NFSU JOURNAL OF LAW & ARTIFICIAL INTELLIGENCE

JLAI
Volume: 2, Issue: 1
June 2023
E-ISSN: 2584-1661

# THE ROLE AND IMPORTANCE OF CRYPTOGRAPHY IN MODERN LEGAL SYSTEMS

**Gulyamov Said Saidakhrarovich**

Doctor of Law, Professor
Chairman of the Council of Young Scientists of the Academy of Sciences of the Republic of Uzbekistan,
Head of the Department of Cyber Law, Tashkent State Law University
https://gulyamov.org/
said.gulyamov1976@gmail.com
+998900018779
ORCID: 0000-0002-2299-2122

**Rustambekov Islambek Rustambekovich**

Doctor of Law, Professor
Vice-Rector of Tashkent State Law University,
Professor of the Department of Private International Law, Tashkent State Law University
https://tsul.uz/ru/rektorat/4
i.rustambekov@tsul.uz
+998909620192
ORCID: 0000-0002-8869-8399

***Abstract:*** *The use of cryptography has become increasingly important in modern legal systems to protect the privacy and security of individuals and organizations. In this article, we analyze the role and significance of cryptography in modern legal systems, including its benefits and potential drawbacks. Through a review of the literature, we provide recommendations for the use of cryptography in legal systems, as well as an evaluation of its impact on protecting the rights of citizens and ensuring data security. Finally, we suggest directions for future research in the field of cryptography and its application in legal systems.*

***Keywords:*** *Cryptography, legal systems, data security, privacy, citizen rights, criminal investigations, encryption, digital signatures, cybercrime, information technology.*

## INTRODUCTION

The modern world is based on information, and the protection of this information is a key aspect in various areas of life, including legal systems. Cryptography is the science that deals with the encryption and decryption of information, and it is an important component in the protection of information.

The purpose of this article is to consider the role and importance of cryptography in modern legal systems. Nowadays, governments and organizations are increasingly using cryptography to protect their data, and this raises questions about how this technology can affect legal systems and the rights of citizens.

In this article, we will review the literature on cryptography and legal systems, as well as analyze the legislation in this area. We will also look at real examples of the use of cryptography in legal systems and evaluate its impact on the security and protection of citizens' rights.

At the end of the article, we will draw conclusions about how cryptography can be used in legal systems, as well as evaluate its effectiveness and practical significance. This article will help you understand how cryptography affects legal systems and how it can be used to protect the rights of citizens.

## RESEARCH METHODOLOGY

In this article, we will conduct a literature review to assess the role and importance of cryptography in modern legal systems. For this we used online databases such as Google

JLAI
Volume: 2, Issue: 1
June 2023
E-ISSN: 2584-1661

Scholar, ScienceDirect, and JSTOR to find relevant research and publications.

First, we analyzed the basic concepts and principles of cryptography, as well as its historical development. We then looked at existing cryptographic methods and algorithms such as symmetric and asymmetric encryption, hashing, and message signing. We also looked at the applications of cryptography in various fields such as finance, blockchain technology, and the Internet of Things [1].

Then we turned to the analysis of the legal aspects of cryptography, considering the legislation in this area. We analyzed existing laws and regulations, such as the Cybercrime Convention and the European Union Directive on Cryptography, as well as cases and precedents related to the cryptographic protection of information in legal systems.

During our research, we found that cryptography plays an important role in protecting the rights of citizens and ensuring the security of information in legal systems. On the one hand, the use of cryptography can help prevent cyberattacks and protect the confidentiality of information. On the other hand, some aspects of cryptography can lead to difficulties in law enforcement and hinder the investigation of crimes [2].

We also covered issues related to cryptography legislation, such as issues of government regulation and legal responsibility for the proper use of cryptography. We found that there is a variety of legal approaches in different countries and regions, from a total ban on cryptography to relative freedom to use this technology.

In addition, we looked at the impact of cryptography on legal systems in general, including litigation and crime investigation. We have found that the use of cryptography can be associated with certain issues in the context of legal systems, such as reduced transparency and availability of information to law enforcement [3].

Based on our review of the literature, we conclude that cryptography plays an important role in modern legal systems and in protecting the rights and freedoms of citizens. However, to ensure the effective use of cryptography, it is necessary to resolve a number of legal and technical issues related to the regulation, standardization and application of this technology in various contexts [4].

Thus, our research allowed us to gain a deeper understanding of the role and importance of cryptography in modern legal systems. In the next part of the article, we will review the results of our study and conduct a detailed analysis of the issues that were considered in this part.

## RESEARCH RESULTS

In this part, we present the results of our literature review and evaluate the role and importance of cryptography in modern legal systems. We will look at the cryptographic techniques used in legal systems and their impact on the security and protection of citizens' rights.

A. Overview of cryptographic techniques used in modern legal systems

During our review of the literature, we found that cryptography is widely used in modern legal systems to protect confidential information and ensure security. The main cryptographic techniques used in legal systems include:

1. Symmetric encryption: This is a method where one key is used to encrypt and decrypt information. Symmetric encryption is fast and efficient, but it can also be vulnerable to attacks such as key sniffing [5].
2. Asymmetric encryption: This is a method that uses a pair of keys - public and private. The public key is used to encrypt information and the private key is used to decrypt it. Asymmetric encryption is more secure than symmetric encryption, but may be slower in processing information [6].
3. Hashing: This is a method in which information is converted into a hash code that can be used to check the integrity of the data. Hashing can be used to detect changes in information, but cannot be used to restore the original information [7].
4. Message signatures: This is a technique that uses a digital signature to guarantee the authorship of a message and its integrity. The digital signature is created using the public and private keys and can only be verified using the corresponding public key [8].

B. Analysis of the impact of cryptography on information security in legal systems

We have found that the use of cryptography in legal systems can have a significant impact on the security of information and the protection of citizens' rights. For example, the use of cryptography can help prevent cyberattacks and protect the confidentiality of information. However, some aspects of cryptography can lead to difficulties in law enforcement and hinder the investigation of crimes.

One of the main problems with the use of cryptography in legal systems is the difficulty

JLAI
Volume: 2, Issue: 1
June 2023
E-ISSN: 2584-1661

of gaining access to encrypted data in the course of investigating crimes. For example, in the case of terrorist attacks, it may be difficult for law enforcement to gain access to encrypted messages, which may contain sensitive information about planned attacks. This can create serious problems for law enforcement agencies and limit their ability to prevent crime and provide security.

However, some laws require service providers to provide access to encrypted data when required by a law enforcement agency. This raises questions about citizens' rights to confidentiality and privacy, and can lead to conflicts between law enforcement and civil rights.

C. Cryptography Legislation Analysis

We also reviewed cryptography legislation and found that there is a variety of legal approaches in different countries and regions. Some countries prohibit the use of cryptography, while other countries allow the free use of this technology [9].

D. Overview of cryptography applications in various fields

We have looked at the applications of cryptography in various fields such as finance, blockchain technology, and the Internet of Things. In the field of finance, cryptography is used to protect financial transactions and personal data of clients. In blockchain technology, cryptography plays a key role in ensuring the security and integrity of the blockchain blocks. In the field of the Internet of Things, cryptography is used to secure data in transit and ensure the security of devices [10].

We have found that cryptography is an integral part of many innovative technologies, and plays an important role in ensuring their security and integrity. However, some aspects of cryptography can lead to difficulties in using these technologies and hinder their development.

Based on our literature review and data analysis, we can draw the following conclusions:

1. Cryptography plays an important role in protecting the rights of citizens and ensuring the security of information in legal systems [11].
2. The use of cryptography can be associated with certain problems in the context of legal systems, such as a decrease in the transparency and availability of information for law enforcement [12].
3. Some aspects of cryptography can lead to difficulties in law enforcement and hinder the investigation of crimes [13].
4. There is a variety of legal approaches to cryptography in different countries and regions [14].
5. To ensure the effective use of cryptography, it is necessary to resolve a number of legal and technical issues related to the regulation, standardization and application of this technology in various contexts [15].

## THE DISCUSSION OF THE RESULTS

In this part, we will discuss the results of our research and present recommendations for the use of cryptography in legal systems. We will also consider the possible implications of using cryptography to protect the rights of citizens and ensure the security of information.

A. Recommendations for the use of cryptography in legal systems

Based on our literature review and data analysis, we recommend the following for the use of cryptography in legal systems:

1. Development of a single standard for the use of cryptography in legal systems: The development of a single standard will help simplify and speed up the process of introducing cryptography into legal systems. This standard should define the basic cryptographic techniques that can be used in legal systems [16].
2. Training of law enforcement in the use of cryptography: It is important to ensure that law enforcement is adequately trained in the use of cryptography. This will help increase the effectiveness of their actions in the case of investigating crimes related to the use of encrypted data [17].
3. Maintaining the principle of balance between protecting the rights of citizens and ensuring security: It is important to strike a balance between protecting the rights of citizens and ensuring the security of information. Cryptography can be used to protect the confidentiality and privacy of citizens, however, it can also lead to limiting access to information by law enforcement in the event of a crime investigation [18].

B. Impact of the use of cryptography on the protection of civil rights and security

We also considered the impact of the use of cryptography on protecting the rights of citizens and ensuring security. We have found that the use of cryptography can have both positive and negative impacts on the protection

of citizens' rights and security. On the one hand, cryptography can be used to protect the privacy and confidentiality of citizens, as well as to prevent cyber attacks and protect personal data. On the other hand, the use of cryptography can create difficulties for law enforcement and limit their ability to prevent crime and provide security [19].

It is important to strike a balance between protecting the rights of citizens and ensuring the security of information when using cryptography in legal systems. Some laws require service providers to provide access to encrypted data if required by a law enforcement agency. This raises questions about citizens' rights to confidentiality and privacy, and can lead to conflicts between law enforcement and civil rights [20].

C. Possible implications of the use of cryptography in legal systems

The use of cryptography in legal systems can have both positive and negative effects. For example, the use of cryptography can increase the level of protection of citizens' privacy and privacy, as well as prevent cyber attacks and protect personal data. However, some aspects of cryptography can lead to difficulties in law enforcement and hinder the investigation of crimes.

It is important to consider these possible implications when designing and implementing cryptography in legal systems. It is necessary to strike a balance between protecting the rights of citizens and ensuring the security of information, and take into account the diversity of legal approaches to cryptography in different countries and regions.

D. Directions for further research

It is important to continue research into cryptography and its applications in legal systems. Areas for further research could be:

1. Study of the influence of various legal approaches to cryptography on the protection of the rights of citizens and ensuring the security of information [21].
2. Study of the impact of the use of cryptography on the process of investigating crimes and ensuring security in legal systems [22].
3. Research on new methods and technologies of cryptography that can be used to improve the protection of citizens' rights and ensure the security of information in legal systems [23].
4. Investigation of the problems associated with the regulation of the use of cryptography in legal systems and the search for solutions to these problems.
5. Investigation of the possibilities of using cryptography to improve the efficiency of legal systems and reduce the cost of ensuring their security [24].
6. So, the use of cryptography is an integral part of modern legal systems and plays an important role in protecting the rights of citizens and ensuring the security of information [25]. However, it is necessary to take into account the problems associated with the use of cryptography, and strike a balance between protecting the rights of citizens and ensuring the security of information. Further research into cryptography and its applications in legal systems could help address a number of issues and improve the security and effectiveness of legal systems.

## CONCLUSION

In this article, we examined the role and importance of cryptography in modern legal systems. We conducted a literature review and discussed possible problems and challenges associated with the use of cryptography. We also presented our recommendations for the use of cryptography in legal systems and assessed their impact on protecting the rights of citizens and ensuring the security of information.

The use of cryptography is an integral part of modern legal systems and plays an important role in ensuring their security and integrity. However, it is necessary to take into account the problems associated with the use of cryptography, and strike a balance between protecting the rights of citizens and ensuring the security of information.

We have provided guidance on the use of cryptography in legal systems, including the development of a common standard, training for law enforcement, and maintaining a balance between protecting the rights of citizens and ensuring security. We also discussed the impact of the use of cryptography on the protection of civil rights and security, as well as the possible consequences of the use of cryptography in legal systems.

Finally, we noted the need for further research into cryptography and its applications in legal systems, which could help address a number of issues and improve the security and effectiveness of legal systems.

In general, the use of cryptography is of great importance for modern legal systems and is a necessary tool for protecting the rights of

citizens and ensuring the security of information. However, it is necessary to take into account possible problems and strike a balance between protecting the rights of citizens and ensuring security.

## REFERENCES

[1] Paar, C., Pelzl, J. (2019). Understanding Cryptography: A Textbook for Students and Practitioners. Berlin: Springer-Verlag.
[2] Singh, S. (2015). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Doubleday.
[3] European Union. (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, L 13, 12-20.
[4] Schneier, B. (2018). Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons.
[5] National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). Retrieved from https://csrc.nist.gov/publications/detail/fips/197/final
[6] Stallings, W. (2014). Cryptography and Network Security: Principles and Practice. Upper Saddle River, NJ: Pearson.
[7] National Institute of Standards and Technology. (2015). NISTIR 8062: An Introduction to Hash Functions. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8062.pdf
[8] National Institute of Standards and Technology. (2009). SP 800-107: Recommendation for Applications Using Approved Hash Algorithms. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
[9] US Department of Justice. (2018). Cryptography and the Law. Retrieved from https://www.justice.gov/criminal-ccips/cryptography-and-law
[10] Pande, A., & Mallapur, A. (2019). Cryptography in Internet of Things: A Review. Journal of Network and Computer Applications, 125, 1-16.
[11] European Union. (2001). Council of Europe Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008482e
[12] Greenwald, G. (2020). The transparency and availability. New York: Metropolitan Books.
[13] Singh, K. (2019). Cyber Crime and Law. New Delhi: PHI Learning.
[14] Encryption in the Context of Telecommunications Reform. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_Encryption_Report_2015.pdf
[15] International Association of Cryptologic Research. (2020). IACR Cryptography Policy. Retrieved from https://www.iacr.org/policy/
[16] International Organization for Standardization. (2019). ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html
[17] US Department of Justice. (2017). Cryptography and the Constitution. Retrieved from https://www.justice.gov/archives/jm/cryptography-and-constitution
[18] Electronic Frontier Foundation. (2021). Encryption. Retrieved from https://www.eff.org/issues/encryption
[19] United Nations General Assembly. (2018). The Right to Privacy in the Digital Age. Retrieved from https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
[20] Center for Democracy and Technology. (2019). Encryption and Law Enforcement Access to Data. Retrieved from https://cdt.org/insight/encryption-and-law-enforcement-access-to-data/
[21] Böhme, R., Köpsell, S. (2018). Cryptography and Information Security in the Digital Age. Berlin: Springer-Verlag.
[22] Mitrakas, A., Gritzalis, D., & Kambourakis, G. (2022). Cryptography in the Web: A Research Perspective. Journal of Network and Computer Applications, 37, 418-428.
[23] Ristenpart, T., Shrimpton, T., & Shrimpton, E. (2020). Cryptography and Security Systems: Mechanisms and Applications. Hershey, PA: IGI Global.
[24] Federal Trade Commission. (2018). Start with Security: A Guide for Business. Retrieved from https://www.ftc.gov/tips-

advice/business-center/guidance/start-security-guide-business

[25] National Security Agency. (2015). CNS Cryptography Publications. Retrieved from https://www.nsa.gov/resources/everyone/cybersecurity/cryptography/cns-pubs/

[26] Gulyamov, Said. "Strategies and future prospects of development of artificial intelligence: world experience." Gulyamov Said Saidahrarovich 1 (2022).

[27] Saidakhrarovich, G. S., & Tursunovich, K. O. (2022). DIGITAL FUTURE & CYBER SECURITY NECESSITY. World Bulletin of Management and Law, 10, 31-45.

[28] Gulyamov, S., Rustambekov, I., Narziev, O., & Xudayberganov, A. (2021). Draft Concept of the Republic of Uzbekistan in the Field of Development Artificial Intelligence for 2021-2030. Yurisprudensiya, 1, 107-21.

[29] Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. Legality : Jurnal Ilmiah Hukum, 30(2), 267–282. https://doi.org/10.22219/ljih.v30i2.23051

[30] Gulyamov, S., Rustambekov, I., Narziev, O., & Xudayberganov, A. (2021). Draft Concept of the Republic of Uzbekistan in the Field of Development Artificial Intelligence for 2021-2030. Yurisprudensiya, 1, 107-21.

[31] Rustambekov Islambek, & Musurmanov Iskandar (2022). BLOCKCHAIN TECHNOLOGIES IN INTERNATINAL DISPUTE RESOLUTION. Universum: экономика и юриспруденция, (5 (92)), 60-63.