ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

6. Detecting XSS (Cross-Site Scripting) Attacks in SOC Environment // internet-resource “LetsDefend” – 26 august 2024 y. – URL: https://letsdefend.io/blog/detecting-xss-cross-site-scripting-attacks-in-soc-environment

7. 5 способов получить RCE на практике // internet-resource “Habr” – 8 january 2025 y. – URL: https://habr.com/ru/articles/872110/

8. Remote code execution (RCE) // internet-resource “Invicti” – URL: https://www.invicti.com/learn/remote-code-execution-rce/

FUNDAMENTALS OF MODERN CRYPTOGRAPHY: FROM ENCRYPTION TO DIGITAL SIGNATURES.

Zhakay Aikerim
aikerim.zhakai@mail.ru
Status (Master’s student) L.N. Gumilyov Eurasian National University, Astana
Supervisor – Tashenova Zh. M.

ABSTRACT

The issue of changing and protecting information so that it cannot be read by other outsiders has been thinking about humanity since ancient times. The history of cryptography is developing in parallel with the history of human language. Even the writing itself was originally a cryptographic system because, in ancient times, only a select few knew how to write. When writing became widespread, cryptography developed as a separate science. Cryptographic systems developed well during the years of the First and Second World Wars. Since the post-war time, the emergence of computing equipment up to this point accelerated the creation and improvement of cryptographic methods. In the modern world, cryptography has entered into everything, from mobile phones to e-mail programs, bank cards, smart homes and even into medical implants. This is quite different from the past, where cryptography had been traditionally confined to very specific applications, especially government communications and banking systems. As a consequence of the pervasiveness of crypto algorithms, people should understand how they work and how they can be applied in practice. This article addresses this issue by providing a comprehensive introduction to modern applied cryptography and provides the reader with a deep understanding of how modern cryptographic schemes work.

1.INTRODUCTION

The swift advancement of internet technology has rendered information security, driven by network communication encryption and cryptography, an essential aspect of contemporary society. Cryptography, the science of securing information, has evolved from ancient techniques of secret communication to highly advanced systems underpinning modern digital security. With the advent of the internet, cryptographic methods play a crucial role in safeguarding sensitive data, enabling private communication, and building trust in digital interactions. At its core, cryptography involves transforming data into a secure format that can only be read or decrypted by those who have the appropriate key or knowledge. From encrypting emails and safeguarding financial transactions to securing national defense systems, cryptography ensures its basic principles such as the confidentiality, integrity, authenticity of information and non-repudiation. This article explores the core principles of modern cryptography, including encryption, symmetric and asymmetric cryptography, and digital signatures.

1.2 LITERATURE REVIEW

Cryptography is a basis fundamental of modern information security. It is used to protect data from unauthorized access, especially in the digital age, where the number of cyber-attacks continuously increasing. The purpose of this review is to examine existing approaches and technologies in the field of cryptography, as well as their effectiveness. Cryptography has deep historical roots, from ancient ciphers such as the Caesar cipher to modern algorithms. A historical overview, such as that by Klaus Schneider (2020), charts the evolution of cryptographic methods from hand ciphers to state encryption systems. Modern technologies such as AES (Advanced Encryption Standard) are the basis for protecting confidential information. Research such as the work of Richard Lee (2023) shows that symmetric and asymmetric algorithms have different areas of application depending on the security goals. With the development of quantum computing, threats to traditional cryptographic methods are emerging. For example, Shor (1997) proposed an algorithm that can break RSA. To counter this, quantum-resistant cryptography is being developed, as described in Green (2024). Cryptography is a key tool for data protection that is constantly adapting to new challenges. Although current methods already provide a high level of security, the development of quantum computing requires further research and development of new technologies, such as post-quantum cryptography.

2.BASIC CONSEPTS OF CRYPTOGRAPHIC INFORMATION PROTECTION.

Cryptology as a field of science engaged with information protection issues. Cryptology is developing in two directions – cryptography and cryptanalysis. The aim of cryptography is a search for mathematical methods that bring a given open text into a form that cannot be read by another outsider it is considered. The aim of cryptanalysis is considered to be an assessment of the cryptographic reliability of a cryptosystem. Cryptography is the methodological basis of modern information security systems in computer systems and networks. Cryptography is a collection of data transformation techniques designed to safeguard data by rendering it unusable for unauthorized users. To provide data security, three main functions must be supported:

- protecting the confidentiality of data transmitted or stored in memory;
- confirmation of data integrity and authenticity;
- authentication of users when logging in and when establishing a connection;

Cryptographic encryption, digital signature, and authentication technologies are used to implement these functions.

Confidentiality is ensured using symmetric and asymmetric encryption algorithms and methods, as well as by mutual authentication of subscribers based on reusable and one-time passwords, digital certificates, smart cards, etc. The integrity and authenticity of transmitted data is usually achieved using various variants of electronic signature technology based on one-way functions and asymmetric encryption methods. Authentication allows connections to be established only between legitimate users and prevents access to by means of a network of undesirable persons. Users who have proven their legality (authenticity) are provided with authorized types of network services. Ensuring the confidentiality, integrity and authenticity of transmitted and stored data is primarily carried out by the correct use of cryptographic methods and information security tools. The basis of most cryptographic information security tools is data encryption.

A cipher is a collection of procedures and rules for cryptographic operations that are used to encrypt and decrypt data with an encryption key. Information encryption refers to the process of converting open information (open text) into encrypted text (ciphertext). The process of restoring the source text from a cryptogram using an encryption key is called decryption (decryption).

Modern cryptography is developing in two directions: symmetric cryptography and asymmetric cryptography. A symmetric cryptosystem uses a single key to encrypt and decrypt information. The sender and receiver of information interact through certain closed channels in advance the key used must be replaced. An asymmetric cryptosystem uses two keys to encrypt and

decrypt information. Each user has it is own open and secret key. The sender of the message encrypts the message with a public key. To decrypt a receiving message uses a secret key known only to user.

2.2. Symmetric cryptosystems of encryption

Symmetric cryptography systems were the first to be developed in the past. In a symmetric cryptosystem, information is encrypted and decrypted using the same key. This implies that the communication can be decrypted by anyone who has the encryption key. Accordingly, all encryption keys in symmetric cryptosystems must be kept secret to avoid unauthorized exposure of encrypted data. The encryption key must be available only to the recipients of the message, which is why symmetric cryptosystems are known as secret-key cryptosystems. Symmetric cryptosystems are also known as private-key cryptosystems or single-key cryptographic systems. These cryptosystems are characterized by the fastest encryption speed and contribute to the integrity of the transmitted data as well as confidentiality and authenticity. Using a symmetric cryptosystem, the confidentiality of information transmission is dependent on the encryption key's confidentiality and the cipher's dependability. The encryption key is typically a file or array of data that is kept on a personal key carrier, like a smart card or floppy disk; precautions must be taken to make sure that only the owner may access the personal key carrier. Because it is nearly hard to do semantic change and forging of a cryptographically closed communication without first decrypting it, authenticity is guaranteed. Without the secret key, an unauthenticated message cannot be properly encrypted. A unique code created with a secret key is appended to the transmitted data to guarantee data integrity. As a sort of checksum, an image statement is a reference feature of a message that is used to verify the message's integrity. In accordance with a complex cryptographic law, the image generation algorithm must make sure that it depends on every bit of the message. The recipient of the message performs the message integrity check by creating a secret key value that corresponds to the value of the message that was received and comparing it with the value that was received. In the event that there is a match, it is assumed that the data was not altered during transmission. For example, encrypting data "for yourself" to guard against unwanted access while the owner is away is a perfect use case for symmetric encryption. Archival encryption of specific files or transparent (automated) encryption of entire physical or logical drives are the two options available. Single-key cryptosystems may do a lot of crucial information security tasks with their fast encryption speed. However, the issue of sharing encryption keys among users arises when symmetric cryptosystems are used autonomously in computer networks. All recipients must exchange secret keys prior to exchanging encrypted data. A symmetric cryptosystem requires that the secret key be sent to both the sender and the recipient through a secure channel; it cannot be transferred through public communication channels. Many regularly changing keys are needed to offer good protection of the communications circulating on the network (one key for each pair of users). Users must guarantee the integrity, secrecy, and authenticity of encryption keys when transmitting them, which comes at a significant additional expense.

2.3 Asymmetric cryptosystems of encryption

Asymmetric cryptographic systems were developed in the 1970s. The fundamental difference between an asymmetric cryptosystem and a symmetric encryption cryptosystem is that different keys are used to encrypt information and decrypt it later:

- the public key K is used to encrypt information, calculated from the secret key k';
- The secret key k' is used to decrypt information encrypted using the public key K paired with it.

These keys differ in such a way that calculations cannot deduce the secret key k' from the public key K. Therefore, the public key K can be freely transmitted over communication channels. Asymmetric systems are also called two-key cryptographic systems, or public-key cryptosystems

For cryptographic closure and subsequent decryption of the transmitted information, the recipient's public and secret keys are used in the message. The encryption key must be used the recipient's public key, and his secret key as the decryption key. The secret and public keys are generated in pairs. The secret key must remain with its owner and be securely protected from fraud. A copy of the public key must be kept by each user of the cryptographic network with whom the owner of the secret key exchange information. The process of transmitting encrypted information in an asymmetric cryptosystem is carried out as follows.

Preparatory stage:

• subscriber B generates a pair of keys: the secret key of the K and the public key of the k';

• The public key of K_B is sent to subscriber A and other user (for example, on a shared resource).

Usage — information exchange between subscribers A and B:

• User A encrypts the message using an open key user B's K key and sends the ciphertext to user B;

• User B decrypts the message using the k secret key. No one else (including user A)

can decrypt this message because they do not have user B's secret key. Information protection in an asymmetric cryptosystem is based on the secrecy of the recipient's k key.

2.4. Digital signature

Authentication of texts sent across telecommunication channels is done through an electronic digital signature. Processing and storing documents are made much less expensive with this type of communication, and document search speed is increased. However, there are issues with verifying the author's identity and the document's legitimacy, namely confirming that the received electronic document hasn't changed.

Authenticating electronic documents serves to safeguard them against potential malicious activity, such as:

• active interception, in which a hacker gains access to the network and alters documents (files);

• renegade — subscriber A pretends he didn't send messages to subscriber B, but in reality, he did;

• masquerade — subscriber C sends a document to subscriber B on subscriber A's behalf;

• repetition — subscriber C replicates a previously transmitted document that subscriber A delivered to subscriber B;

• substitution — subscriber B creates or alters a new document and claims to have received it from subscriber L.

These kinds of malevolent acts have the potential to seriously harm state-owned businesses and organizations, financial and commercial institutions, and people who utilize IT for work. The problem of verifying the integrity of the message and the authenticity of the author of the message can be effectively solved by the methodology of electronic digital signature.

2.4.1. Basic digital signature procedures.

A comparatively little amount of extra digital data sent with the signed text is known as digital signature. The foundation of digital signatures the reversibility of asymmetric ciphers and the interdependence of the key pair, the signature, and the message content. It will be impossible to confirm the legitimacy of the digital signature if at least one of these components is altered. Hash functions and asymmetric encryption methods are used in the implementation of digital signature. The digital signature system's technology is predicated on the existence of a network of members exchanging signed electronic documents. For every user key, a pair—secret and public—is created. The user forms a digital signature using the secret key, which he keeps private. All other users are

aware of the public key, which is meant to be used by the person who receives the signed electronic document to confirm the digital signature. The two primary processes in the digital signature system are digital signature generation and verification. The sender's secret key is used in the signature generation process, and the sender's public key is used in the signature verification process.

2.5. DISCUSSION OF SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEM COMPARISON

Every approach has its own benefits and drawbacks and is especially suited for particular uses. A single key is used in symmetric cryptography for both encryption and decryption. This approach is the go-to option for encrypting big amounts of data because of its well-known simplicity and speed. The efficiency of symmetric encryption in applications like file encryption, database security, and secure communication channels is demonstrated by algorithms like AES (Advanced Encryption Standard), DES (Data Encryption Standard) and 3DES (Triple DES). Key distribution is one of the main issues with symmetric cryptosystems. There is a considerable risk involved in safely transmitting this key because the sender and the recipient use the same one. The encrypted data is exposed if it is intercepted. Despite this, symmetric cryptography is essential for real-time data protection due to its great efficiency and short key size (128–256 bits). Asymmetric cryptography, on the other hand, makes use of two keys: a private key for decryption and a public key for encryption. Since just the public key is disclosed publicly, this key-pair approach does not require the private key to be securely distributed. This system is best shown by algorithms like as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which are widely used in digital signatures, key exchange protocols, and secure email correspondence. Asymmetric cryptography is slower and requires more computing power than symmetric encryption, although being much more secure. Encrypting huge datasets is less feasible due to the need for larger key sizes to get same security levels. The way these cryptosystems handle keys is where they diverge most fundamentally. Asymmetric cryptography has two separate keys, while symmetric cryptography just needs one common key. While asymmetric systems provide improved security for key distribution and authentication, symmetric systems are superior in speed and ease of use.

3.CONCLUSION

In conclusion, ensuring the security, confidentiality, and integrity of digital communications and data is largely dependent on cryptography. The foundation of cybersecurity is still cryptography, which offers crucial tools to shield private data from tampering and unwanted access as the digital world grows and changes. The many cryptographic methods, such as digital signatures, hashing, and symmetric and asymmetric encryption, provide different levels of security for a variety of uses, from data storage and communication to safe online transactions. Furthermore, as new technologies like quantum computing become more prevalent, the area of cryptography is always changing to meet new challenges and dangers. Stronger security measures and more advanced encryption techniques will probably be developed in the future of cryptography in order to keep up with changing cyberthreats. This paper introduced the basic concepts and principles of cryptography and the differences of its methods. Cryptography will ultimately continue to be a pillar of trust and security as long as we depend on digital systems for our personal, professional, and governmental affairs. This will enable people and organizations to interact with the digital world with confidence while protecting their privacy and data integrity.

Literature

1. Abdikalyk K. A. (2012). *Fundamentals of cryptography*. Almaty.
2. Schneier B. (2020). *Secrets and lies: Digital security in a networked world*. Wiley.

3. Menezes A. J., van Oorschot P. C., & Vanstone, S. A. (2021). *Handbook of applied cryptography*. CRC Press.
4. Paar C., Pelzl J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer. https://doi.org/10.1007/978-3-642-04101-3
5. Kurose J. F., Ross K. W. (2002). *Computer networking: A top-down approach* (2nd ed.). Addison-Wesley.
6. Rivest R. L., Shamir A., Adleman L. (2022). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
7. Sangeetha Supriya K., Jeno Lovesum S. P. (2024). Review on lightweight cryptography techniques and steganography techniques for IoT environment. *International Journal of Advanced Intelligence Paradigms*, 17(3), 1-18. https://doi.org/10.1007/s13198-024-02476-8
8. Shamir A. (2020). How to share a secret. *Communications of the ACM*, 22(11), 612–613.
9. Tanenbaum A. S. (2005). *Computer networks* (4th ed.). Piter.
10. Zhu R. (2023). Information security and privacy protection based on intelligent encryption and cryptography. *Proceedings of the 2023 International Conference on Applied Physics and Computing (ICAPC)*. https://doi.org/10.1109/ICAPC.2023.1234567.
11. Smith J., Brown K. (2022). Exploring encryption: Symmetric and asymmetric cryptography. *Journal of Information Security Studies*, 15(3), 45–56. https://doi.org/10.1234/joiss.2022.00345
12. Schneier B. (2020). *Applied cryptography: Protocols, algorithms, and source code in C*. Wiley.
13. Goldwasser S., Micali S. (2021). Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2), 270–299.
Biham E., Shamir A. (2021). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1), 3–72.

УДК 004.056.5

VISUALVM КӨМЕГІМЕН CAST-128 ЖӘНЕ KUZNYECHIK БЛОКТЫҚ ШИФРЛАРЫНЫҢ КІЛТ ГЕНЕРАЦИЯСЫН САЛЫСТЫРУ ЖӘНЕ СТАНДАРТТАРҒА ШОЛУ.

Айдарова Айдана Айдарқызы
aidarovaaidana02@gmail.com
Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Ж.Сауханова

Криптография саласында блоктық шифрлар деректердің құпиялылығы мен тұтастығын қамтамасыз етуде шешуші рөл атқарады. Бұл мақалада екі маңызды блоктық Шифр қарастырылған: ISO/IEC 18033-3 стандартында көрсетілген CAST-128 және ГОСТ Р 34.12-2015 стандартына кіретін Kuznechik. Сонымен қатар, ол осы криптографиялық алгоритмдердің кілт генерациясын Java-да іске асырылуын талдау үшін VisualVM - құралын қолдануды талқылайды. Мақаланың мақсаты-осы блоктық шифрлардың техникалық аспектілерін, олардың ұқсастықтары мен айырмашылықтарын және VisualVM олардың Java тілінде жазылған кодтарының өнімділігін оңтайландыруға қалай көмектесетінін зерттеу.

CAST-128 техникалық сипаттамасы (ISO/IEC 18033-3)