ALGORITHM OF THE DIVISION OF THE CONFIDENTIAL KEY OF THE DIGITAL SIGNATURE

Kurzheievskyi I.V., Holubieva H.K.
Naval Academy named after P.S. Nakhimov, Ukraine
E-mail: anettsun@gmail.com

Abstract — The questions of the division of a confidential key of a digital signature without a disclosure of parts are considered.

1. Introduction

The protocol is a distributed algorithm with two and more participants. The cryptographic protocol solves, at least, one of three problems of cryptography: the ensuring confidentiality, the integrity, and a not traceability [1]. Protocols of a secret division are needed to solve an information storage problem in such way that those groups of people which would be allowed to know a secret — could restore it, and those groups which are not allowed to know a secret, couldn`t restore it even by search [2]. The protocol of division of secret consists of two main phases [3].

1) On a distribution phase, or divisions of secret — the dealer knowing a secret of *m*, generates *n* of parts of secret of *m*1, *m*2, … , *mn* and sends *mi* share to the participant of *Pi* (*i*=1,…, *n*) on the defended communication channel. Distribution has to be organized so that the resolved groups of participants, having gathered, could restore unambiguously *m* secret, and not resolved — couldn't.

2) On a phase of restoration of secret any group of structure of access of unites the parts of secrets of *mi* (*i*=1…, *n*) so that to receive *m* secret.

2. Main part

Protocols of secret division are applied to the distributed storage of information. Most often confidential keys or passwords of any subscriber appear such information.

Secret division, or division of keys, represents procedure of crushing of a confidential key on some parts by means of a special technique so that possibility of the enciphering or decoding of messages arose only on condition of collecting all parts together. The main destination of this technology is the equal participation in cryptographic operations of several users, who don't trust each other, as the uniform person [3].

Let's present a situation that at the enterprise there is a director and it has three deputies. The director has a confidential key (*Sk*) by means of which he signs various bank documents. But it happened so that the director is compelled to go to hospital, respectively he will have no opportunity to run financial business of the enterprise independently. Therefore it divides the confidential key (*Sk*) into three parts and distributes to each of deputies a share of a key (*S*1*, S2, S*3). Even if all three deputies will want to sign any third-party document by means of association of the parts of a secret, received digital signature won't correspond a document hash value. It will occur because one of parts of a confidential key already contains a document hash value, and to substitute with a hash value of the document intended for signing, on a hash value of other document participants of division of secret won't be able as for the solution of this task it is necessary to know decomposition of a large number of *N* on simple multipliers.

The scheme of secret division, offered by authors, without a disclosure of parts looks as follows:

1) Generate *P* and *Q* with a size of 512 bits.

2) Calculate $N = P \times Q$.

3) Value of function of Euler is defined $Fi=(P-1)\times(Q-1)$.

4) Choose any confidential key $1<Sk<n$.

5) Calculate the open key $Ok=Sk^{-1} \bmod Fi$.

6) The hash value of the document (*H*) will be transformed to numerical value (*M*).

7) Two parts of a confidential key of digital signature – *S1* and *S2*— choose by random way, and the third part is calculated by formula: $S3 = \frac{Sk}{S1 * S2 * M} \bmod Fi$.

The only restriction at a choice of numbers of *S1, S2, S3* and *M* consists that these numbers have to be in pairs mutually simple as among themselves, and with value of function of Euler.

8) Further calculations do by the following formulas:

$$S_A = M^{S1} \bmod N;$$

$$S_{AB} = S_A{}^{S2} \bmod N;$$

$$S_{ABC} = S_{AB}{}^{S3} \bmod N .$$

9) The received value (*SABC*) is erected in degree a document hash value: $S_{ABCM} = S_{ABC}{}^{M} \bmod N$.

10) Thus, without disclosure of shares the correct digital signature under the concrete document of what it is possible to be convinced was created having analyses the following equation

$$Signature = M^{S_A * S_B * S_C} \bmod N = M^{\frac{S1*S2*M*Sk}{S1*S2*M}} \bmod N = M^{Sk} \bmod N .$$

This algorithm is intended for the one-time signature of the concrete document, which a hash value, is hidden in one of the secret parts. If participants of division of secret try to apply the parts of secret to the signature of other document, this signature will be invalid. On parts of secret it is impossible to restore a confidential key of digital signature for acceptable time because operation of restoration of value of confidential key is carried out on the module to equal value of function of Euler, and calculation of value of function of Euler assumes knowledge of decomposition of number *N* on simple multipliers of *P* and *Q*, that is the solution of a problem of factorization.

3. Conclusion

This algorithm was realized in the program —*Aribas*, successfully passed tests for correctness of results of work and can be used as the division algorithm of a confidential key of a digital signature without a disclosure of parts for the information security from the unauthorized access.

4. References

[1] Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. — СПб.: Профессионал, 2004. — 464 с.

[2] Молдовян Н.А. Введение в криптосистемы с открытым ключом / Н.А. Молдовян, А.А. Молдовян. — СПб.: БХВ-Петербург, 2005. — 288 с.

[3] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер.— М.: ТРИУМФ, 2003. — 816 с.