Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

ҒТАМР 50.47.02
ӘОЖ: 681.518.5
DOI: 10.53002/103

Baimagambetova A. H.

Karaganda Industrial University, Temirtau, Kazakhstan
(E-mail: altinai_76@mail.ru)

Encryption of information using Arduino microcontrollers

This work comprehensively describes the theoretical foundations of symmetric and asymmetric encryption algorithms, their features, advantages and limitations. The scope of these algorithms in the field of data protection is also considered and the role in ensuring information security is analyzed. The paper presents options for the practical implementation of cryptographic libraries and algorithms widely distributed on the Arduino platform, discusses the principles of their work, application conditions, and effectiveness on limited device resources. The presented materials will allow you to evaluate the possibilities of data encryption on microcontrollers, as well as choose the right algorithm in the development of security-oriented applications.

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.

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.

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 such a scenario [2].

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.

Methodology

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.

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.

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.

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.

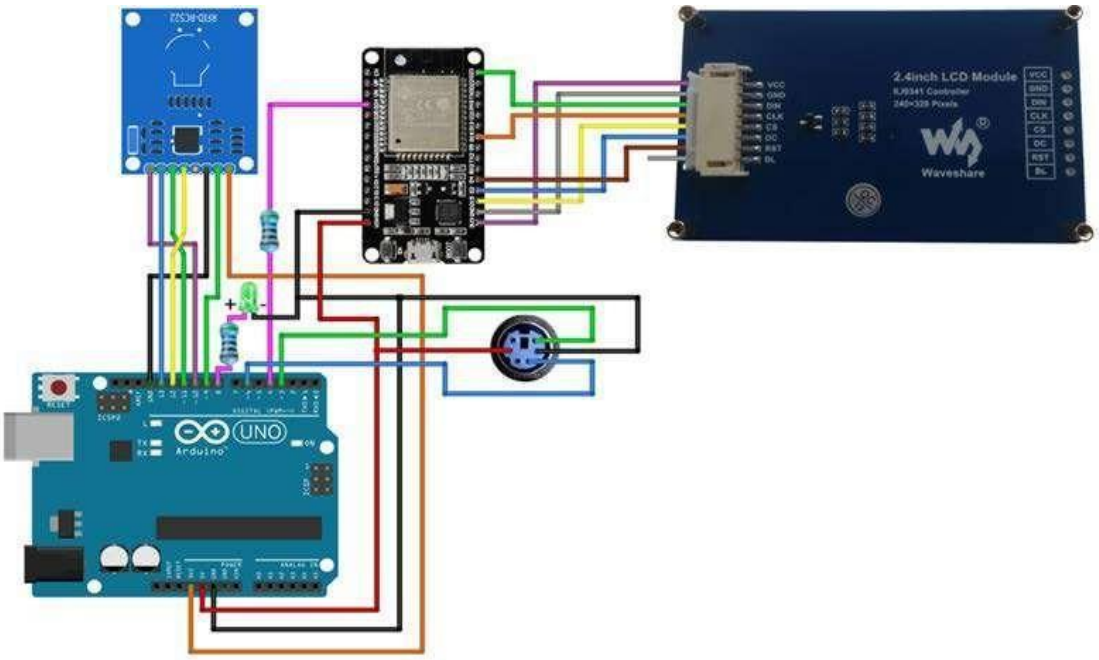
Arduino is a trademark of hardware and software tools for the creation and prototyping of systems, models and experiments in the field of Electronics, Automation, Process Automation and robotics.

You can use the popular AESLib library to encrypt information with Arduino microcontrollers. 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.

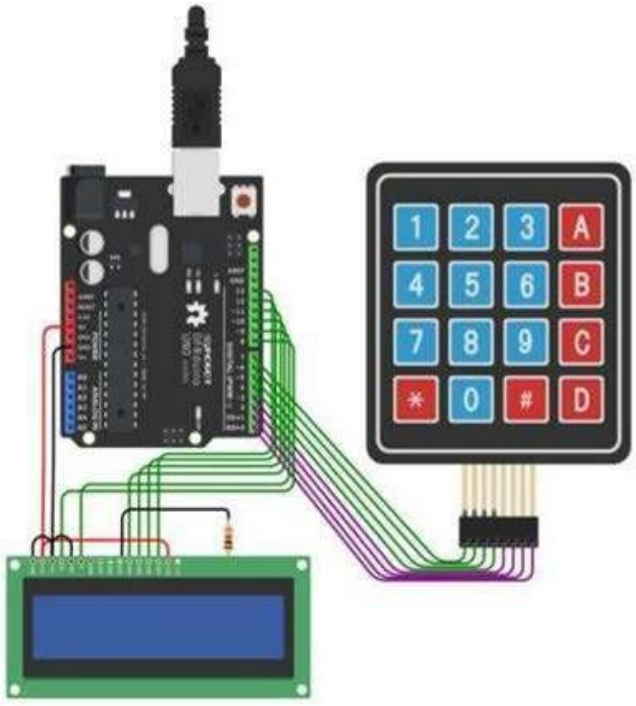
Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»



Сурет 1. Schematic diagram of cipherbox supercoders.

Also on the English-language internet, you can find the implementation of asymmetric encryption algorithms, such as RSA, in Arduino microcontrollers. 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". The main difference between the user" Aditya Pandey " from the implementation is that users do not need a computer to exchange messages, two microcontrollers connected to the Internet are enough.



Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

Сурет. 2. Microcontroller schemes for downloading firmware

In addition to these two examples, there are many implementations of AES and RSA on microcontrollers on the Internet, designed as training tools that cannot be used in real projects, but help novice programmers understand this topic.

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.

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. This approach opens up new opportunities for the development of the information security industry. In the future, further improvements in hardware cryptography and the emergence of new encryption libraries will make microcontrollers an integral part of security systems.

Referernces

1. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. - Berlin: Springer, 2002. - Access mode: DOI: 10.1007/978-3-662-04722-4.

2. Schneier B. Description of a new variable-length key, 64-bit block cipher (Blowfish) // Fast Software Encryption: Cambridge Security Workshop. - Berlin: Springer, 1993. - Access mode: DOI: 10.1007/3-540-58108-1_24.

3. Anderson R., Kuhn M. Tamper resistance – a cautionary note // Proceedings of the Second USENIX Workshop on Electronic Commerce. — 1996. — P. 1–11.

4. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. - 1987. - Vol. 48, № 177. - P. 203–209. - Access mode: DOI: 10.1090/S0025-5718-1987-0866112-7.

5. Arduino. Arduino Documentation. — Arduino S.r.l., 2023. - Access mode: https://docs.arduino.cc/ (date of request: 25.11.2025)

6. Arduino. Arduino Documentation. — Arduino S.r.l., 2023. - Access mode: https://docs.arduino.cc/ (date of request: 25.11.2025)

Баймагамбетова А. Х.

Arduino микроконтроллерлері арқылы ақпаратты шифрлау

Бұл жұмыс симметриялық және асимметриялық шифрлау алгоритмдерінің теориялық негіздерін, олардың ерекшеліктерін, артықшылықтары мен шектеулерін жан-жақты сипаттайды. Сонымен қатар деректерді қорғау саласындағы осы алгоритмдердің қолданылу аясы қарастырылып, ақпараттық қауіпсіздікті қамтамасыз етудегі рөлі талданады. Жұмыста Arduino платформасында кең таралған криптографиялық кітапханалар мен алгоритмдердің практикалық іске асырылу нұсқалары ұсынылады, олардың жұмыс принциптері, қолдану жағдайлары және құрылғылардың шектеулі ресурстарында тиімділігі талқыланады. Ұсынылған материалдар микроконтроллерлерде деректерді шифрлау мүмкіндіктерін

Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

бағалауға, сондай-ақ қауіпсіздікке бағытталған қолданбалар әзірлеуде дұрыс алгоритмді таңдауға мүмкіндік береді.

Түйін сөздер: шифрлау, 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.

Баймагамбетова А. Х.

Шифрование информации с помощью микроконтроллеров Arduino

В данной работе подробно описаны теоретические основы симметричных и асимметричных алгоритмов шифрования, их особенности, преимущества и ограничения. Также рассматривается сфера применения данных алгоритмов в области защиты данных и анализируется их роль в обеспечении информационной безопасности. В работе представлены варианты практической реализации криптографических библиотек и алгоритмов, распространенных на платформе Arduino, обсуждаются принципы их работы, варианты применения и эффективность на ограниченных ресурсах устройств. Представленные материалы позволяют оценить возможности шифрования данных в микроконтроллерах, а также выбрать правильный алгоритм при разработке приложений, ориентированных на безопасность.

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.

Список литературы

1. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. - Berlin: Springer, 2002. - Режим доступа: DOI: 10.1007/978-3-662-04722-4.

2. Schneier B. Description of a new variable-length key, 64-bit block cipher (Blowfish) // Fast Software Encryption: Cambridge Security Workshop. - Berlin: Springer, 1993. - Режим доступа: DOI: 10.1007/3-540-58108-1_24.

3. Anderson R., Kuhn M. Tamper resistance – a cautionary note // Proceedings of the Second USENIX Workshop on Electronic Commerce. — 1996. — P. 1–11.

4. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. - 1987. - Vol. 48, № 177. - P. 203–209. - Режим доступа: DOI: 10.1090/S0025-5718-1987-0866112-7.

5. Arduino. Arduino Documentation. — Arduino S.r.l., 2023. - Режим доступа: https://docs.arduino.cc/ (дата обращения: 25.11.2025)

6. Arduino. Arduino Documentation. — Arduino S.r.l., 2023. - Режим доступа: https://docs.arduino.cc/ (дата обращения: 25.11.2025)