УДК 621.391:004.75

CLASSIC AND MODERN ENCRYPTION ALGORITHMS FOR BIG DATA PROCESSING

Y. Liashchevich
Postgraduate of the BSUIR

Cai Yuxin
Graduate of Luoyang Normal University

Y. Liashchevich

Graduated from BSUIR. Postgraduate in the Department of Electronic Engineering and Technology. His research interests include the effects of infrasound on biological tissue, infocommunication signals and systems.

Cai Yuxin

Graduate of Luoyang Normal University. The area of scientific interest is research into encryption and decryption technologies for communication signals based on new algorithms.

Abstract. The article discusses the using methods of research into encryption and decryption technologies for communication signals based on new algorithms in big data systems

Keywords: encryption, decryption, channel coding, burst interference.

Introduction. The modern world is living in an era of rapid development in wireless technologies and big data processing. Wireless systems such as 5G and 6G IoT, satellite communications transmit massive amounts of sensitive data, must ensure data transmission security [1]. As data transfer speeds increase, so does the volume of data. Routing and data storage devices must ensure maximum data protection from unauthorized access. Modern data encryption algorithms, are used for this purpose. Research Questions it is how effective are new encryption algorithms for communication signals? And can these algorithms resist emerging threats? What trade-offs exist between speed, security, and resource usage?

Basic encryption algorithms. Encryption is a technique for securing the information so only the authorized parties can interpret the data. What happens is that encryption provides transformations on the plaintext and transforms it into ciphertext which isn't human-readable. Not only in the digital era but ciphers have also been widely used throughout history. In the figure below, we present the general view of the classification of the ciphers. As we've seen, we categorize ciphers in terms of some characteristics that they have or according to their usage. They are mainly divided into two different types; classical and modern classes. The most common and used in digital are is modern class. It's because of its dynamic and static cryptographic techniques that pave the way for more detailed classes, symmetric and asymmetric ciphers (Fig. 1):

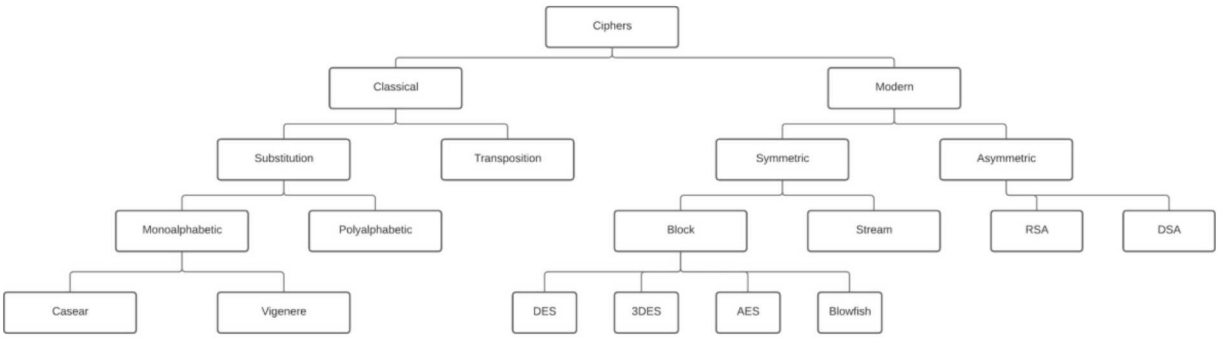

Figure 1. Classification of encryption algorithms

Symmetric encryption uses only one key to encrypt and decrypt data, while asymmetric encryption uses two different keys [2]. A public key is used for encryption, and a private key is used for decryption. Despite the differences between the public and private keys, they are related and are therefore called a key pair. DES, 3DES, AES, and Blowfish belong to the class of symmetric block ciphers.

Encryption Algorithms. DES is developed by IBM and based on a design by Horst Feistel. It was one of the widely used and publicly available cryptographic systems when it was first released. Even though its first debut is in the 70s, it was later adopted by the National Institute of Standards and Technology (NIST). It's a symmetric-key algorithm for the encryption of digital data. It has a block size of 64 bits and uses the Feistel network as a structure. It's slow and not used in the software.

Triple DES, 3DES, or TDES is officially the Triple Data Encryption Algorithm. It's a symmetric-key block cipher and it applies the DES algorithm three times to each block. It has a block size of 64 bits and a key length of 112 or 168 bits. It also uses the Feistel network since it's based on DES [2,3].

Due to the modern cryptology techniques and supercomputing, like the DES, 3DES has also some serious vulnerabilities. That's why the NIST has deprecated DES and 3DES for new applications in 2017 and for all applications by 2023. Blowfish is another symmetric-key encryption technique designed by Bruce Schneier in 1993 as an alternative to the DES encryption algorithm. Therefore, it is significantly faster than DES and provides a good encryption rate. Its key length is 446 bits, and way better than DES, and 3DES. Therefore, it's more difficult to crack the key of Blowfish. It also has a block size of 64 bits. It can be used in software as well. However, AES receives more attention today, and Schneier recommends Towfish as an alternative to Blowfish. It has a free license and is available for all uses. AES is another type of cipher that protects the data from malicious parties. It's currently one of the strongest encryption algorithms available. Since AES combines speed and security properly, it allows us to carry on with our online activities without any interruption. As AES uses the same key to both encrypt and decrypt data, it is also a symmetric type of encryption. There are three types of lengths of AES encryption keys 128, 192, and 256 bits. Each key length has different possible key combinations. It has a different structure than other encryption algorithms, it uses the substitution-permutation network.

Emerging Encryption Algorithms. Recent developments and emerging trends of cyber security

There are many recent developments in cyber security with the help of new algorithms, procedures and frameworks. Quantum Key Distribution (QKD) is a groundbreaking method in quantum cryptography that enables secure communication through the exchange of cryptographic keys [4]. Its security is rooted in the principles of quantum mechanics, particularly the no-cloning theorem and quantum entanglement, which make it virtually impossible for an eavesdropper to intercept or duplicate the key without being detected. Basic Principle:

QKD allows two parties (usually referred to as A and B) to securely exchange a cryptographic key over a potentially insecure channel. The security of QKD comes from quantum properties such as quantum superposition and entanglement.

- **Quantum Mechanics Behind QKD:**
- **No-Cloning Theorem**: It states that an arbitrary quantum state cannot be copied exactly, meaning any attempt to intercept a quantum key would disturb the state and be detectable.
- **Heisenberg Uncertainty Principle**: Measuring a quantum state disturbs it, so any eavesdropping attempts can be easily detected by the parties involved.

Types of QKD Protocols

There are several types of QKD protocols, but the most well-known ones include:

- **BB84 Protocol (1984)**:
- The first and most widely used QKD protocol, developed by Charles Bennett and Gilles Brassard.
- It uses **polarization** states of photons (or other quantum particles) to encode information. Alice sends photons in one of four states, and Bob measures them using randomly chosen bases.
- If no eavesdropping occurs, Alice and Bob will share a secure key.
- **E91 Protocol (1991)**:
- Based on **quantum entanglement**, where two particles (photons) are entangled in such a way that the measurement of one instantly affects the state of the other, even if they are far apart.
- This protocol uses **Bell's theorem** to ensure the authenticity and security of the key exchange.
- **Decoy State Protocols:**
- A modification to the basic QKD protocols, designed to mitigate the impact of photon number splitting (PNS) attacks, which can occur when an eavesdropper tries to intercept the photons in a weak coherent pulse.
- **Measurement-Device-Independent QKD (MDI-QKD):**
- Addresses the vulnerability of QKD systems to imperfections in detectors by enabling secure communication even when measurement devices are compromised.

Security of QKD

- **Quantum Security:**
- The key feature of QKD is its **unconditional security**. In theory, QKD can offer perfect security against any computational or classical cryptographic attack.
- Any eavesdropping or interference with the quantum channel results in observable errors that alert the communicating parties. This is because the quantum state will be disturbed, revealing the presence of an intruder.
- **Practical Security Concerns:**
- **Side-Channel Attacks**: Despite the inherent security of QKD, practical implementations can still be vulnerable to side-channel attacks, which exploit weaknesses in the physical hardware, such as detectors or transmission equipment.
- **Device Calibration & Trust**: The security of QKD systems relies heavily on trusted devices. If any device is compromised, the whole system's security can be compromised.

Post-Quantum Cryptography (PQC) involves developing cryptographic algorithms run on conventional computers that are secure against attacks from future, powerful quantum computers. These algorithms, such as lattice-based cryptography, replace current standards like RSA and ECC, which are vulnerable to Shor's algorithm [3,4]. PQC ensures long-term data security, preventing "harvest now, decrypt later" threats.

Categories of PQC Algorithms

PQC algorithms fall into several categories based on the type of problem they aim to solve and the type of cryptographic function they support.

- **Public-Key Cryptography** (asymmetric encryption):
- These are algorithms that rely on the difficulty of certain problems (e.g., integer factorization, discrete logarithms) which quantum computers can break but classical computers cannot efficiently solve.
- **Symmetric Cryptography**:
- These are used to encrypt and authenticate data using shared secrets. Quantum computers pose a smaller threat here (as Grover's algorithm only offers quadratic speedup, not an exponential one), but adjustments (like doubling key sizes) can maintain security.
- **Hash-Based Cryptography**:
- These use hash functions as the foundation for creating signatures and other forms of public-key cryptography. They are quantum-safe because quantum computers don't offer significant speedup over classical brute-force attacks on hash functions.

Candidate Algorithms for PQC (NIST Standardization)

The **NIST Post-Quantum Cryptography Standardization Process** aims to evaluate and standardize quantum-resistant algorithms. As of 2026, the final selections are still ongoing, but several promising candidates have emerged:

Public-Key Algorithms

- **Lattice-Based Cryptography**:
- Based on the hardness of lattice problems, which are believed to be resistant to quantum algorithms.
- Examples:
- **Kyber** (Encryption and Key Establishment)
- **NTRU** (Encryption and Key Exchange)
- **FrodoKEM** (Key Encapsulation)
- **NTS-KEM** (Key Encapsulation)
- **Code-Based Cryptography**:
- Based on error-correcting codes, specifically the difficulty of decoding random linear codes.
- Example: **McEliece** (Encryption)
- Known for large key sizes, but extremely resistant to quantum attacks.

- **Multivariate Polynomial Cryptography**:
- Relies on the difficulty of solving systems of multivariate polynomial equations over finite fields.
- Example: **Rainbow** (Digital Signatures)
- **Hash-Based Cryptography**:
- Based on the security of hash functions. While these are quantum-resistant, they generally have large signature sizes.
- Example: **XMSS** (Extended Merkle Signature Scheme)
- Used for signing messages with a smaller state, suitable for high-speed environments.
- **Isogeny-Based Cryptography**:
- Uses the mathematical structure of elliptic curves and their isogenies (maps between elliptic curves).
- Example: **SIKE** (Supersingular Isogeny Key Exchange)
- Considered a potential lightweight and efficient choice for key exchange.

Symmetric-Key Cryptography

- **AES (Advanced Encryption Standard)**:
- AES is already considered secure, but in a post-quantum world, it would require key lengths to be doubled (e.g., AES-256 instead of AES-128) to maintain security.
- **SHA-3 (Secure Hash Algorithm 3)**:
- SHA-3 is designed to be resistant to quantum attacks, as quantum computers do not provide significant speedup for hash functions.

Current State of PQC. NIST Standardization Process: The NIST post-quantum cryptography initiative is working towards finalizing the quantum-resistant standards. As of 2026, the finalists for encryption and key exchange are Kyber and NTRU, and FrodoKEM is a possible alternative for scenarios requiring more conservative security. For digital signatures, FALCON (lattice-based) and Rainbow (multivariate) are among the leading candidates.

Industry Adoption. While no large-scale commercial implementations of PQC are widespread yet, various companies and organizations are testing PQC algorithms in pilot projects. Some entities are using hybrid systems combining classical and quantum-safe algorithms to ensure security today and in the future.

Future of PQC.

- **Hybrid Cryptographic Systems**:
- During the transition period (while quantum computers are still under development), hybrid systems using both classical and post-quantum algorithms will likely be implemented for additional security.
- **Quantum Networks & Quantum Key Distribution (QKD)**:
- As quantum communication networks develop, PQC algorithms will be integrated into these systems, potentially along with QKD, to provide an extra layer of security.
- **AI and Machine Learning in Cryptography**:
- Machine learning and AI might help optimize PQC systems or analyze vulnerabilities in new PQC algorithms, driving further innovation.

Conclusion. In this article, we've briefly given some information about DES, 3DES, Blowfish, and AES, QKD, PQC. Also, we compared and evaluated them in terms of some metrics. Although we think that encryption algorithms protect the data both in theory and practice, keep in mind that there are various attacks such as malware, key search, brute force, phishing, side-channel, and more. These attacks aim to find a way to hack the system. To sum up, while every encryption algorithm has weaknesses and advantages, some of them can lose their reliability over time. So, we should be careful when we select cryptographic algorithms. We should both consider our application and the specifics of the encryption algorithm.

References

[1] Andrea Goldsmith - Wireless Communications. -Cambridge University Press. – 2005 pp. 204-207

[2] Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[3] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[4] Abdulbast A. Abushgra Variations of QKD Protocols Based on Conventional System Measurements. - 2024

Author's contribution

The authors contributed equally to the writing of the article.

КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Е.И. Лещевич
Выпускник БГУИР, преподаватель в Лоянский Педагогический Университет

Цай Юйсинь
Выпускник в Лоянский Педагогический Университет

Аннотация. В статье рассматриваются методы исследования технологий шифрования и дешифрования коммуникационных сигналов на основе новых алгоритмов в системах обработки больших данных.

Ключевые слова: шифрование, дешифрование, канальное кодирование, пакетные помехи.