I. Kurzheievskyi, senior teacher,
Y. Tolmachova, student,
A. Shumkova, student.
Nakhimov's Navy Academy of Ukraine, Sevastopol
Dybenko St. 1A, Sevastopol, 99028

INCREASE OF THE CRYPTOSTRENGTH OF ELECTRONIC DIGITAL SIGNATURE SCHEME ELGAMAL WITH COMPOSITE MODULUS

This article deals with the questions of improving the cryptostrength of the algorithm of electronic digital signature (EDS) ElGamal with a composite module, based on the complexity of solving the factorization problem. To improve the reliability of electronic digital signature schemes with a composite module authors suggest using an additional parameter H', which is the hash value of the shared key users K, formed on the Diffie-Hellman parameters and signature r and S.

Keywords: electronic digital signature, the factorization problem, the Diffie-Hellman algorithm.

Introduction. The application of information technologies and use of information communications systems in different spheres of activity of society led to peaking of a problem of information security from illegal access. Now the majority of the organizations transferred to electronic document management. For support of integrity of electronic documents and giving of the legal significance to them the digital signature is widely used.

The electronic digital signature provides check of integrity of documents, establishment of the person who has sent the document that allows to improve procedure of preparation, delivery, the account and document storage, to guarantee their reliability. The sign-code signature represents rather small amount of the additional digital information transferred together with the signed text. In procedure of generation of EDS the secret key of the message sender, and in procedure of verification of the signature - public key of the sender is used.

In procedures of formation and check of a digital signature is used a hashing function. Hashing function – it is the oblate binary submission of the main message of arbitrary length. Function of hashing shall possess the following properties:

- hashing function can be applied to the document of any size;
- output value of hashing function has the fixed size;
- hashing function is sensitive to various changes in the text, such as insertions, swaps, etc.;
- hashing function shall be unidirectional, that is possess property of irreversibility;
- probability of that values of hashing functions of two different documents will match, shall be insignificant is small [1].

Wide application received the EDS scheme ElGamal with a simple module p, which, in the opinion of many experts, in some cases not provide the reliability required. Therefore, it is advisable to use a digital signature scheme ElGamal with a composite modulus [3].

To improve the cryptostrength of schemes EDS ElGamal with a composite module in this article, the authors propose to use an additional parameter H', which is the hash value of the shared key K, formed on the Diffie-Hellman algorithm [2] and the parameters of the EDS r and S.

Main material of research. Consider the signature algorithm with a composite module, based on the complexity of the solution of the factorization problem. The use of electronic digital signature schemes in such a system of El-Gamal, a composite modulus instead of simply due to the fact that a large number of these schemes do not provide resistance to attacks based on the computation of signatures by selecting parameter r in form $r = \alpha^t y^u \bmod p$. Parameter r sets in the equation signature generation unknown k, which varies with each procedure signature generation. This is to prevent attacks related to the attempt to calculate the private key from the equation of signature [3].

In such attacks requires knowledge of the Euler function of the module, so they can be removed using a composite module, such modules in the system RSA.

A row of possible diagrams of implementation of a digital signature with the composite module, an one-time session key *k* and additional parameter H' is provided in the table 1.

Table 1 – EDS options with a composite unit and an additional parameter H'.

№	Check equation signature	The equation of signature	Signature
1	$r^H = y^r \alpha^S \bmod n$ $H_1 = h(r, S, K)$	$kH = xr + S \bmod q'$ $H' = h(r, S, K)$	(r, S, H')
2	$\alpha^H = y^r r^S \bmod n$ $H_1 = h(r, S, K)$	$H = xr + kS \bmod q'$ $H' = h(r, S, K)$	(r, S, H')
3	$r^H = y^{rS} \bmod n$ $H_1 = h(r, S, K)$	$kH = xrS \bmod q'$ $H' = h(r, S, K)$	(r, S, H')
4	$r^H = y^{r+S^2} \bmod n$ $H_1 = h(r, S, K)$	$kH = xr + S^2 \bmod q'$ $H' = h(r, S, K)$	(r, S, H')
5	$r^S = \alpha^{r+H} \bmod n$ $H_1 = h(r, S, K)$	$kS = r + H \bmod q'$ $H' = h(r, S, K)$	(r, S, H')

Where n – a composite module, which is a product of large prime numbers p and q; H – the hash of the document; x – the private key; y – public key; q' –generated a large prime size of 160-256 bits, which is a subgroup of large prime numbers $p-1$ and $q-1$; α – the smallest number such that $\alpha^{q'} \bmod n = 1$; the parameter signature r is given by: $r = \alpha^k \bmod n$ [2] ; K – a shared secret key generated by Diffie-Hellman; H' – hash concatenation of numbers, K, r and S; a set

of numbers (r, S, H') is the signature of the document. A detailed discussion of the algorithm signature generation and verification on the example of scheme 1, presented in table 1.

The owner of the private key selects two large prime numbers p and q multiplies them to obtain the module:

$$n = pq \tag{1}$$

Values of prime factors p and q are kept secret or destroyed after computing the Euler function:

$$\varphi(n) = (p-1)(q-1). \tag{2}$$

User A selects as the private key x belonging to the set $x \in \{1, ..., q'-1\}$. To ensure the impossibility of calculating the private key x on the basis of the known signature public key y is used:

$$y = \alpha^x \bmod n. \tag{3}$$

For a potential intruder to generate the signature equation has two unknown sizes: x and k. Therefore, he has no opportunity is likely to compute a secret key x. Therefore, he has no opportunity is likely to compute a secret key x.

When you create a electronic digital signature parameter k must be a one-off, because the signature generation r and S to two different messages having the prerequisites for the calculation $\varphi(n)$ and the secret key x. With two signatures have the following system of two equations with the unknown x and $\varphi(n)$ that the attacker can decide:

$$h(m) = xr \bmod \varphi(n) \tag{4}$$

$$h(m) = xS \bmod \varphi(n) \tag{5}$$

Length of number α can be chosen rather small (less than a size of used values p and q), such that:

$$\alpha^{q'} \bmod n = 1 \tag{6}$$

Open information of the subscriber A are numbers (y, n, α).

From Scheme 1 by the equation of signature subscriber A is calculated parameter r:

$$r = \alpha^k \bmod n. \tag{7}$$

To improve the cryptostrength of electronic digital signature scheme with a composite module can also be applied the algorithm Diffie-Hellman.

A shared secret key K for subscribers A and B is formed as follows. Subscribers know some two numbers g and p' that are not confidential and may be known to other interested parties (p' – a random prime number, g – a primitive root module p'). In order to create, unknown to anyone

over the secret key, both parties generate large random numbers: user A - the number a, the subscriber B – number b. Then a subscriber A calculates:

$$A' = g^a \bmod p' \tag{8}$$

and sends it to the subscriber B, which calculates:

$$B' = g^b \bmod p' \tag{9}$$

and transfers the subscriber A. In the second stage the first person on the basis of available a and received on the network B' calculates:

$$B'^a \bmod p' = g^{ab} \bmod p', \tag{10}$$

and the other person on the basis of available numbers b and A' calculates:

$$A'^b \bmod p' = g^{ab} \bmod p'. \tag{11}$$

Thus, subscribers A and B forms the shared secret key K as follows:

$$K = g^{ab} \bmod p'. \tag{12}$$

The attacker will meet almost impossible (for a reasonable time), the problem of computing (11) or (12) in the intercepted $g^a \bmod p'$ and $g^b \bmod p'$, if the numbers p', a and b selected large enough [4]. In practical implementations for a and b are used numbers about 10^{100} and p' about 10^{300}.

From scheme 1 by the equation of signature (see table 1) is calculated S:

$$kH = xr + S \bmod q' \tag{13}$$

To everyone's secret key K added values of EDS and a set of numbers r and S and it is hashed. The resulting hash H' is optional digital signature, the use of which, according to the authors, enhances the cryptostrength signature scheme ElGamal with a composite module. Signing the electronic document in this case is a set of values (r, S, H').

Procedure to check the authenticity of the document signed with a digital signature with a composite unit and an additional parameter H', as follows. The recipient has passed an electronic document with a electronic digital signature (r, S, H'). User B knows the value of a public key y, number α and the composite module n, as well as the generated shared secret K.

EDS verification equation, the scheme 1 (see Table 1) is as follows:

$$r^H = y^r \alpha^S \bmod n \tag{14}$$

Calculated separately the left lch and right pch side of the equation:

$$lch = r^H, \tag{15}$$

$$pch = y^r \alpha^S \bmod n. \tag{16}$$

Recipient of an electronic document shall concatenation formed previously shared secret key K and the parameters r and S:

$$M = K \| r \| S \tag{17}$$

and computes a hash H_1:

$$H_1 = h(M). \tag{18}$$

If both sides of the equation are equal and $H' = H_1$ validation (user B can be sure that the subscriber A knows the shared secret key K), then the digital signature corresponds to the document, and it can be considered authentic. If the results differ, the signature forged.

For a software implementation of modified signature schemes with a composite module, shown in Table 1, the selected object-oriented programming language Java programming environment and NetBeans IDE 7.0.1. The Java language has such advantages as multitasking, support for Internet protocols and multiple platforms.

Consider the results of the signature algorithm with a composite module on the Java programming language in the environment NetBeans IDE 7.0.1:

Generated a large prime numbers:

q' = 22309695667816411565143736 12860150572827242382955591950668225474862195232833177;

p = 32125961761655632653806980025186168248712290314560524089622446838015611352797748 9;

q = 58005208736322670069373713934363914893508301956845390717373862346417076053662602 1.

Composite module n = 18634731178399553393445422055225217906696381624222908727345434830884113863348947299283825527892199622535851214871045499812712879698244643846872989336447209964126 9.

The secret key x = 11399724628339681174632203768855988487809088413097655879377150053016373924122 9.

A one-time secret key k = 11953879415841651271422144285746235378795161096097640803599045936013867239462 45.

The public key y = 17110713605751079860846482549812935427692807757264806993865214343984593746252904189634623441464061874028733297035969295671860601771413917749397035823187261054441.

The smallest number of α, such that $q'^{\alpha} \bmod n = 1$:

α =43333.

Formed a shared secret key K = 22215858046529138111949802472177706837106896625663263470867113862818175878683 14.

Electronic digital signature is a set of numbers (r, S, H'):

r = 12293626409530795524058344999624980430219055805489704380170418409403089282856007851446156690401547400624155608059602328905081087475429430037752035541137 4104458302;

S = 13106706031451077244415217781068040918391215270201913865637892952215916635777 05;

H' = 74826547982636546812734598473821774 32.

The left side of check lch = 10743725797184136866718230211392336317084611634004497185732061709455078138585664284075768456884562453313241837909123871881635419523300404438364991032912660258920.

The right side of check pch = 10743725797184136866718230211392336317084611634004497185732061709455078138585664284075768456884562453313241837909123871881635419532330040443836499103291266025892 0.

The resulting hash value H_1 = 74826547982636546812734598473821774 32.

Transferred a hash value H' = 74826547982636546812734598473821774 32.

Both sides of checks are equal, therefore the electronic digital signature corresponds to an electronic document, and it can be considered authentic.

Conclusions. Realized in language of object-oriented programming of Java in the environment of NetBeans IDE 7.0.1 algorithms of EDS with the compound module and the additional parameter which cryptofirmness is based on the solution of a problem of factorization, passed test for correctness of results of formation and digital signature check. Use of the compound module and additional parameter allows to construct more cryptostrength schemes of EDS in comparison with a case of use of the simple module that accelerates process of creation and EDS check.

BIBLIOGRAPHY

1. Barichev S.G. The foundations of modern cryptography. / SG Barichev, RE Serov. - M.: Hotline - Telecom, 2002. - 175 p.

2. Venbo Mao. Modern Cryptography: Theory and Practice. / - Moscow Williams Publishing House, 2005. - 297 p.

3. Moldovyan N.A. Public-key cryptography. / N.A.Moldovyan, A.A.Moldovyan, M.A.Eremeev. - St.: BHV - Petersburg, 2004. - 288 p.