ELECTRONIC DIGITAL SIGNATURE ALGORITHMS

Akmuradova Anora Qurbon qizi

Master of the National University of Uzbekistan

ANNOTATION

In today's highly developed entire civilization, the widespread use of documents, including classified documents, in electronic form, and in communication systems, the transmission of electronic documents and electronic signatures, creates the importance of determining the authenticity of electronic documents and electronic signatures.

***Key words**:* hash value, signature formation, signature verification, rejection, integrity.

We will talk about the issue of determining whether the actual amount of information received is invalid, that is, about the essence of the issue of data authentication.

It is quite natural that at the end of the document any paragraph letter is the signature of the person responsible for drawing up the same document as the compiler. This situation usually arises from the following two goals. First, the party receiving the information makes sure that this information is valid by comparing the signature in the information received to the existing signature message. Secondly, a personal signature guarantees legal authorship to the reference document. Such a guarantee, on the other hand, is of particular importance in trade, power of attorney, obligation and similar transactions. The elaboration of personal signatures affixed to documents is relatively complex, and the authors of personal signatures can be identified through the use of current modern advanced criminalistics techniques. But the properties of the Electronic Digital Signature are different from this, depending on the memory register bits, which are determined by the

properties of the binary number system. Copying an electronic signature that consists of a certain of memory bits and placing it somewhere does not cause complexity in the è change computer-based communication systems.

No matter how convenient and cryptocurrencies are, public key cryptographic systems cannot respond to the full resolution of the authentication issue. Therefore, authentication techniques and tools are required to be applied in combination with cryptographic algorithms in a complex.

The following measures are taken to protect against such illegal methods.

- imitation tolerance – impersonality;

- to sort the information entered into the cryptosystem based on the objectives of the protection.

In electronic digital signature communication systems, several types provide protection against rule violations, namely:

- if the secret key is known only to the user (a)himself, then it cannot be denied that the information received by the user (B) was sent only by (A) ;

- possibility of violation of the rules of the communication system of the law violator (opponent party) without knowing the secret key: mediatization, forgery, active modification, masking and other similar

does not give birth;

- eliminates many disagreements in the attitude of users of the communication system to conduct business in connection with each other, and when such disagreements arise, it is possible to clarify without an intermediary.

In many cases, it will be necessary to confirm the information that has been transmitted with an electronic digital signature, without the need to

encrypt it. In such cases, the Open Text is encrypted with the sender's key, and the received cipher is sent along with the Open Text. The party receiving the information can decipher the cipher in the sender's public key, comparing it with the Open Text.

Asymmetric shirring algorithms are not widely used to encrypt large amounts of data, as proven above. Asymmetric encryption algorithms are widely used in the field of cryptography, mainly in Electronic Digital Signature Systems.

REFERENCES

1. Gurstelle W. - Building Bots. Designing and Building Warrior Robots, URL: https://www.biblio.com/book/building-bots-designing-building-warrior-robots/d/1047120377– 2002.

2.Intermediate Robot Building, David Cook, URL: https://www.amazon.com/Intermediate-Robot-Building-Technology-Action/dp/1430227540 - 2010.

3.Jonathan H. Tomkin and Matthew West., (https://stemeducationjournal.springeropen.com/articles/10.1186/s40594-022-

Grades in college and university STEM courses are an important determinant of student persistence in STEM fields. Recent studies have used the grade offset/grade penalty method to explore why students have low...., International Journal of STEM Education 2022 9:27., Research Published on: 17 March 2022.

4. Kuang-Chao Yu, Pai-Hsing Wu, Kuen-Yi Lin, Szu-Chun Fan, Sy-Yi Tzeng and Chih-Jung Ku., Behavioral intentions of technology teachers to implement an engineering-focused curriculum., Citation:International Journal of STEM Education 2021 8:48,Content type:ResearchPublished on: 28 July 2021.