Impact Factor: 9.2 ISSN-L: 2544-980X

PROSPECTS FOR USE OF ELECTRONIC SIGNATURE IN MANAGEMENT OF ELECTRONIC DOCUMENTS IN ENTERPRISES AND ORGANIZATIONS

M.M.Turdimatov[1] , S.S.Askarov[2]

[1]Associate Professor, Department of Information Security, Fergana Branch of TUIT named after. Muhammad al-Khwarizmi

[2] Master's student of the department of "Information Security" of the Fergana branch of TUIT named after Muhammad al-Khorezmi

ANNOTATION: *This article examines the details of an electronic document obtained as a result of cryptographic modification of data using a private key signature and problems of checking data corruption as a result of which several schemes have been developed , It is recommended to create an electronic digital signature. Also based on symmetric and asymmetric encryption algorithms. Other types of electronic signatures (group signatures, irrefutable signatures, reliable signatures) with modified schemes are a solution to problems solved by electronic devices .*

Keywords: *cryptography , electronic document , details , xesh _ function , fixation , electronic digital signature , symmetric and asymmetric encryption , algorithms , modification , group signature , non-repudiation signature, trusted signature , electronic devices.*

INTRODUCTION:

We know that the authorship of the electronic digital signature (DS) allows you to confirm sieve throne document (either a real person or, for example, a crypto currency account in the system). The signature is placed by the author and the document using cryptographic methods. also binds to itself and cannot be forged by simple copying.

Private signature key data using is a requisite of an electronic document obtained as a result of a cryptographic change, and allows you to check the absence of distortions (integrity) of information in the electronic document from the moment the signature is formed [1,2].

A symmetrical keys for encryption based on the following principles. For example, it is possible to create many pairs of numbers (public key and private key) such that, given the public key, the private key cannot be calculated in a reasonable time. The key generation mechanism is clearly defined and well known. In this case, each public key corresponds to a specific private key. If, for example, Ivan Ivanov publishes his public key, you can be sure that he only has the corresponding private key.

There are strong encryption methods that allow you to encrypt a message using a private key only to decrypt it using a public key.

If an electronic document can be decrypted using a public key you can be sure that it is encrypted using a unique private key. If a document is encrypted with Ivan Ivanov's public key, this

confirms its authorship: only Ivanov can encrypt this document, since he is the sole owner of the private key[2].

However, it would be inconvenient to encrypt the entire document, so only its hash is sufficient. encrypted - a small amount of information strictly tied to a document and identifying it using mathematical transformations. The hashing mechanism is well defined and well known. An encrypted hash is an electronic signature.

BASIC ALGORITHMS

There are several schemes for creating an electronic digital signature :

- Symmetric encryption algorithms based on This scheme assumes the presence in the system of a third party - an arbiter, who is trusted by both parties. Authorization of a document is the fact that it is encrypted with a secret key and transferred to the verifier.
- Asymmetric encryption algorithms based on Currently such DS schemes are the most common and widely used.

In addition, there are other types of digital signatures (group signature, irrefutable signature, trusted signature), which are modifications of the schemes described above. Their appearance is associated with the variety of problems solved by electronic devices.

Rules for using hash functions

Hash function yes

Because signed documents have a variable (and usually very large) size, in electronic signature schemes the signature is often placed not on the document itself, but on its hash . Cryptographic hash functions are used to calculate a hash, which ensures that changes made to a document can be detected when the signature is verified. Hash functions are not part of the DS algorithm , so any reliable hash function can be used in the scheme[3,4].

Using hash functions provides the following advantages:

- **Difficulty of calculation.** Typically, the hash of a digital document is made many times smaller than the size of the original document, and hash calculation algorithms are faster than digital signature algorithms. Therefore, creating a document hash and signing it is faster than signing the document itself.
- **Compatibility.** Most algorithms work with strings of data bits, but some use other representations. A hash function can be used to convert any input text into a suitable format.
- **Honesty.** Without using a hash function, some schemes require that a large electronic document be divided into blocks small enough to use an electronic signature. When checking, it is impossible to determine whether all blocks have been received and whether they are in the correct order.

An electronic signature does not have to use a hash function, and the function itself is not part of the electronic signature algorithm, so you can use any hash function or none at all.

Such systems are vulnerable to attacks on public keys because the original text can be obtained by selecting an arbitrary digital signature and applying a verification algorithm to it. Hash along with digital signature, function is used , that is, the signature is calculated not from the document itself, but from its hash. In this case, the verification can only produce a hash of the original text, so if the hash function used is cryptographically strong, it will be computationally difficult to obtain the original text, which becomes this type of attack.

Symmetrical scheme

Symmetric electronic signature schemes are less common than asymmetric ones, since after the emergence of the concept of a digital signature, effective signature algorithms based on the then known symmetric ciphers could not be implemented. Diffie and Hellman, the founders of the concept

of electronic digital signature, were the first to draw attention to the possibilities of a symmetric digital signature scheme. Also, to increase cryptographic power, it is necessary to increase the length of the keys, which leads to the need to rewrite programs that implement asymmetric schemes and, in some cases, redesign the equipment. Symmetric schemes are based on well-studied block ciphers.

In this regard, symmetrical circuits have the following advantages:

- The reliability of symmetric electronic signature schemes is also due to the reliability of the well-studied block ciphers used.
- If a cipher is not strong enough, it can be easily replaced with a more secure one with minimal implementation changes.

However, symmetrical VP also has a number of disadvantages:

- Each bit of transmitted data must be individually signed, resulting in a significantly larger signature. The signature can be twice as long as the message.
- Keys generated for signing can only be used once, since half of the secret key is revealed after signing.

Due to the disadvantages discussed, the symmetric Diffie-Hellman electronic digital signature scheme is not used, but its modification developed by Berezin and Doroshkevich is used, in which several groups of bits are signed simultaneously. This results in a smaller signature size, but an increase in computational effort. To overcome the problem of "one-time use" of keys, the generation of individual keys from the master key is used.

Asymmetrical circuit

Diagram explaining signature and verification algorithms

Asymmetric electronic signature schemes belong to public key cryptosystems.

But unlike asymmetric encryption algorithms, encryption is carried out using a public key, and encryption is carried out using a private key (only the recipient who knows the secret can decrypt), signature in asymmetric DS schemes is carried out using a private key, and verification of the signature is public (any recipient can decrypt and verify the signature).

The generally accepted electronic digital signature scheme covers three processes:

- **Key pair create** Using a key generation algorithm, a private key is selected with equal probability from the set of possible secret keys and is the corresponding public key.
- **Creating a signature.** The signature for a given electronic document is calculated using the private key.
- **Signature verification.** For document and signature data, the validity of the signature is determined using the public key.

electronic digital signature made sense, two conditions must be met:

- Verification of the signature must be performed using a public key that exactly matches the private key used during signing.
- Without a private key, creating a legitimate digital signature must be computationally difficult.

Authentication of a message with an electronic digital signature from code should be distinguished.

asymmetric algorithms are complex. count process there must be

Ensuring this in all asymmetric digital signature algorithms is based on solving the following computational problems:

- restrained logarithm problem (EGSA)
- Factorization problem, that is, the root of the number factorization (RSA).

Electronic signatures are divided into traditional digital signatures and electronic digital signatures with document recovery.

Public Key Management

Public key management, including digital signature systems, is public key management. Since the public key is available to any user, a mechanism is needed to verify that the key belongs to its owner. It is necessary to ensure that any user has access to the real public key of any other user, to protect these keys from being changed by an attacker, and to arrange for the key to be revoked if it is compromised.

The problem of protection against key substitution has been solved with the help of certificates . It allows you to confirm information about the certificate owner and his public key with the signature of any trusted person. There are two types of certification systems: centralized and decentralized. In decentralized systems, each user creates a network of trust by mutually signing certificates from known and trusted individuals. Centralized certification systems use certification authorities managed by trusted organizations.

The CA generates the private key and its own certificate, generates end-user certificates, and verifies their validity using its own digital signature. The center also revokes expired and non-functioning certificates and maintains databases (lists) of issued and revoked certificates. By contacting a certification authority, you can obtain your public key certificate, another user's certificate, and find out which keys have been revoked[5,6].

Storing private keys

The private key is the weakest component of the entire digital signature cryptosystem. An attacker who steals a user's private key can create a valid digital signature for any electronic document on behalf of that user. Therefore, special attention should be paid to how the private key is stored. The user can store the private key on his personal computer, protecting it with a password. However, this storage method has a number of disadvantages, in particular, the security of the key depends entirely on the security of the computer, and the user can sign documents only on this computer.

The following private key storage devices are currently available:

- smart cards
- USB keys
- " tablets " Touch Memory
- registry (in protected computer memory).

Theft or loss of one of these storage devices can be easily detected by the user, after which the corresponding certificate should be immediately revoked.

The most secure way to store your private key is on a smart card. To use a smart card, the user must not only have it, but also enter a PIN code , that is, two-factor authentication is obtained. After this, the document to be signed or its hash is transferred to the card, its processor signs the hash and sends the signature back. When creating a signature this way, the private key is not copied, so there is only ever one copy of the key. Additionally, copying data from a smart card is a little more difficult than from other storage devices.

According to the Law "On Electronic Signature", the owner is responsible for the safety of the private key[7,8].

electronic signatures

electronic signatures will allow the implementation of the following important directions in the electronic economy:

- Full control of the integrity of the transmitted electronic payment document : in the event of an accidental or intentional change in the document, the electronic digital signature loses its legal

force, since it is calculated and compared using a special algorithm based on the original state of the document.

- Effective protection against document alteration (forgery). An electronic signature guarantees the detection of all types of forgery and integrity control. As a result, falsifying documents is often impractical.
- Determination of the impossibility of denying the authorship of this document. This aspect is based on the fact that if you have a so-called private key, then you can create a correct electronic signature, which, in turn, should be known only to the owner of this key (the author of the document). In this case, the owner cannot refuse his signature and, therefore, the document.
- Either one is based on the fact that a valid electronic signature can be created by knowing the key , and by definition it must only be known by the owner-author. The owner of the keys of X document can clearly prove the authorship of the signature under the document. In addition, you can sign only individual fields of the document, such as "author", "modified", "time stamp", etc. That is, not the entire document, but authorship can be proven.

The above features of the electronic digital signature allow it to be used for the following main purposes of the electronic economy and electronic documents and monetary transactions :

- Use in banking payment systems;
- E- commerce (trade);
- Electronic registration of real estate transactions;
- goods and services (customs declaration). Functions of monitoring the execution of the state budget (if we are talking about a country) and monitoring the implementation of budget targets and limits of budget obligations (in this case, if we are talking about an industry or a specific budget institution). Management of government orders;
- in electronic communication systems within the framework of the "Electronic Government " and " Electronic Citizen" projects;
- Formation of mandatory tax, budget, statistical and other reporting to government bodies and extra-budgetary funds;
- Legal organization of intra-enterprise, intranet or national electronic document flow;
- Using DS in various accounting and trading systems, as well as on Forex;
- Management of authorized capital and participation in capital;
- Odin is one of the main components of cryptocurrency transactions.
- **Simple electronic signature** is an electronic signature confirming the formation of an electronic signature by a specific person using codes, passwords or other means.
- **Advanced unqualified electronic A signature** is an electronic signature that:

  - obtained as a result of cryptographic data transformation using an electronic signature key;

  -electronic allows you to identify the person who signed the document;

  - makes it possible to determine the fact of making changes to an electronic document after it has been signed;

  - created using electronic signature tools.

CONCLUSION. In conclusion, we can say that when restoring documents during a DS check , the main part of the document is restored automatically; it is not necessary to attach it to the signature. Traditional digital signatures require a document to be attached to the signature. It is clear that all algorithms that sign a document hash relate to ordinary electronic signatures. Electronic signatures with document recovery include, in particular, RSA.

Electronic signature schemes can be one-time or reusable. In one-time schemes, after verifying the validity of the signature, it is necessary to exchange keys, but in reusable schemes this is not necessary.

Deterministic electronic signatures compute the same signature given the same input data. The implementation of probabilistic algorithms is more difficult because it requires a reliable source of entropy , but given the same input data, signatures can be different, which increases cryptographic strength. Currently, many deterministic schemes have been converted into probabilistic ones.

In some cases, such as data transmission, digital algorithms can be very slow. In such cases, a fast digital signature is used . Signature acceleration is achieved by moving to algorithms with less modular computations and radically different computational methods.

REFERENCES

1. *Ryabko B. Yes.* , *Fionov A. N.* Fundamentals of modern cryptography for information technology specialists - Scientific World , 2004. - 173 p. - ISBN 978-5-89176-233-6.
2. *Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V.* Fundamentals of cryptography. - "Helios ARV", 2002. - 480 p. - ISBN 5-85438-137-0 .
3. *Neils Ferguson* , *Bruce Schnaer* . Applied cryptography: design and implementation of secure cryptographic systems. – M.: Dialectics, 2004. – 432 p. - ISBN 5-8459-0733-0 , ISBN 0-4712-2357-3 .
4. *B. A. Foruzan.* El -Gamal digital signature scheme // Encryption key management and network security / Transl. A. N. Berlin.
5. *Menezes A.J.* , *Oorschot P. Vanstone S.A.* Handbook of Practical Cryptography (English) - CRC Press , 1996. - 816 p. - (Discrete Mathematics and Its Applications) - ISBN 978-0-8493-8523-0
6. *Mao V.* Modern cryptography : theory and practice / trans. D. A. Klyushina - M.: Williams , 2005. - 768 p. - ISBN 978-5-8459-0847-6.
7. Umarov A., Rakhmatov R., Khudaynazarov U. (2023, October). ANALYSIS OF DISCRETE CONVOLUTION IN MATLAB FOR SIGNAL PROCESSING USING FILTERS. At the conference on digital innovation: "Modern problems and solutions".
8. Khusanova M., Rakhmatov R. (2023, October). STUDY OF PROTOCOLS FOR MONITORING AND DETECTION OF MOBILE THREATS. At the conference on digital innovation: "Modern problems and solutions".