IT technologies, energy, automation and computer engineering

DOI: https://doi.org/10.53002/103

ENCRYPTION OF INFORMATION USING ARDUINO MICROCONTROLLERS

[1*]Baimagambetova A., [2]Faridl M.

[1]NPJSC "Karaganda Industrial University", Temirtau, Kazakhstan
[2]Elementry Education IKIP PGRI Wates (IPW), Yogyakarta, Indonesia
**Corresponding author e-mail: altinai_76@mail.ru*

Authors information:
Baimagambetova Altynai, NPJSC "Karaganda Industrial University", Temirtau, Kazakhstan, e-mail: altinai_76@mail.ru
Faridl Musyadad, Elementry Education IKIP PGRI Wates (IPW), Yogyakarta, Indonesia. Orcid: https://orcid.org/0000-0002-3968 -7845, e-mail: faridlmusyadad@ipw.ac.id

Abstract — This paper presents a comprehensive analysis of symmetric and asymmetric encryption algorithms and their application in embedded systems based on the Arduino platform. The rapid growth of Internet of Things (IoT) technologies and resource-constrained devices has increased the demand for efficient cryptographic solutions capable of ensuring data confidentiality, integrity, and authenticity while operating under limited computational and memory resources. In this context, selecting an appropriate encryption algorithm is a critical factor in developing secure embedded applications. The study examines the theoretical principles of symmetric and asymmetric cryptography, highlighting their operational mechanisms, key management approaches, advantages, and limitations. Particular attention is given to widely used algorithms and cryptographic libraries available for the Arduino platform. Their implementation features, computational complexity, memory consumption, execution speed, and suitability for low-power microcontrollers are analyzed. The paper also discusses the practical aspects of integrating cryptographic functions into embedded applications designed for secure communication and data protection. The analysis demonstrates that symmetric encryption algorithms provide high processing speed and low resource consumption, making them suitable for real-time applications on microcontrollers, whereas asymmetric algorithms offer enhanced key distribution and authentication capabilities despite their higher computational requirements. The obtained results indicate that the effectiveness of cryptographic protection depends on balancing the required security level with the hardware limitations of embedded devices. The study concludes with practical recommendations for selecting encryption algorithms and cryptographic libraries for Arduino-based systems, contributing to the development of reliable and secure IoT applications and embedded information security solutions.
Keywords — encryption, cryptography, symmetric algorithms, asymmetric algorithms, data protection, Arduino, microcontroller, devices with limited resources, programming, cryptographic libraries, security protocols, information security, implementation of encryption algorithms, data authentication, hash functions.

ARDUINO МИКРОКОНТРОЛЛЕРЛЕРІ АРҚЫЛЫ АҚПАРАТТЫ ШИФРЛАУ

[1*]Баймагамбетова А. Х., [2]Faridl M.

«Қарағанды индустриялық университеті» КеАҚ, Теміртау, Қазақстан
[2]Elementry Education IKIP PGRI Wates (IPW), Yogyakarta, Indonesia
**Автор-корреспондент e-mail: altinai_76@mail.ru*

Авторлар туралы ақпарат:
Баймагамбетова Алтынай Хамитовна, «Қарағанды индустриялық университеті» КеАҚ, Теміртау, Қазақстан, e-mail: altinai_76@mail.ru
Faridl Musyadad, Elementry Education IKIP PGRI Wates (IPW), Джогякарта, Индонезия Orcid: https://orcid.org/0000-0002-3968 -7845, e-mail: faridlmusyadad@ipw.ac.id

Аңдатпа — Жұмыста Arduino платформасына негізделген ендірілген жүйелерде қолданылатын симметриялық және асимметриялық шифрлау алгоритмдеріне кешенді талдау жүргізілді. Заттар интернеті (IoT) технологияларының және есептеу ресурстары шектеулі құрылғылардың қарқынды дамуы деректердің құпиялылығын, тұтастығын және түпнұсқалығын қамтамасыз ететін тиімді криптографиялық құралдарды қолдану қажеттілігін арттырды. Осыған байланысты қорғалған ендірілген қосымшаларды әзірлеу барысында

шифрлау алгоритмін дұрыс таңдау маңызды міндеттердің бірі болып табылады. Зерттеуде симметриялық және асимметриялық криптографияның теориялық негіздері қарастырылып, олардың жұмыс істеу қағидалары, криптографиялық кілттерді басқару ерекшеліктері, артықшылықтары мен шектеулері сипатталды. Arduino платформасында кеңінен қолданылатын криптографиялық алгоритмдер мен кітапханалардың іске асырылу ерекшеліктеріне ерекше назар аударылды. Олардың есептеу күрделілігі, жадты пайдалану деңгейі, орындау жылдамдығы және аппараттық ресурстары шектеулі микроконтроллерлерде қолдануға жарамдылығы талданды. Сонымен қатар, криптографиялық функцияларды қауіпсіз деректерді беру және сақтау жүйелеріне енгізудің практикалық аспектілері қарастырылды. Зерттеу нәтижелері симметриялық алгоритмдердің жоғары жылдамдықпен жұмыс істейтінін және есептеу ресурстарын аз қажет ететінін көрсетті, сондықтан олар нақты уақыт режиміндегі микроконтроллерлік жүйелер үшін тиімді болып табылады. Ал асимметриялық алгоритмдер аутентификациялау мен криптографиялық кілттерді қауіпсіз тарату мүмкіндіктерін кеңейтеді, бірақ есептеу ресурстарын көбірек талап етеді. Алынған нәтижелер Arduino платформасында қорғалған қосымшаларды әзірлеу кезінде тиімді криптографиялық алгоритмдер мен кітапханаларды таңдауға негіз болады және Заттар интернеті құрылғыларының ақпараттық қауіпсіздігін арттыруға мүмкіндік береді.
Түйін сөздер — криптография, симметриялық алгоритмдер, асимметриялық алгоритмдер, деректерді қорғау, Arduino, микроконтроллер, ресурсы шектеулі құрылғылар, бағдарламалау, криптографиялық кітапханалар, қауіпсіздік протоколдары, ақпараттық қауіпсіздік, шифрлау алгоритмдерін іске асыру, деректер аутентификациясы, хэш-функциялар.

ШИФРОВАНИЕ ИНФОРМАЦИИ С ПОМОЩЬЮ МИКРОКОНТРОЛЛЕРОВ ARDUINO

[1*]Баймагамбетова А. Х., [2]Faridl M.

НАО «Карагандинский индустриальный университет», Темиртау, Казахстан
**Автор-корреспондент e-mail: altinai_76@mail.ru*

Информация об авторах:
Баймагамбетова Алтынай Хамитовна, НАО «Карагандинский индустриальный университет», Темиртау, Казахстан, e-mail: altinai_76@mail.ru
Faridl Musyadad, Elementry Education IKIP PGRI Wates (IPW), Джогякарта, Индонезия Orcid: https://orcid.org/0000-0002-3968 -7845, e-mail: faridlmusyadad@ipw.ac.id

Аннотация — В работе представлен комплексный анализ симметричных и асимметричных алгоритмов шифрования, а также особенностей их применения во встраиваемых системах на базе платформы Arduino. Стремительное развитие технологий Интернета вещей (IoT) и устройств с ограниченными вычислительными ресурсами обусловило необходимость использования эффективных криптографических средств, обеспечивающих конфиденциальность, целостность и подлинность передаваемых данных при минимальных затратах вычислительных ресурсов. В связи с этим выбор оптимального алгоритма шифрования является одним из ключевых факторов при разработке защищенных встроенных приложений. В исследовании рассмотрены теоретические основы симметричной и асимметричной криптографии, раскрыты принципы их работы, особенности управления криптографическими ключами, преимущества и ограничения. Особое внимание уделено наиболее распространённым алгоритмам и криптографическим библиотекам, реализованным для платформы Arduino. Выполнен анализ их вычислительной сложности, потребления памяти, скорости выполнения операций и пригодности для использования на микроконтроллерах с ограниченными аппаратными ресурсами. Также рассмотрены практические аспекты интеграции криптографических функций в системы безопасной передачи и хранения данных. Результаты исследования показали, что симметричные алгоритмы обеспечивают высокую скорость шифрования и низкое потребление ресурсов, что делает их наиболее эффективными для работы в режиме реального времени. Асимметричные алгоритмы обладают более широкими возможностями аутентификации и безопасного распределения ключей, однако требуют значительно больших вычислительных затрат. Полученные результаты позволяют обосновать выбор криптографических алгоритмов и библиотек при разработке защищённых приложений на платформе Arduino и способствуют повышению уровня информационной безопасности устройств Интернета вещей.
Ключевые слова — шифрование, криптография, симметричные алгоритмы, асимметричные алгоритмы, защита данных, Arduino, микроконтроллер, устройства с ограниченными ресурсами, Программирование, криптографические библиотеки, протоколы безопасности, Информационная безопасность, реализация алгоритмов шифрования, аутентификация данных, хеш-функции.

MAIN PROVISION

The implementation of modern cryptographic algorithms on Arduino-based embedded systems provides an effective approach to protecting transmitted and stored data while maintaining low hardware and energy requirements.

The integration of symmetric encryption methods, secure key management, and authentication mechanisms significantly enhances the cybersecurity of Internet of Things (IoT) devices based on Arduino platforms.

The use of lightweight cryptographic solutions enables the development of secure embedded systems suitable for real-time applications and resource-constrained environments.

INTRODUCTION

Every person has heard of data encryption, because it is used everywhere in our digital age. When visiting websites on the internet, traffic is encrypted using the https protocol, our data is stored encrypted on servers, not to mention that every person involved in the field of information security at least once faced the implementation of one or another encryption algorithm [1-3].

Most encryption programs run on a specific operating system installed on a particular computer, in this regard, no matter how reliable a particular encryption algorithm is, the original text can be stolen by an intruder if the computer was infected with a virus before the data was encrypted. Therefore, it is imperative to stop a scenario [4,5].

One alternative to encrypting data through a computer can be data encryption on a separate microcontroller, which is more difficult to crack and consumes less power.

One of the difficulties of this project is the implementation of the idea, since along with the time spent on development, financial investments will be required. To purchase the microcontrollers themselves and additional modules for entering text, displaying it on the screen, and a module for transferring it to another microcontroller [6].

Research gap. Although numerous studies have investigated cryptographic algorithms and information security, limited attention has been devoted to their practical implementation on low-cost Arduino-based embedded platforms. Most existing research focuses either on theoretical cryptographic methods or on high-performance computing systems, while comprehensive evaluations of lightweight encryption techniques, implementation complexity, computational performance, and applicability to resource-constrained IoT devices remain insufficient. Furthermore, comparative analyses of modern security standards and Arduino-based implementations are still limited.

Novelty statement. The novelty of this study lies in the comprehensive analysis of modern cryptographic methods for Arduino-based embedded systems with emphasis on lightweight implementation, secure data transmission, and practical cybersecurity applications. The study summarizes recent international security standards (ISO/IEC, NIST), evaluates the applicability of modern encryption techniques for resource-constrained devices, and provides practical recommendations for improving the security of Arduino-based IoT systems through efficient encryption, authentication, and key management mechanisms.

METODOLOGY

The methodology of this study was aimed at a comprehensive analysis of the technical capabilities of implementing encryption algorithms based on microcontrollers. At first, a review of domestic and foreign literature, research and open source projects was carried out regarding the application of cryptographic algorithms on the Arduino and ESP8266 platforms. This step allowed a better understanding of the practical differences between symmetric and asymmetric encryption approaches, their computational resource requirements, and the limitations of microcontrollers.

In the course of the study, the Arduino Uno, Arduino Mega and ESP8266 microcontrollers were chosen as the experimental base. The choice was justified by their wide distribution, available documentation and a large number of cryptographic libraries. The processes of text encryption and decryption were tested using specially prepared software modules. Indicators such as the execution time of encryption operations, the level of memory use, processor load were systematically measured. The effectiveness of each algorithm was evaluated in the context of specific hardware constraints, and the results obtained were analyzed in comparison [7,9].

A qualitative analysis of the security level of algorithms was also carried out. The cryptographic stability of each algorithm, key length-dependent weaknesses, and resistance against hardware attacks were studied. Separately, it was considered how key exchange procedures are performed in practice when exchanging data between devices, since this section defines the features of the application of symmetric and asymmetric approaches [9].

The use of these methodological approaches made it possible to comprehensively assess the effectiveness of the implementation of encryption algorithms on microcontrollers and justify the possibilities of their application in specific projects.

RESEARCH RESULTS AND DISCUSSION

If you choose a symmetric encryption algorithm, the encryption keys must be exchanged between the two devices in advance. And if you choose an asymmetric encryption algorithm, you do not need to exchange encryption keys in advance. Microcontroller algorithm with symmetric encryption algorithm:

1) two users exchange encryption keys by placing devices next to each other through a special module.

2) user a encrypts the message and sends it to user B.

3) User B decrypts the message.

Microcontroller algorithm with symmetric encryption algorithm:

1) Users A and B create private and public keys.

2) users exchange public keys over the Internet.

3) user a encrypts the message and sends it to user B.

4) user b decrypts the message.

The difference with pagers is that pagers are bought abroad and, as in Lebanon, there is a high probability that someone will intercept their batch and install explosive devices on them. If you encrypt using microcontrollers, then the probability of deploying an explosive device will be zero.

To implement data encryption algorithms, you can use Arduino microcontrollers, which are a popular tool in the world of electronics.

Arduino is a trademark of hardware and software tools for the creation and prototyping of systems, models and experiments in the field of Electronics, Automation, Process Automation and robotics.

You can use the popular AESLib library to encrypt information with Arduino microcontrollers (Fig. 1) [5]. As the name suggests, this library allows you to encrypt data using the AES symmetric encryption algorithm. They can be encrypted both for storage on the device and for sending via the internet module.

You can also use the ArduinoDES library. It provides the same functionality as AES, but the DES encryption algorithm is less secure than AES. Because AES is an improved version of the Des encryption algorithm.

A popular example of using the AESLib library in Arduino microcontrollers is the creation of the cipherbox supercoder by Dmitry Bright, a user of the habr website. He carried out the encryption, storage and decryption of the text. As well as the account system, including authorization and registration to access the data of new users. In its development, not only the AES encryption algorithm is used, but also Blowfish and Serpent.

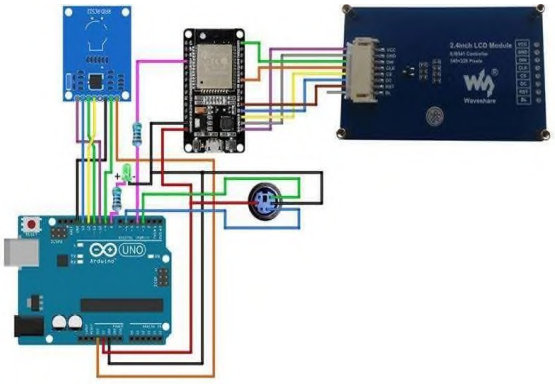

Fig. 1 – Schematic diagram of cipherbox supercoders

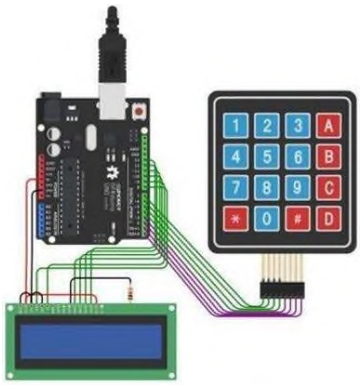

Fig. 2 – Microcontroller schemes for downloading firmware

Also on the English-language internet, you can find the implementation of asymmetric encryption algorithms, such as RSA, in Arduino microcontrollers (Fig. 2) [6]. A user named Aditya Pandey announced the implementation of cryptographic protocols between a personal computer and an Arduino board on the GitHub platform.

Arduino also has an implementation of the RSA encryption algorithm and esp8266 microcontrollers on GitHub, a user of “Murali mahadeva”.

Thus, despite the fact that there are ready-made implementations of symmetric and asymmetric encryption algorithms on the Internet, this topic does not lose its relevance, since it contains a huge potential for many developments in the field of Information Security, which, thanks to technical progress, can be implemented by anyone [10].

CONCLUSION

The analysis showed that microcontrollers have significant capabilities in implementing encryption algorithms. Modern Arduino and ESP8266 platforms are capable of performing complex cryptographic techniques such as AES or RSA, which makes them promising for autonomous security devices, data protection modules or network-independent

messaging systems. Despite the hardware limitations, the use of correctly selected algorithms and optimized libraries ensures sufficient encryption performance.

At the same time, the use of microcontrollers not only increases the security of data, but also reduces dependence on computer viruses and reduces the likelihood of attacks. In the future, further improvements in hardware cryptography and the emergence of new encryption libraries will make microcontrollers an integral part of security systems.

AUTHOR'S CONTRIBUTION

(taxonomy CRediT):

Baimagambetova A.: Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Visualization, Writing – original draft.

Faridl M.: Supervision, Validation, Writing-review & editing, Writing – review & editing.

CONFLICT OF INTEREST

The author claims that there is no conflict of interest in the implementation of this study and the publication of the article.

FUNDING

This research received no external funding.

ACKNOWLEDGMENT

The author expresses sincere gratitude to the editor and reviewer of the journal for valuable comments and recommendations that made it possible to carefully consider the manuscript and significantly improve the content and quality of the article.

REFERENCES

[1] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS PUB 197, Updated Edition. Gaithersburg, MD, USA: NIST, 2023.

[2] ISO/IEC 18033-3:2023, Information Security — Encryption Algorithms — Part 3: Block Ciphers. Geneva, Switzerland: International Organization for Standardization, 2023.

[3] National Institute of Standards and Technology (NIST), Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5. Gaithersburg, MD, USA: NIST, 2024.

[4] ISO/IEC 14888-3:2024, Information Security — Digital Signatures with Appendix — Part 3: Discrete Logarithm Based Mechanisms. Geneva, Switzerland: International Organization for Standardization, 2024.

[5] Arduino, "Arduino Documentation," Arduino S.r.l., 2025. [Online]. Available: https://docs.arduino.cc/. Accessed: Nov. 25, 2025.

[6] Arduino, “Arduino IDE 2 Documentation”, Arduino S.r.l., 2025. [Online]. Available: https://docs.arduino.cc/software/ide-v2/. Accessed: Nov. 25, 2025.

[7] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024. Heraklion, Greece: ENISA, 2024.

[8] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD, USA: NIST, Jan. 2023.

[9] ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: International Organization for Standardization, 2022.

[10] ISO/IEC 27400:2022, Internet of Things (IoT) — Security and Privacy — Guidance. Geneva, Switzerland: International Organization for Standardization, 2022.