

Subscribe to DeepL Pro to edit this document.  
Visit [www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document) for more information.

Odesa College of Computer Technology "Server"

Practical work report No. 4

From the subject "Information security technologies"

Topic : "Description of modern regulatory encryption systems and their application in Ukraine"

Performed by:

Student of group K21.1

Mashkov Vladimir

Odesa 2024

INTRODUCTION

Modern regulatory encryption systems play a key role in ensuring data security in Ukraine, especially in the context of growing cyber threats and the need to protect state and commercial information. The complexity of data protection tasks requires the diverse and combined use of cryptographic algorithms, taking into account the specifics of information threats. Data encryption has become the foundation of information security, and it is important to understand what systems are used, how they work, and what their strengths and weaknesses are.

MODERN DATA ENCRYPTION SYSTEMS AND THEIR APPLICATION

To demonstrate and provide examples, we have chosen Ukraine, which uses different types of encryption, namely :

* channel encryption,
* end-to-end encryption,
* combined encryption,
* file encryption.

Each of these systems solves its own problems by providing different levels of data protection depending on the specific security requirements.

In the following, we will briefly consider what encryption systems exist and are used:

1. Channel encryption

This type of encryption is used to protect data transmitted over communication channels. Encryption is applied at the stage of data transmission between the sender and the recipient, which prevents unauthorized access to information during transmission. Examples include telecommunications security systems such as IPsec (Internet Protocol Security) and SSL/TLS (Secure Sockets Layer/Transport Layer Security).

1. End-to-end encryption

End-to-end encryption ensures the confidentiality of data all the way from the sender to the recipient. This means that the data is encrypted on the sender's device and decrypted only on the recipient's device, making it impossible for third parties, including communication service providers, to access it. An example of such systems is the widely used messenger system in Ukraine and the world, such as WhatsApp and Signal, where end-to-end encryption is implemented to protect personal correspondence.

1. Combined encryption

This method combines different types of encryption, including symmetric and asymmetric algorithms, to provide a higher degree of data protection. For example, digital signature systems use asymmetric algorithms to sign messages and symmetric algorithms to speed up the encryption process. An example is the use of a hybrid encryption scheme in data transfer protocols such as PGP (Pretty Good Privacy).

1. File encryption

File encryption is used to protect data stored in storages or transmitted over networks. This method of encryption makes information inaccessible to third parties even in the case of physical access to the data carrier. Examples of file encryption systems include VeraCrypt and BitLocker, which are popular in Ukraine.

To ensure the operation of the above cryptographic systems, various encryption algorithms are used, each of which has certain characteristics and is used to solve specific problems. Next, we will consider the AES (Advanced Encryption Standard) encryption scheme:

Advanced Encryption Standard is one of the most widely used algorithms in Ukraine. It is a symmetric block encryption algorithm used to encrypt files and data in various security systems. It was adopted as an encryption standard by the US government in 2001 and is used to protect sensitive information, including military and government data.

The scheme of AES :

1. Key generation: Generates a unique symmetric key that will be used to encrypt and decrypt data. The key can be 128, 192, or 256 bits long.
2. Splitting data into blocks: Data is divided into fixed-length blocks (128 bits).
3. Block encryption: Each block of data goes through several transformation cycles, including substitutions, permutations, and linear transformations. The number of such cycles depends on the key length (for example, 10 cycles for a 128-bit key).
4. Result: After all the cycles are completed, encrypted data blocks are obtained, which are then combined into a final encrypted file or message.

This encryption method has the following disadvantages:

* High speed, making it suitable for encrypting large amounts of data.
* High level of security that makes it resistant to most known attacks, including brute force attacks.
* Flexibility of use due to the ability to choose the key length.

However, despite its wide popularity and recognition as a secure algorithm, AES is not without certain drawbacks, especially in the context of specific threats and data protection requirements, namely:

* Vulnerability to side-channel attacks: AES, as a symmetric encryption algorithm, is vulnerable to side-channel attacks that exploit physical characteristics of the device to obtain data such as electromagnetic emissions, power consumption, or the timing of operations. For example, if an AES-encrypted device is not protected, an attacker can analyze the electromagnetic radiation and use this data to recover the encryption key.
* The threat of hacking when using weak or repetitive keys: While the AES algorithm is secure in itself, its security is directly dependent on the length and quality of the key. Using weak, short, or repetitive keys can significantly reduce the level of protection and leave the system vulnerable to brute force attacks. In the case of 128-bit keys, there is a possibility that in the future, with the advent of quantum computers, such keys can be cracked relatively quickly.
* Ineffective for protecting small amounts of data: AES was designed to encrypt large amounts of data, making it inefficient for protecting small files or short messages. In such cases, it can be resource-intensive and slow down system performance.
* Inability to protect against some types of attacks: AES is not protected against attacks using quantum computing. Quantum computers may in the future implement attacks such as the Grover method, which could potentially cut the time to crack symmetric keys in half, making 128-bit keys vulnerable.
* Lack of built-in support for key management: AES does not provide built-in key management mechanisms, which can be a problem when implementing a cryptosystem in practice. Without proper key management, such as key rotation or key confidentiality, even a secure algorithm becomes vulnerable.

RELEVANCE AND POPULARIZATION OF CRYPTOGRAPHIC SYSTEMS

The relevance of cryptographic systems in Ukraine is driven by the need to protect data in the face of growing cyber threats and political instability. Government agencies, financial organizations and the business sector are increasingly using modern technologies to protect information. Among all these types of encryption, end-to-end encryption and file encryption are the most widespread. This is due to the massive shift to remote work, the use of cloud technologies, and the growing number of cyberattacks aimed at identity theft and industrial espionage.

The use of hybrid encryption systems that combine symmetric and asymmetric algorithms has also become more popular, as such systems strike a balance between security and data processing speed.

CONCLUSION

Modern cryptographic systems in Ukraine play a key role in ensuring the security of both public and private information. Methods such as end-to-end encryption and file encryption are widely used, due to the need to protect data at different levels. The AES algorithm is one of the most popular solutions due to its reliability and high performance. Given the complexity and diversity of threats, the combined use of encryption algorithms remains the most effective data protection strategy in today's information security environment.