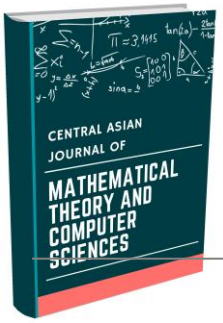

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 3 | Mar 2023 ISSN: 2660-5309

THE NEED TO IMPLEMENT CRYPTOGRAPHIC INFORMATION PROTECTION TOOLS IN THE OPERATING SYSTEM AND EXISTING SOLUTIONS

Nurullaev Mirkhon Muhammadovich

Department of Information communication technology, Bukhara Engineering Technological Institute, Uzbekistan

nurullayevmirxon@gmail.com

Abstract

The article discusses the importance of implementing cryptographic information protection tools in operating systems and existing solutions. With the increasing amount of sensitive information being stored and transmitted online, it is crucial to protect it from cyber attacks and data breaches. Cryptography helps to ensure the confidentiality, integrity, and authenticity of information by using mathematical algorithms to encrypt it. The article explores some of the existing cryptographic information protection solutions, such as SSL/TLS, disk encryption, VPNs, PGP, and SSH, and explains how to implement them effectively by assessing the security needs of the system, selecting the appropriate tools, integrating them into the system architecture, and regularly updating and maintaining them. By implementing these tools correctly, we can protect our sensitive information from cyber attacks and data breaches.

ARTICLEINFO

Article history:
Received 12 Jan 2023
Revised form 13 Feb 2023
Accepted 14 Mar 2023

Keywords: *protection tools, cryptographic algorithms, encryption, cryptographic tools.*

Introduction

In today's digital age, information security has become a top priority for individuals, organizations, and governments. With the increasing amount of sensitive information being stored and transmitted online, it has become imperative to implement effective cryptographic information protection tools in operating systems and existing solutions. Cryptography is the science of secret communication, and it involves the use of mathematical algorithms to ensure the confidentiality, integrity, and authenticity of information. In this article, we will explore the need to implement cryptographic information protection tools in the operating system and existing solutions, as well as some of the solutions that are currently available.

The Need for Cryptographic Information Protection Tools

In today's world, almost every aspect of our lives is connected to the internet. We use it for communication, online banking, shopping, and even healthcare. However, this convenience comes with the risk of cyber attacks and data breaches, which can result in the loss or theft of sensitive information. The consequences of these attacks can be severe, including financial losses, damage to reputation, and legal liability.

Therefore, the need to implement cryptographic information protection tools in the operating system and existing solutions is crucial. These tools help protect information by encrypting it, making it unreadable to unauthorized individuals. Cryptography also helps to ensure the integrity of the information, which means that it cannot be modified without detection. Additionally, cryptography provides authentication, which means that the recipient can be sure that the information has not been tampered with and comes from the expected source.

Existing Cryptographic Information Protection Solutions

There are several existing cryptographic information protection solutions available that can be used to protect information in operating systems and other solutions. Some of these solutions include:

1. SSL/TLS - SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that are used to secure internet communication. They ensure that the data transmitted between a client and server is encrypted, making it unreadable to anyone who intercepts it.
2. Disk Encryption - Disk encryption is the process of encrypting the data stored on a hard drive or other storage device. This helps to ensure that if the device is lost or stolen, the data cannot be accessed by unauthorized individuals.
3. VPN - A Virtual Private Network (VPN) is a secure connection between two devices over the internet. VPNs encrypt the data transmitted between the devices, making it unreadable to anyone who intercepts it.
4. PGP - Pretty Good Privacy (PGP) is a software program that is used to encrypt and decrypt email messages. It provides end-to-end encryption, meaning that only the sender and recipient can read the message.
5. SSH - Secure Shell (SSH) is a protocol that is used to secure remote access to a computer. It provides encrypted communication between the client and server, making it difficult for anyone to intercept the data transmitted.

Implementing Cryptographic Information Protection Tools

To implement cryptographic information protection tools, it is important to first assess the security needs of the system and the data being transmitted. This will help determine which cryptographic protocols and tools are best suited for the system.

The use of national tools by state organizations in ensuring the security of interactive services provided to the public, as well as in ensuring the cryptographic protection of information during the exchange of inter-organizational electronic documents is an important security principle [1].

Currently, in the Republic of Uzbekistan, residents are provided with keys for using an electronic digital signature both online and offline. Digital signature keys are mostly stored in flash memory. In this case, it is very difficult to store the key file securely. With a virus or physical damage to the flash memory, the use of keys becomes impossible if there is no backup.

The use of tokens and smart cards when storing keys can provide reliable security. But it is considered impractical to establish the distribution of keys among the population by this method. Given that most citizens have smartphones, it is possible to use the tools created within the framework of this study to ensure the safety of keys on smartphones. Since the key generation is also carried out on the smartphone of the key owner, the probability of using the key by unauthorized persons is reduced [2].

In software developed for the Windows operating system abroad, cryptographic operations are mainly performed using a cryptographic provider. CSP is a cryptographic module that provides a service for performing cryptographic actions with the operating system and application programs and runs on the Windows operating system. Starting with the Windows Vista version, CSP CNG began to be used in Microsoft operating systems. Unlike the previous generation, CSP CNG supports new algorithms, in particular algorithms based on elliptic curves [3].

Table 1 lists the New Generation CSPs developed by Microsoft and supporting their algorithms, as well as the encryption speed. [4].

Table 1 – CSP New Generation developed by Microsoft

	Microsoft Software Key Storage Provider	**Microsoft Smart Card Key Storage Provider**	**Microsoft Primitive Provider**	**Microsoft SSL Protocol Provider**
Symmetric-key algorithms			AES, DES, DESX, 3DES, RC2, RC4	AES, DES, 3DES, RC4
Asymmetric encryption algorithms	RSA	RSA	DSA, RSA	
Hash functions			MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512	MD5, SHA-1, SHA-256, SHA-384
Key Exchange	Diffie-Hellman, ECDH	Diffie-Hellman, ECDH	Diffie-Hellman, ECDH	Diffie-Hellman, ECDH
EDS	DSA, ECDSA, RSA	RSA, ECDSA	DSA, ECDSA, RSA	DSS, RSA, ECDSA
Encryption speed (mb/s)			382,3	383,3
Hashing speed (mb/s)			333,6	334,6
Opportunities (according to the 10-point system)	**10**	**9**	**9**	**8**

Once the appropriate tools have been selected, they should be integrated into the system architecture and configured to ensure that they are used correctly [5].

It is also important to ensure that the cryptographic tools are regularly updated and maintained to address any vulnerabilities that may arise. Additionally, it is essential to educate users on how to use the cryptographic tools correctly and the importance of protecting sensitive information [6].

The speed of encryption and hashing of data, CSP created by Microsoft is analyzed, the possibilities are evaluated. It was found that CSPs developed by Microsoft provide high speed of performing cryptographic operations using SHA1 and RC4 algorithms.

Conclusion

In conclusion, the need to implement cryptographic information protection tools in operating systems and existing solutions is crucial in today's digital age. Cryptography helps to ensure the confidentiality, integrity,

and authenticity of information, protecting it from unauthorized access and modification. There are several existing cryptographic information protection solutions available, including SSL/TLS, disk encryption, VPNs, PGP, and SSH. To implement these tools effectively, it is essential to assess the security needs of the system, select the appropriate tools, integrate them into the system architecture, and regularly update and maintain them [7].

As technology continues to evolve, so do the threats to information security. It is therefore crucial to remain vigilant and up-to-date with the latest cryptographic information protection tools and technologies. By doing so, we can ensure that our sensitive information remains secure and protected from cyber attacks and data breaches.

In conclusion, the implementation of cryptographic information protection tools in operating systems and existing solutions is essential to ensure the confidentiality, integrity, and authenticity of information. With the use of these tools, we can protect our sensitive information from unauthorized access and modification, ensuring its security in an increasingly connected world.

References

1. R.D. Aloev, M.M. Nurullaev, “Software, algorithms and methods of data encryption based on national standards”, IIUM Engineering Journal 21 (1), pp. 142–166, 2020. doi: 10.31436/iiumej.v21i1.1179.
2. Mukhammadovich N. M., Djuraevich A. R. “Working with cryptographic key information”, International Journal of Electrical and Computer Engineering. – 2023. – Т. 13. – №. 1. – С. 911. doi: 10.11591/ijece.v13i1.pp911-919
3. Alaev R.H. Cryptographic key management in the Windows operating system. // International scientific conference “Information Technologies, Networks and Telecommunications” ITN&T-2021. Urgench 2021, may 25-26. – pp. 272-275.
4. https://docs.microsoft.com/en-us/windows/win32/seccng/cryptographic-primitives
5. R.D. Aloev, M.M. Nurullaev, ”Development of the Software Cryptographic Service Provider on the Basis of National Standards”, Journal of Systemics, Cybernetics and Informatics, 17 (1), pp. 260–272, 2019.
6. M.M. Nurullaev, “Modeling of information processes in integrated security systems”, Journal Molodoy uchoniy, 17(203), pp. 26-27, 2018.
7. R.D. Aloev, M.M. Nurullaev, “Cryptography Service Provider – Data Encryption”, in Proc. Conference on Complexity, Informatics and Cybernetics, Orlando, Florida, USA, pp.127–131, 2019.