The idea of working out of algorithm EDC was developed using operations of algebra parameters. Mathematical model of the digital signature, including parts of formation and the signature check, satisfying to conditions of demanded firmness in a composition of algorithm of enciphering and existing complexities of calculations are developed.

In this article also methods of estimation crypto stability of stream cipher algorithm of enciphering and practical results of an estimation of the new developed algorithm are resulted. Also the criteria of protection documentary, vocal and information video in information-communication systems and using cryptographic means are given in this article.

1. Introduction

Nowadays it is very important to organize effective ways of data exchange in the info communication systems. Development of technologies gives society more opportunities to use new types of info service. Informational security is also important in fast data exchange systems such as banking, data exchange in analyzing state or society information. As it is known, any information deals with the needs of info-communication system users.

Now the civilization of a human society passes from a technical civilization in the information. In connection with development of information technologies and, accordingly, various kinds of information services, questions of protection of the information became actually in wide spheres of a life of activity of a society. The volume of the information necessary for normal functioning of a modern society grows, approximately, to proportionally square of development of industrial potential.

The base of the stream cipher algorithm is the generator, which generate enough long pseudo-casual sequence with use short 128-2048 bits secret key. One of the main requirements to the generator of pseudo-casual sequence is simplicity of realizable function in algorithm of generator, which enables the estimations of practical crypto stability. Is

conformity the algorithms parameter will be tested to estimate crypto stability with following requirements:

Estimation of the used transformations:
Simplicity of the transformations;
high level nonlinearity of a cryptographic primitive;
irreversible transformation;
strictly avalanche effect criterion;

Estimation of the generated sequence:
high level degree to accidents a generated pseudo-casual sequence;
absence of short cycles, the periods.

Estimation stability to different types of cryptoattacks:
possibility finding secret key with method of full try;
finding the secret key with use was generated sequences fragment;
prediction of the following gamma with big probability knowing part of gamma;
stability of the transformations to differential cryptanalysis;
stability of the transformations to linear cryptanalysis

2. Use of parameter R of the Elliptic Curve as Parameter of Check EDS with Application of Algorithm of Enciphering

In cryptography the following canonical form of an elliptic curve [1-9] is used:

$$y^2 = x^3 + ax + b(\mathrm{mod}\, p)\text{, where simple number } p > 3,$$

which is expedient for the appendix.

As it has been noted in work [7] for increase crypto firmness at the expense of unknown parameter R it is offered to use the following implicit kind of an elliptic curve [6]:

$$y^{\backslash 2} = x^{\backslash 3} + ax + b(\mathrm{mod}\, p),\ p > 3,$$

where

$$y^{\backslash 2} = y \quad y = y + y + yRy(\mathrm{mod}\, p) = (2 + Ry)y(\mathrm{mod}\, p)$$

and

$$x^{\backslash 3} = (x \quad x) \quad x = (2 + Rx)x \quad x = (2 + Rx)x + x + (2 + Rx)x\ R\ x\ (\mathrm{mod}\, p) =$$
$$= R^2x^3 + 3Rx^2 + 3x\ (\mathrm{mod}\, p).$$

Taking into account last equalities the offered elliptic curve with parameter R assumes the following obvious air:

$$Ry^2 + 2y = R^2x^3 + 3Rx^2 + (3 + a)x + b(\mathrm{mod}\, p) \text{ or}$$

$$\left(\frac{1}{\sqrt{R}}\right)^2 (y + \frac{1}{R})^2 = [(x + \frac{1}{R})^3 + \frac{a}{R^2}(x + \frac{1}{R}) - \frac{a}{R^3} + \frac{b}{R^2}](\mathrm{mod}\, p)$$

From this equation with following designations

$$\frac{1}{\sqrt{R}}(y+\frac{1}{R})=Y \quad (x+\frac{1}{R})=X \quad \frac{a}{R^2}=A \quad \text{and} \quad -\frac{a}{R^3}+\frac{b}{R^2}=B$$

we pass to the equation

$$Y^2 = X^3 + AX + B(\mathrm{mod}\, p)$$

and on a turn on replacements:

$$Y=\frac{1}{\sqrt{R}}(y+\frac{1}{R}) \quad X=x+\frac{1}{R} \quad A=\frac{a}{R^2} \quad \text{and} \quad B=-\frac{a}{R^3}+\frac{b}{R^2}$$

from the equation $Y^2 = X^3 + AX + B(\mathrm{mod}\, p)$ we pass to the equation $Ry^2 + 2y = R^2x^3 + 3Rx^2 + (3+a)x + b(\mathrm{mod}\, p)$ or $y^{\backslash 2} = x^{\backslash 3} + ax + b(\mathrm{mod}\, p)$.

Number $[Aa(Ab-Ba)^{-1}]^{\mu}(\mathrm{mod}\, q) = \delta(R^{\mu}) = \Delta$ is called *as binding coefficient* of degree μ of an elliptic curve of an implicit kind with its obvious kind on module *q* [7].

Further, new algorithm EDC with latent use of parameter *R* of the elliptic curve connected in casually chosen parameter $\alpha \in (1,\ q)$, with application of algorithm of enciphering of data is resulted. This algorithm is ideological development on an improvement way criptofirmness, the offered method in work [7] where hesh-function is applied.

Algorithm. For the signature of message *M*, the signing party generates keys: *e* -opened and *d* –confidential from comparison $de \equiv 1 \bmod \varphi(n)$ where big enough number $n = p_1 q_1$, p_1, q_1 – unknown simple numbers (satisfying to conditions $p_1 > 2^{512},\ q_1 > 2^{512}$), ϕ (*n*) Euler's-function, for accuracy, let $p_1 > q_1$, gets out a random number *k* and *x* , and $1 < k < q$, *q* - simple number and $1\ q < q$, $1 < x < q$ and LCD (*x*, *n*) =1, parameter $g < n$ gets out on condition $\mathrm{LCD}(g, n) = 1$ and $g^q \bmod n \neq 1$, and also *q* is not divider ϕ (*n*) . Open keys are: $y = g^{axd} \bmod n$, the number *an* is defined from equality $ed - a\varphi(n) = 1$ and $Q = ([t]G,\ [x]G) = (Q_1, Q_2)$, where *G* the base point having an order *q* (where *q*-simple number) on the derivative elliptic curve (4), corresponding to an implicit kind (2), natural number $1 < t < q$.

In algorithm EDC following parameters are used:

1) Open keys: *y*-generated by rule $y = g^{axd} \bmod n$, and $1 < x < q$ where confidential keys *x* and *d*, are known only to the signed person; *e* - generated from comparison $de \equiv 1 \bmod \varphi(n)$; *Q*-steam of points of an elliptic curve generated by rule $Q = ([t]G,\ [x]G) = (Q_1, Q_2)$, where $G = (X_G, Y_G)$ the -base point having an order *q*, on the derivative elliptic curve (4), corresponding to an implicit kind (2).

2) Hesh-function *H* (*M*) which under the initial message (text) *M* forms an integer.

Each user EDC should possess personal keys:

a) *d*, *x*, *t* - integers - closed keys EDC and signed a chosen random number *k*, where $1 < k < q$;

b) *e* , *y* the-whole natural numbers and $\bar{Q} = (Q_1, Q_2)$- pair of points on an elliptic curve open keys

EDC.

The simple number *q* is opened and can be the general for group of users.

Processes of formation of the electronic digital signature under set message *M* и of acknowledgement of authenticity it is carried out as follows.

For realization of the given processes it is necessary, that to all users parameters of algorithm of the electronic digital signature, listed above were known.

Besides, each user to have closed key EDC (*d, x, t*) and open key EDC (*e, y, Q*).

Algorithm generation (formation) of the signature. Entrance data: message *M*, initial parameters (including binding coefficient $\Delta = \delta(R^{\mu})$ where μ it -is unknown), confidential and opening keys. Rely, that to users unknown persons are coefficients *a* and *b* equation (2), and coefficients *A* and *B* the equations (3), and also value of binding coefficient $\Delta = \delta(R^{\mu})$ are known. Such assumption allows hiding parameter *R* from users of a network. But in case of need *a b* (2) corresponding implicit kinds concerning a kind (3) as coefficients of the equation (4) are defined on parameter *R* with coefficients of the equation (2) give the

chance restoration of coefficients and with the centre of registration of keys, hence, the equations.

Target data: signature ς -is concatenation values of parameters (*r, s, w* ,γ , σ , τ), i.e. (*r s w* γ σ τ) =ς .

Steps of algorithm of generation of the signature:

1. To calculate value *H* (*M*) according to *M,* i.e. *h=H* (*M*).

2. On chosen random number *k* it is calculated: $[k]G = (X_k, Y_k)$. Besides, on random number θ it is calculated $\alpha = \Delta^{\theta} \bmod q$, in essence too is a random number and on it is calculated $[\alpha]G = (X_{\alpha}, Y_{\alpha})$.

These numbers *k* andα hold in confidentially and to destroy right after forming signatures.

3. It is calculated: $r = g^{X_k d} \bmod q$.

4. It is calculated: $\sigma = E_{X_k}(X_{\alpha}) \bmod q$

.

5. It is calculated: $\tau = E_{X_{\alpha}}(X_k) \bmod q$.

6. It is calculated: $\rho = g^{d} \bmod n$.

7. It is calculated: $\gamma = (g^{-ax}\rho) \bmod n$.

8. It is calculated: $s = [H(M)\rho t_{+} r\rho x + \alpha][rE_{X_k}(X_{\alpha})]^{-1} \bmod q$

9. It is calculated: $w = [H(M)\rho t_{+} r\rho x + k][rE_{X_{\alpha}}(X_k)]^{-1} \bmod q$ 10. The signature is binary or hexadecimal representation concatenation: $(r \quad s \quad w \quad \gamma \quad \sigma \quad \tau) = \varsigma$ Further the signed message is transferred in the reception party.

Acknowledgement of authenticity EDC. For acknowledgement of authenticity EDC under received message *M* it is necessary to execute following actions (steps).

Algorithm signature check.

Entrance data: message *M*, the initial parameters, an open key of check of the signature and the signature to *M* - concatenation (r s w $^{\gamma}$ $^{\sigma}$ $^{\tau}$) =ς .

Target data: the statement, that «the signature valid» or «the signature void».

1. If conditions $1 \le r, s, w, \sigma, \tau < q$ and $1 \le \gamma < n$ are broken, «the signature void» and to finish algorithm work.
2. To calculate value $H(M)$ according to *M*, i.e. $h=H(M)$.
3. To calculate: $\psi = y^{e} \bmod n$.
4. To calculate: $\beta = \psi\gamma \bmod n \quad (= \rho \bmod n = \rho)$, as $\rho < n$
5. To calculate: $u_1 = [H(M)\beta] \bmod q \ (= H(M)\rho - a_1 q)$.
6. To calculate: $u_2 = (r\beta) \bmod q \ (= r\rho - a_2 q)$.
7. To calculate: $\lambda = rs\sigma \bmod q$
8. To calculate: $v = rw\tau \bmod q$
9. To calculate: $[\lambda]G + [q-u_1]Q_1 + [q-u_2]Q_2 = (X_3, Y_3)$
10. To calculate: $[v]G + [q-u_1]Q_1 + [q-u_2]Q_2 = (X_4, Y_4)$
11. If $E_{X_4}(X_3) \bmod q = \sigma$ the signature is valid, differently it is void.

Correctness of algorithm EDC. For the correctness proof it is necessary to show justice of equalities:

$$[\lambda]G + [q-u_1]\bar{Q}_1 + [q-u_2]Q_2 = (X_3, Y_3) = (X_\alpha, \bar{Y}_\alpha) = [\alpha]G \text{ and}$$
$$[v]G + [q-u_1]Q_1 + [q-u_2]Q_2 = (X_4, Y_4) = (X_k, Y_k) = [k]G.$$

Really, from expression

$$s = [H(M)\rho t + r\rho x + \alpha][rE_{X_k}(X_\alpha)]^{-1} \bmod q$$

we find:

$$\alpha = [srE_{X_k}(X_\alpha) - H(M)\rho t - r\rho x] \bmod q = [\lambda - H(M)\rho t - r\rho x] - a_3 q$$

Then:

$$[\alpha]G = [\lambda - H(M)\rho t - r\rho x - a_3 q]G = [\lambda]G - [H(M)\rho][t]G - [r\rho][x]G - [a_3][q]G =$$
$$= [\lambda]G + [q-u_1]Q_1 + [q-u_2]Q_2.$$

On the other hand:

$$[\lambda]G + [q-u_1]Q_1 + [q-u_2]Q_2 = \{\lambda + [q - H(M)\rho t (\bmod q)] + [q - r\rho x (\bmod q)]\}G = [\lambda]G -$$
$$-[H(M)\rho][t]G - [r\rho][x]G - [a_3][q]G = [\lambda - H(M)\rho t - r\rho x - a_3 q]G = [\alpha]G.$$

Similarly from expression

$$v = [H(M)\rho t + r\rho x + k][rE_{X_\alpha}(X_k)]^{-1} \bmod q$$

we find:

$$k = [wrE_{X_\alpha}(X_k) - H(M)\rho t - r\rho x] \bmod q = [v - H(M)\rho t - r\rho x] - a_3 q$$

Then:

$$[k]G = [v - H(M)\rho t - r\rho x - a_3 q]G = [v]G - [H(M)\rho][t]G - [r\rho][x]G - [a_3][q]G =$$
$$= [v]G + [q-u_1]Q_1 + [q-u_2]Q_2.$$

On the other hand:

$$[v]G+[q-u_1]Q_1+[q-u_2]Q_2 = \{v+[q-H(M)\rho t(\mathrm{mod}\, q)]+[q-r\rho x(\mathrm{mod}\, q)]\}G = [v]G - [H(M)\rho][t]G-[r\rho][x]G-[a_3][q]G = [v-H(M)\rho t-r\rho x-a_3 q]G = [k]G.$$

Thus, the algorithm correctness is proved.

On an algorithm design on each complexity the closed and open keys which are used at formation and checks authenticity of the signature accordingly are generated. Besides, parameter σ is calculated as value the enciphering block of co-ordinate X_α of point $[\alpha]G=(X_\alpha,Y_\alpha)$ on co-ordinate X_k of point $[k]G=(X_k,Y_k)$, i.e. $\sigma=E_{X_k}(X_\alpha)\bmod q$, that considerably raises firmness of algorithm EDC at the expense of firmness of applied algorithm of enciphering as X_α and X_k -as casual parameters it is known only signed, X_3 and X_4 -are calculated in dependence of the certificated open keys on algorithm of check of the signature.

These features of the offered algorithm allow increasing firmness EDC. Besides, though binding coefficient Δ is determined from some degree $\mu>2^{256}$ of unknown parameter *R* in a final field, information of value Δ does not allow direct calculation of value *R*.

The entered binding coefficient allows is hidden value of coefficient *R*. Besides, at algorithm of formation EDC casually chosen numbers *k* and α on which are entered, using base point *G* , casual points $[k]G=(X_k,Y_k)$ and $[\alpha]G=(X_\alpha,Y_\alpha)$ are accordingly calculated. In a combination of binding coefficient Δ with co-ordinates of these points $[k]G=(X_k,Y_k)$ and $[\alpha]G=(X_\alpha,Y_\alpha)$, chosen signed, parameters of algorithm of formation EDC that allows to increase reliability of algorithm of formation of the signature are calculated. And by value ciphered blocks, i.e. equality $E_{X_4}(X_3)\bmod q=\sigma=E_{X_k}(X_\alpha)$ it is checked the signature validity that allows increasing reliability of algorithm of check of the signature.

3. Cryptographic protection of the information in information telecommunication systems with application of composite models

3.1 Cryptographic protection of the information

The cores question information protection: privacy, integrity, non-failure operation from authorship and maintenance of working out of steady keys. Conformity of cryptographic means of decisions of these questions; data encryption algorithm (DEA), functions hash (FH), the electronically-digital signature (EDS) and the generator of working out pseudo-casual sequences. Necessity for process protection of an exchange of electronic documents in information - communication networks, from Creations of means EDS and FH.

Further short data shown to qualities for application in uniform information communication networks with creation of standards data encryption algorithm (DEA) and requirements shown to use are presented.

3.2 Uses of symmetric algorithms

If DEA is symmetric algorithm of enciphering for maintenance of privacy of an exchange of electronic documents in communication networks, in that case completeness and

authenticity maintenance of the decision of problems EDS is carried out on the given function chart (Fig. 1).

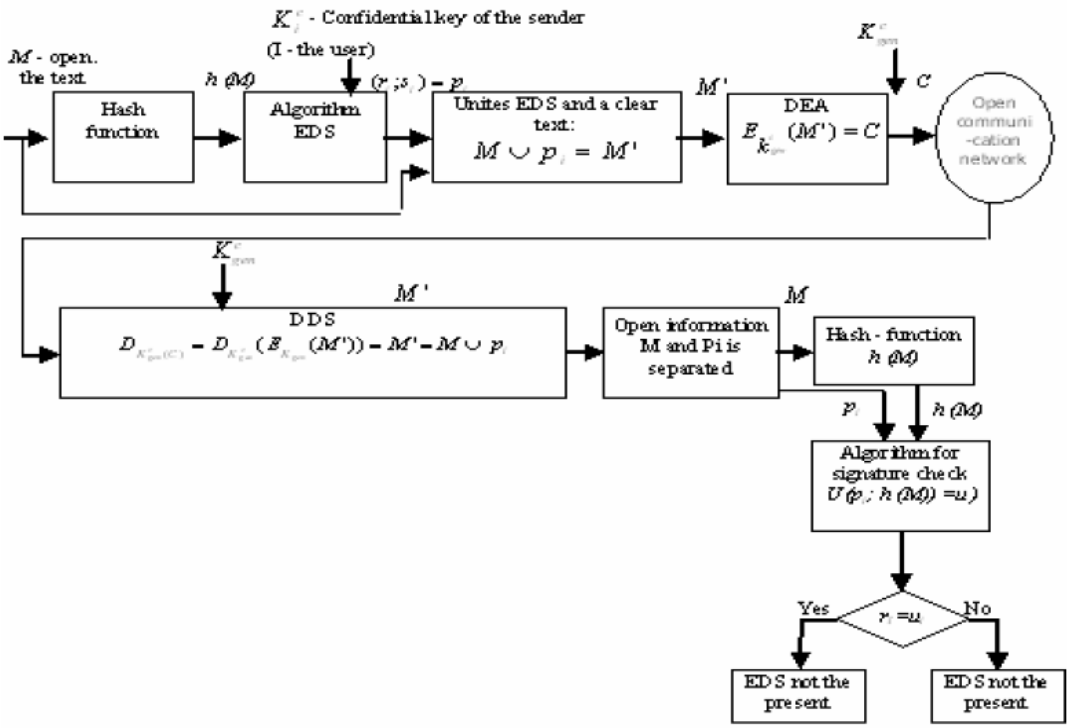

Figure 1. Enciphering by symmetric algorithm

EDS it is formed on the bases of algorithm of digital signatures - $(r_i, s_i) = p_i$ paired relationship of numbers on *h (m)* hash by cost of sent *M* of data and $(k_i^c$ *i* -user) a confidential key of the sender;

The subsequent, *M* sent given and formed $(r_i, s_i) = p_i$ - paired relationship of numbers as EDS unite expanded on once data

$$M \cup p_i = M^{'}$$

the general *c gen k* symmetric key is ciphered

$$E_{K_{gen}^c}(M') = C$$

with algorithm of enciphering also it is passed through an open communication network in the user-*j*;

The receiving party *C* ciphered will decryptions the given k_{gen}^c (general key) a key

$$D_{k_{gen}^c}(C) = D_{k_{gen}^c}(E_{k_{gen}^c}(M^{'}) = M^{'} = M \cup p_i$$

$$_c$$

$$M^{'} = M \cup p_i$$

$M' = M \cup p_i$ from the expanded data the initial open given M for $h(M)$ hashing separates $h(M)$;

The result hashing and $h(M)$ expressing the signature paired relationship of numbers, $(r_i, s_i) = p_i$ is initial cost for algorithm of check EDS, it is considered on them

$$u_i(p_i, h(M)) = u_i$$

It is compared numbers and $r_i u_i$

• if is, $r_i = u_i$ in this case the signature present, i.e. the electronic document present.

• if is, $r_i \neq u_i$ in this case the digital signature is not the present, i.e. the electronic document not present.

3.3. Uses of asymmetric algorithms

If DEA is asymmetric algorithm of enciphering for maintenance of privacy of an exchange of electronic documents in communication networks, in that case completeness and identification maintenance of the decision of problems EDS is carried out on the given function chart (a Fig. 2).

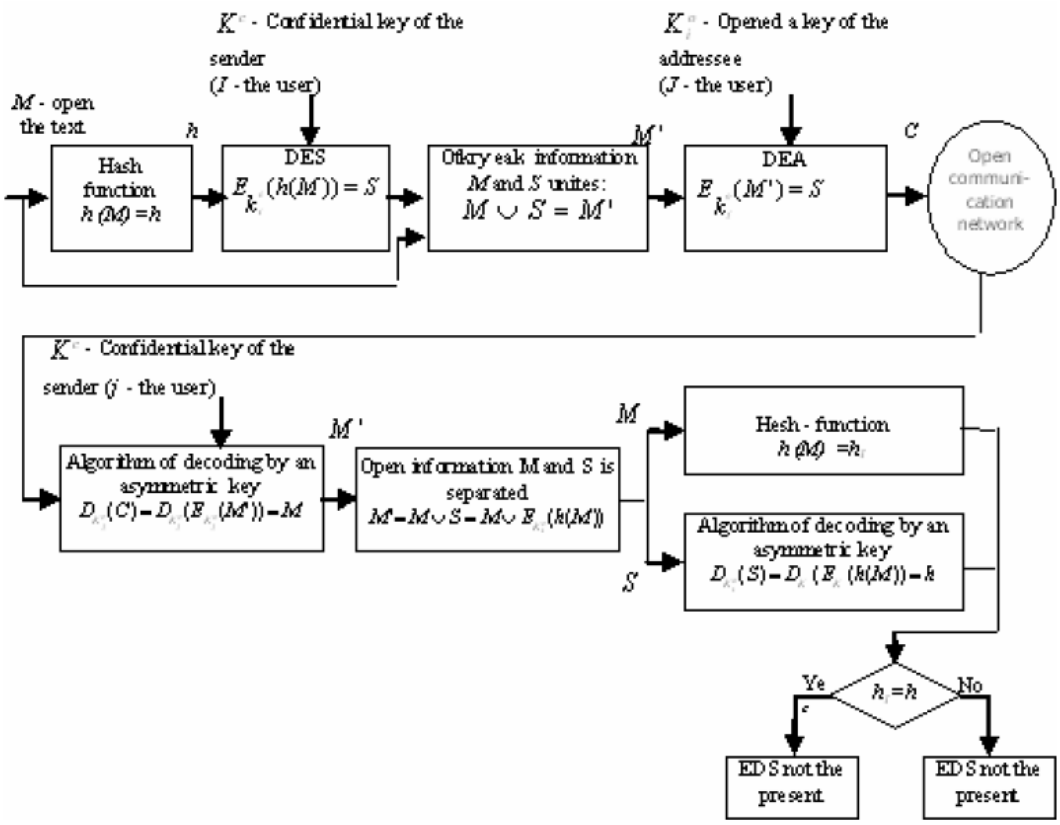

Figure 2. Enciphering by asymmetric algorithm

To such images if the user - *i* wishes to send confidential data confirmed with EDS to the user - *j*, it is carried out in the following manner.

1. The given *M* with the help it is known to all users in networks hash functions it is compressed $h(M) = H$;

2. Hash-value is ciphered $h(M) = H$ to sweep asymmetric DEA $E_{k_i^c}(h(M)) = S$

3. The *M* a clear text and *S* digital the signature unites, is ciphered by means of an open key of the addressee k_j^o of data

$$E_{k_j^o}(M \cup S) = E_{k_j^o}(M) \cup E_{k_j^o}(S) = E_{k_j^o}(M) \cup E_{k_j^o}\left(E_{k_i^c}(h(M))\right) = C_1 \cup C_2 = C$$

4. Cipher information C sending to the user - *j* (addressee)

Used–*j* with the help the confidential key will decryptions k_j^c acceptances ciphered

$D_{k_j^c}(C) = D_{k_j^c}(E_{k_j^o}(M)) \cup D_{k_j^c}(E_{k_j^o}(E_{k_i^c}(h(M)))) = M \cup E_{k_i^c}(h(M))$ here the expressing is frequent EDS is not decoded $E_{k_i^c}(h(M))$.

5. By means of k_i^o the-opened key of the user-*i* the expressing is frequent EDS it will be decoded and turns out $E_{k_i^c}(h(M))$ $h(M)$hash values.

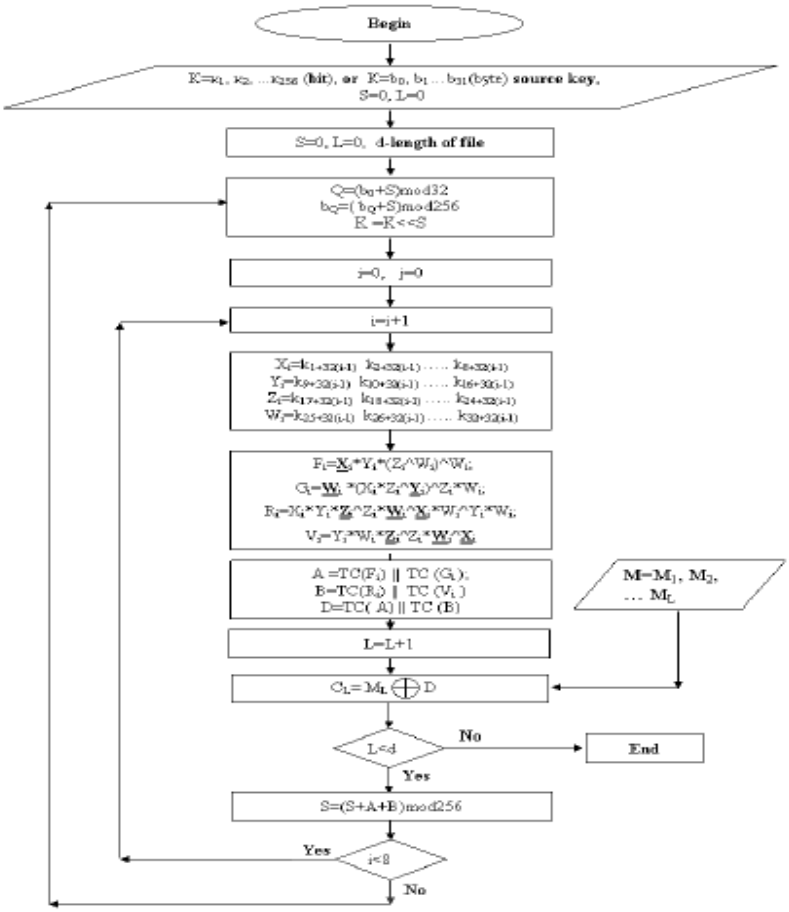

Figure 3. Block schemes of stream cipher algorithm.

6. It is compared hash values of the user – *j* c hash by value of M opened data received on 4 level if they are equal that electronic document present, otherwise electronic document not the present. Correctness EDS means integrity of the information and guarantees authenticity of its source In modern information-communication networks there is a high need for a protection of documentary, sound and video information. Protection of documentary information is provided by means of confidentiality, EDS, generation and distribution of keys among users along with application of hardware software and program cryptographic means. Meanwhile, protection of sound and video information can be maintained with the help of confidentiality, generation and distribution of keys.

4. Estimation crypto stability of the stream cipher algorithm

4.1. The developed new stream cipher algorithm

On the basis of the specified requirements the developed stream cipher algorithm will be tested. The block the scheme of the new developed stream cipher algorithm is shown in Fig.3.

Entrance data:

Source key - $K [k_1, k_2, k_3, \ldots, k_{254}, k_{255}]$ (in bits), $K [b_0, b_1, b_2, \ldots, b_{30}, b_{31}]$ (in bytes)

Table 1. The table compression (TC) - TC [16] [16] - one-byte values is compressed to half-byte

x/y	0	1	2	3	4	5	6	7	8	9	10	1	12	13	14	15
0	5	13	6	11	1	10	15	8	0	4	7	9	2	12	3	14
1	8	7	2	14	15	3	11	6	1	12	13	10	5	4	9	0
2	14	2	13	4	12	7	1	11	6	9	0	5	3	10	8	15
3	0	14	9	12	3	13	7	4	15	6	5	1	11	2	10	8
4	3	10	7	2	4	12	9	1	14	13	15	8	0	5	11	6
5	2	3	1	8	0	14	5	9	12	11	6	7	10	15	13	4
6	10	4	14	15	9	5	8	2	11	0	1	3	12	6	7	13
7	11	9	10	1	6	4	13	15	3	5	14	0	8	7	2	12
8	1	0	3	7	13	11	10	12	9	14	4	6	15	8	5	2
x/y	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**1**	**12**	**13**	**14**	**15**
9	4	8	11	9	14	6	2	5	10	3	12	15	7	13	0	1
10	9	12	15	0	2	1	14	10	5	8	11	13	4	3	6	7
11	6	11	8	13	7	9	0	3	4	15	10	2	14	1	12	5
12	15	1	0	5	10	8	3	7	13	2	9	12	6	14	4	11
13	12	5	4	10	11	2	6	13	8	7	3	14	1	0	15	9
14	7	15	12	6	5	0	4	14	2	10	8	11	13	9	1	3
15	13	6	5	3	8	15	12	0	7	1	2	4	9	11	14	10

Stages:

1. To - 256 bit key is divided into 8 parts on 4 bytes:

$$X_i=b_{i*4};\ i = \text{from } 0 \text{ to } 7$$
$$Y_i=b_{i*4+1};$$
$$Z_i = b_{i*4+2};$$
$$W_i = b_{i*4+3}$$

2. Will be received 4 byte block from 4 bytes of the source key with use shown here of logic transformations

$$F_i=\underline{X}_i*Y_i\ (Z_i\hat{}W_i)\ \hat{}W_i;$$
$$G_i=\underline{W}_i\ *\ (X_i*Z_i\hat{}\underline{Y}_i)\ \hat{}Z_iW_i;$$
$$R_i=X_i*Y_i*\underline{Z}_i\hat{}Z_i*\underline{W}_i\hat{}\underline{X}_i*W_i\hat{}Y_i*W_i;$$
$$V_i=Y_i*W_i*\underline{Z}_i\hat{}Z_i*\underline{W}_i\hat{}\underline{X}_i$$

Xi - operation of logic negation NOT, * - operation of logic multiplication AND, ^ - logic operation XOR.

3. The received 4 byte block (Fi, Gi, Ri, Vi)2 times is compressed with the table of compression (**Table 1**) to 1 byte

$$A = TC\ (F_i)\ ||\ TC\ (G_i);$$
$$B = TC\ (R_i)\ ||\ TC\ (V_i);$$
$$D = TC\ (A)\ ||\ TC\ (B)$$

|| - Here concatenation half-byte results of compression and reception byte values.

4. Received byte value D will addition with 1 byte of plain text M by logic transformation XOR and

received ciphertext C:

$$C = M \oplus D$$

4. After each 8 cycles is transformed by rule shown here, part of bites and bytes source key:

$$S = (S+A+B)\ mod256$$
$$Q = (b_0+S)\ mod32$$
$$b_Q = (b_Q+S)\ mod256$$
$$K = K <<S$$

<<-here cyclic shift 256 bit keys on S positions

6. By quantity in bytes of length of a plain text 1-5 stages will be repeating.

4.2 Crypto stability of the stream cipher algorithm

Simplicity a used transformations is estimated by possibility of their effective application in hardware and program realization. The factor non-linearity cryptographic transformations is estimated with adduction them in models type Boolean function $Y = : GF(2^n) \text{->} GF(2^m)$. The characteristic Boolean function every transformations is analyzed for non-linearity.

The indicator of nonlinearity of cryptographic transformations is estimated with their reduction in model a Boolean function

$$Y = \varphi(X) : GF\ (2^n) \rightarrow GF\ (2^m)$$

Properties Boolean functions of each transformation it was analyzed on nonlinearity.

In algorithm it is used from 4 nonlinear logic functions F, G, R, V which can be described as $GF(2^4) \rightarrow GF\ (2^4)$

Irreversibility of transformations is provided with use of the table of compression (TC) shown on Table 1 as one byte of the information is compressed to half-byte. From half-byte calculation exact value of entrance byte it is impossible.

Strictly avalanche effect is provided in 5 stage with transformations mod256, mod32, K =K <<S.

The estimation to accidents generated sequences were conducted by program designed Xi-square criterion Pearson. Generated sequence miscellaneous from 100 to 1500 bits was tested on accident. As a result grade to accidents to pseudo-casual sequence lie within 85-100% independently any initial secret key. It was revealed also absence of the possibility to generations of the long sequences of "0" or "1". The estimation strictly avalanche effect was tested by spreading in secret key of the error at one bit on generated to sequences.

As a result of modification one bits of secret key is extended to the whole generated pseudo-casual sequence.

The estimation of absence of short cycles of the developed sequence or the maximum period depends on every possible conditions of the generator of pseudo-casual sequence. Every possible 256 bit keys make a condition 2^{256}. Every possible conditions of function of feedback 5 stages are equaled on mod256 is equal on 2^8 and on 8 cycles is equal on 2^3. Or the maximum period of generated pseudo-casual sequence is equaled by an every possible condition of the generator on $2^{256}*2^8*2^3=\mathbf{2^{267}}$

Estimation to stability to different types crypto attacks:

The length of a key 256 bits excludes possibility of a finding of a confidential key full try.

The finding of a confidential key by fragments of the developed sequence is led to a problem in which it is known 1 byte of scale and it is necessary to find 4 bytes of an initial key. Complexity of calculation of possible values of 4 bytes to the compression table makes 2^{24} on the basis of return calculation 3 stages. The finding at known 8 byte to scale makes 256 bit initial keys $(2^{24})^8=2^{192}$; At known 1 byte of scale exact a prediction the following 1 byte of scale does not exceed probability 1/256.

Nonlinearity of used logic functions F, G, R, V excludes application differential and linear cryptanalysis.

Every development cryptographic algorithms will estimated with several approaches. Methods and instruments of the estimation crypto stability stream cipher algorithm and in particular new designed stream cipher algorithm of the encryption, as well as were brought received real test results.

5. Conclusion

In this paper the idea of working out of algorithm EDC was developed using operations of algebra parameters. Mathematical model of the digital signature, including parts of formation and the signature check, satisfying to conditions of demanded firmness in a composition of algorithm of enciphering and existing complexities of calculations are developed. Also the review on methods of estimation crypto stability of stream cipher algorithm of enciphering and practical results of an estimation of the new developed algorithm are resulted. Also the criteria of protection documentary, vocal and information video in information-communication systems and using cryptographic means were considered in this paper.

References

[1] Pr. D.E. Akbarov, S.O. Sabirov, E.J. Azizov “Latent Use of parameter R of the Elliptic Curve, As Parameter of Check EDS, with Application of Algorithm of Enciphering” Proceeding on ITPA 2009 (Sept. 21 ~ 25, 2009), pp.187-191.
[2] Turaev Baxtiyor Temirovich, Komolov Madras Erkinovich, Adenov Bekzod Erkaboevich “Cryptographic protection of the information in information telecommunicationsystems with application of composite models” Proceeding on ITPA 2009 (Sept. 21 ~ 25, 2009), pp.192-195
[3] Musaev Anvar Isakovich “Estimation cryptostability of the stream cipher algorithm” Proceeding on ITPA 2009 (Sept. 21 ~ 25, 2009), pp.196-199
[4] Alfyorov A.P, Zubov A.Y, Kuzmin A.C., Cheremushkin A.V. of a cryptography basis: the manual, 2-editions : Gelios APB, 2002 480 p.
[5] Shnayer B. Applied cryptography. Reports, algorithms, initial texts in language C. M.: publishing house TRIUMPH, 2003 – 816 p.
[6] Akbarov D.E. Ahborot havfsizligini ta’minlashning kriptografic usullari va ularning qo’llanilishi.-Toshkent, “O’zbekiston markazi” nashriyoti, 2009.-432. («Cryptographic methods at protection of the information and their application» publishing house CENTRE UZBEKISTAN, 2003)
[7] Kharin Ю. C, Bernik V. I, Matveev G. V, Agievich S. G «Mathematical and computer bases of cryptology» Open Company «New knowledge» 2003 381 with.
[8] Moldavjan A. A, Moldovayn N.A. introduction in cryptosystem with an open key. Sank- Petersburg "BhV-Peterburg" 2005г. 288с.
[9] Alfyorov A.P, Zubov A.Y, Kuzmin A.C., Cheremushkin A.V. of a cryptography basis: the manual, 2-editions : Gelios APB, 2002 480 p.
[10] Shnayer B. Applied cryptography. Reports, algorithms, initial texts in language C. M.: publishing house TRIUMPH, 2003 – 816 p.
[11] Akbarov D.E. Ahborot havfsizligini ta’minlashning kriptografic usullari va ularning qo’llanilishi.-Toshkent, “O’zbekiston markazi” nashriyoti, 2009.-432. («Cryptographic methods at protection of the information and their application» publishing house CENTRE UZBEKISTAN, 2003).
[12] Dmitry Sklyarov. Art of protection and information breaking St.-Petersburg "BHV-PETERBURG 2004
[13] V.V. Lidovsky. The Information theory Moscow 2003
[14] G.Korobejnikov, J.A.Gatchin, Mathematical bases of cryptology the manual. St.-Petersburg 2004
[15] Молдовян А.А., Молдовян Н.А. Криптография от примитов к синтезу алгоритмов [Book]. - Санкт-Петербург :
[16] Издательство "БХВ-Петербург", 2004. - стр. 448.
[17] Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры [Book]. - Санкт-
[18] Петербург : Издательство "БХВ-Петербург", 2002. - стр. 439.
[19] G. Z. Xiao and J. L. Massey "A spectral characterization of correlation-immune functions," [Conference] // IEEE Trans.
[20] Inform. Theory. - May 1988. - pp. 569-571.
[21] P.Camion, C. Carlet, P. Charpin and N. Sendrier "On correlation-immune functions," [Article] // Advances in
[22] Crypology: Crypto '91 Proc.in Lecture Notes in Computer Science. - Berlin : Springer-Verlag, 1991 г.. - стр. 87-100.
[23] Siegenthaler T. "Correlation-immunity of nonlinear combining functions for cryptographic
[24] applications," [Conference] // IEEE Trans. Inform. Theory. - Oct. 1984. - стр. 776-780.
[25] Харин Ю.С., Берник В.И., Матвеев Г.В, Агиевич С.В. Математические и компьютерные основы криптологии: Учебное пособие [Book]. - Минск : ООО "Новое знание", 2003. - стр. 382.
[26] Moldovyan, N.Moldovyan, N. Goots, B. Izotov. Modern Cryptography: Protect Your Data with Fast Block Ciphers Ю.С., A-LIST Publishing © 2003 (412 pages)