International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 30-34

Electronic Digital Signature

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Sharing electronic documents over the network reduces the cost of processing and storing them, speeds up the search. However, there is a problem with authenticating the author of the electronic document and the document itself, ie determining the authenticity of the author and the absence of changes in the received electronic document. The purpose of authenticating electronic documents is to protect them from possible criminal activity.*

Keywords: verification, secret, subscriber, encryption, secret key, matrix, cryptographic key, encoding key, global network.

INTRODUCTION

1. Electronic digital signature

2. Cryptographic key management

Electronic digital signature

When exchanging electronic documents over the network, the cost of processing and storing them is reduced, the search is faster. However, there is a problem with authenticating the author of the electronic document and the document itself, ie determining the authenticity of the author and the absence of changes in the received electronic document.

METHODS

The purpose of authenticating electronic documents is to protect them from possible criminal activity. Such actions include:

- active detection - intercepts and modifies intruders (files) connected to the network. - masquerade - subscriber S sends documents to subscriber V on behalf of subscriber A;

- renegade - subscriber A says that he sent a message to subscriber B, but did not send it;

- replacement - subscriber V changes the document, or creates a new one and says that he received it from subscriber A;

- repeat - the document sent by subscriber A to subscriber B is repeated by subscriber C.

Digital signatures are similar to simple manuscripts in that they have the following advantages:

- confirms that the signed text belongs to the signatory;

- it does not allow the person to deny his obligations under the signed text;

- guarantees the integrity of the signed text.

The electronic digital signature system performs two main procedures:

- digital signature generation procedure;

- digital signature verification procedure.

Scheme of electronic digital signature formation

Figure 21.1. Digital signature formation procedure.

During the preparation of this procedure, the sending subscriber A generates two keys: the secret key kA. and public key CA. The public key KA is obtained by calculating the secret key kA, which is its pair. The public key KA is distributed to other subscribers of the network for use in signature verification.

Electronic digital signature verification scheme

Figure 21.2. Digital signature verification procedure.

Network subscribers can check the digital signature of the received message "M" with the help of the sender's public key.

Each signature contains the following information:

- date of signing;

- expiration date of this signature key;

- information about the person signing the file (F.I.Sh, position, place of work);

- Signature identifier (public key name);

- The digital signature itself.

Created in the United States in 1977, the RSA system is the first and world-famous electronic digital signature system and implements the above principles. Developed in 1984 by El Gamal, the digital signature algorithm is characterized by high reliability and ease of implementation on personal computers.

Cryptographic key management

The following requirements apply to the distribution of keys:

- efficiency and accuracy of distribution;

- Confidentiality and integrity of distributed keys.

The following basic methods of distributing keys among users of computer networks are used.

1. Use one or more key distribution centers.

2. Direct exchange of keys between network users.

The problem with the first method is that the key distribution center knows to whom and which keys have been distributed. This allows you to read all the messages being transmitted over the network. Potential abuses can lead to serious network security breaches. The problem with the second method is to make sure that the network subjects are genuine.

The method of open distribution of keys, invented by U. Diffie and M. Hellman, allows users to exchange keys through unprotected communication channels. Its safety is based on the difficulty of calculating discrete logarithms in a limited area.

Diffie-Hellman's open distribution scheme of switches

Figure 22.3. Diffie-Hellman's open distribution scheme of switches

The Diffie-Hellman scheme also provides a comprehensive way to protect the confidentiality and authenticity of the transmitted data.

In the Diffie-Hellman scheme, users involved in the exchange of information A and B independently generate their own secret keys kA and kB (keys kA and kB users A and V are confidential chi random large integers).

• User A then calculates the public key based on its secret key kA:

• KA = gKA (mod N).

• Simultaneously, user V calculates the public key based on his secret key kB:

• KB = gKB (mod N).

Here N and g are large whole numbers. This is done by bringing the arithmetic operations to the module. The numbers n and g do not have to be kept secret, as usually these values are common to all users of the network and the system.

Then users exchange their public keys A and B via an unprotected channel and use the public session secret key Kni (split secret) to calculate: user A: K = (Kv) kl (modN) = (gkB) kl (modN), user V: K '= (Kl) kv (modN) = (gkA) kv (modN), where K = K', because (gkB) kl = (gkA) kv (modN).

RESULTS

The method of open distribution of keys, invented by U. Diffie and M. Hellman, allows users to exchange keys through unprotected communication channels. Its safety is based on the difficulty of calculating discrete logarithms in a limited area.

Diffie-Hellman's open distribution scheme of switches

Figure 22.3. Diffie-Hellman's open distribution scheme of switches

The Diffie-Hellman scheme also provides a comprehensive way to protect the confidentiality and authenticity of the transmitted data.

In the Diffie-Hellman scheme, users involved in the exchange of information A and B independently generate their own secret keys kA and kB (keys kA and kB users A and V are confidential chi random large integers).

• User A then calculates the public key based on its secret key kA:

• KA = gKA (mod N).

• Simultaneously, user V calculates the public key based on his secret key kB:

• KB = gKB (mod N).

Here N and g are large whole numbers. This is done by bringing the arithmetic operations to the module. The numbers n and g do not have to be kept secret, as usually these values are common to all users of the network and the system.

DISCUSSION

Figure 21.1. Digital signature formation procedure.

During the preparation of this procedure, the sending subscriber A generates two keys: the secret key kA. and public key CA. The public key KA is obtained by calculating the secret key kA, which is its pair. The public key KA is distributed to other subscribers of the network for use in signature verification.

Electronic digital signature verification scheme

Figure 21.2. Digital signature verification procedure.

Network subscribers can check the digital signature of the received message "M" with the help of the sender's public key.

Each signature contains the following information:

- date of signing;

- expiration date of this signature key;

- information about the person signing the file (F.I.Sh, position, place of work);

- Signature identifier (public key name);

- The digital signature itself.

Created in the United States in 1977, the RSA system is the first and world-famous electronic digital signature system and implements the above principles. Developed in 1984 by El Gamal, the digital signature algorithm is characterized by high reliability and ease of implementation on personal computers.

Cryptographic key management

The following requirements apply to the distribution of keys:

- efficiency and accuracy of distribution;

- Confidentiality and integrity of distributed keys.

The following basic methods of distributing keys among users of computer networks are used.

1. Use one or more key distribution centers.

2. Direct exchange of keys between network users.

The problem with the first method is that the key distribution center knows to whom and which keys have been distributed. This allows you to read all the messages being transmitted over the network. Potential abuses can lead to serious network security breaches. The problem with the second method is to make sure that the network subjects are genuine.

CONCLUSION

During the preparation of this procedure, the sending subscriber A generates two keys: the secret key kA. and public key CA. The public key KA is obtained by calculating the secret key kA, which is its pair. The public key KA is distributed to other subscribers of the network for use in signature verification.

Then users exchange their public keys A and B via an unprotected channel and use the public session secret key Kni (split secret) to calculate: user A: K = (Kv) kl (modN) = (gkB) kl (modN), user V: K '= (Kl) kv (modN) = (gkA) kv (modN), where K = K', because (gkB) kl = (gkA) kv (modN).

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

4 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

5 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

6 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

7 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

8 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

9 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

10 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

11 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

12 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

13 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

14 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.