



Symmetric encryption algorithms and methods for their evaluation

Razzakov Sherbek Tog'aymurod ugli

Normurodov Chori Begaliyevich.

Termez State University

Abstract

This thesis analyzes the mechanisms of operation of modern symmetric encryption algorithms, their main types, and performance indicators. An analysis was also conducted based on the criteria used in the evaluation of encryption algorithms - speed, security, resource consumption, stability, and key length. The advantages and weaknesses of symmetric encryption algorithms in ensuring data security are highlighted.

Keywords Encryption, symmetric algorithm, AES, DES, data security, cryptanalysis, evaluation criteria

Introduction

In ensuring information security, reliable data encryption is extremely important. Encryption algorithms are divided into two types: "symmetric" and "asymmetric." In symmetric encryption, both encryption and decryption are performed using a single key. This method is distinguished by its speed and simplicity.

Basic symmetric algorithms

The following well-known symmetric encryption algorithms were analyzed:

- DES (Data Encryption Standard): 64-bit block algorithm with a 56-bit key. Today, the level of security is considered low.
- AES (Advanced Encryption Standard): 128/192/256-bit key, high level in terms of security and speed.
- Blowfish is fast, has a flexible wrench length, but is used less frequently than nuclear power plants.
- RC5/RC6: Simple and parametric algorithms, in some cases fast at the hardware level.

Evaluation criteria

The following criteria are used to evaluate symmetric algorithms:



1. Speed (Performance): Data encryption and decryption speed (ms/MB).
2. Security level: Resistance to cryptanalysis, key length, block size.
3. Resource requirements: RAM and processor load.
4. Simplicity: Software and hardware flexibility.
5. Stability: Sensitivity to small changes (Avalanche effect).

1. Selected algorithms

Within the framework of the study, the following symmetric encryption algorithms were selected, which are widely used and considered safe:

- Advanced Encryption Standard (AES)
- DES (Data Encryption Standard)

3DES (Triple DES)

- Blowfish
- RC4
- ChaCha20

2. Encryption and decryption processes

The following steps were carried out for each algorithm:

- Text files (various sizes - 1 KB, 100 KB, 1 MB) were prepared.

Each file is encrypted using selected algorithms.

- The encrypted data is decrypted again (restored to its original state).
- Encryption and decryption speeds measured.

3. Evaluation criteria

To compare the algorithms, an assessment was carried out based on the following criteria:

Rating Criteria Description

Speed Encryption and decryption time (ms, measured in seconds)

Storage usage Amount of RAM used during encryption/decryption

Security level Key length, resistance to analyses (differential and statistical analyses)

Block length The length of each block (in bits) when the algorithm works with blocks

Adaptability The suitability of the algorithm for operation on various platforms and the possibility of optimization

4. Environment of practical experience

The experiments were conducted under the following technical conditions:

- Processor: Intel Core i7, 3.2 GHz
- RAM: 16 GB RAM
- Operating system: Ubuntu 22.04 LTS / Windows 11
- Programming language: Python 3.11 (PyCryptodome, Cryptography libraries were used)

5. Statistical analysis

Based on the obtained results, statistical analysis was carried out. For each algorithm, the average operating time and the probability of error were calculated. The results were visually represented using graphs and tables.

For a perfectly secure encryption algorithm, the computational complexity is the same as the key field, which is sometimes also called the entropy of the key. The key field refers to the set of all possible keys and represents the total number of these keys. In other words, the key field represents the total number of combinations that can be created using all secret key bits.

Results

As a result of the analysis, the following conclusions were made:

Nuclear power plants are considered the safest and most widely used symmetric algorithm.

DES is currently outdated and cannot meet modern requirements.

Blowfish is convenient for small systems, but not universal.

According to the assessment results, the NPP algorithm is the most optimal choice in the speed-safety ratio.

Conclusion

Symmetric encryption algorithms allow for fast and efficient information protection. When selecting them, it is necessary to take into account the capabilities of the system and the needs of the security level.

In modern information systems, it is recommended to use the AES algorithm as the main tool.

References

1. Stallings, W. *Cryptography and Network Security*, Pearson, 2020.
2. Schneier, B. *Applied Cryptography*, Wiley, 2015.
3. NIST. *Federal Information Processing Standards (FIPS) 197: AES*, 2001.
4. Behrouz Forouzan. *Cryptography and Network Security*, McGraw-Hill, 2017.
5. Scientific articles and standards on cryptography in Uzbekistan.