Bobylev Yaroslav Olegovich
Student
Ural Federal University named after the first
President of Russia B.N. Yeltsin
Russia, Ekaterinburg
Academic supervisor: Zarifullina Darya Pavlovna

ALGORITHMS AND METHODS OF CRYPTOGRAPHY

Abstract. *Nowadays cryptography means a lot in terms of safety of people's personal data. This article addresses to the main principle of management, storage of private and public keys in cryptography, methods and algorithms including autonomous hardware-based cryptography and improved algorithm of visual cryptography.*

Keywords: *cryptography, blockchain, vulnerability, data leakage, hardware-based security, public key infrastructure.*

Бобылев Ярослав Олегович
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Зарифуллина Дарья Павловна

АЛГОРИТМЫ И МЕТОДЫ КРИПТОГРАФИИ

Аннотация. *В современном мире криптография очень много значит с точки зрения безопасности личных данных людей. В этой статье мы исследуем основной принцип управления, хранения закрытых и открытых ключей в*

криптографии, методы и алгоритмы, включая автономную аппаратную криптографию и улучшенный алгоритм визуальной криптографии. .

Ключевые слова: *криптография, инфраструктура открытых ключей, аппаратная безопасность, блокчейн, уязвимость, утечка данных.*

Nowadays there is a huge information flow, which has increased significantly over the past decades, due to the fact that many areas of life and production are undergoing digitalization, and some have already completely switched to a digital society. Therefore, it is necessary to think about data security. It is important to study cryptography.

Efficient and secure key management is a challenge for any cryptographic system. If intruder is able to discover the keys to any mechanism like bruit force, side channel attack, physical access of system, weak encryption, replay attack etc. then intruder is able to steal everything from the targeted system. Therefore, the management of keys is one of the most critical components of the cryptographic system. The infrastructure is not secured if its keys have public access. Blockchain infrastructure uses PKI (Public Key Infrastructure) to authenticate the IoT devices and the security of the infrastructure depends on the trustiness of the third party.

Public Key Infrastructure is one of the mechanisms to manage the keys in the public key cryptographic systems. Blockchain also utilizes the services of the third party through PKI to authenticate the nodes of the Blockchain network. There are many Blockchain based PKI approaches in the field of Blockchain Technology which reduce the dependency on the third party for authenticating the nodes. However, minimizing the dependency on the third party by using the efficient key management is still a big challenge in the field of Blockchain Technology.

The principle of key management through PKI is simple, first of all, the user creates a key pair through the registration authority, which sends the confirmed data to certification authority. The certification authority issues a public key certificate to the user confirming that he owns the private key that corresponds to that public key.

Further, the verification authority can confirm the ownership of the public key to the user upon presentation of the private one [1].

With the advent of this key management there is the growth of independent device features such as microcontrollers, development cards or any device with Linux embedded, cryptography tasks can be decentralized and therefore provide security to any required information without the use of PC-type devices, smart phones or similar.

To have very independent systems that offer a sufficient security scheme has become a necessity, this because of the proliferation of IoT type systems and similar. In general, it is required to make stand-alone systems very independent and distributed to offer users a solution to this need.

The work of this type is limited. Therefore, for solving information security problems it is necessary to study the applications of light cryptography. One of the lightweight algorithms with better performance is a hardware key application that uses as a basis the HIGHT algorithm. It is used in a microcontroller in standard C++ code. It is easily portable to any device of similar characteristics and supports this programming language. It is able to make a very independent stand-alone application that has the ability to perform cryptographic functions and then implement a Hardware Safety Module that meets the needs of embedded applications today.

The implementation of the algorithm in C++ code was done in a standard way, so its migration to other devices did not require executing big changes in the programming. Now discuss the cipher scheme of the HIGHT algorithm. Starting with the plain text (64 bits) and the key (128 bits), the Key Schedule function is in charge of generating the Whitening Key used in the initial and final transformation. Then the initial transformation is performed, using the first 4 Whitening Keys generated previously and performing XOR operations and modular addition with the plain text. The last step of the encryption process is the final transformation, this function uses the latest Whitening Key, and the 8-byte text generated and performs XOR and modular addiction operations easily implemented in C language, the result of this process is a 64-bit (8 bytes) text called cipher text. While for the decryption block, it is necessary to do the following [2]:

1. The Key Schedule process is performed exactly as in the encryption process.

2. Firstly the final transformation is applied and finally the initial transformation, after the 32 rounds the initial one is applied.

3. In the opposite direction, the XOR operation is kept the same, although the modular addition is changed by modular subtraction, in C language it is only changing the + sign by -.

Cryptography is one of the vital techniques, which not only provides data privacy but also ensures message integrity and authentication. However, the conventional cryptography algorithm needs more computation for enciphering and deciphering the data as well as it is liable to many security attacks.

One of the new cryptographic techniques is Visual Cryptography based on secret sharing developed by Naor and Shamir, which provides more data confidentiality while it requires less computation power only. This technique can decode concealed images without any mathematical computations. Any user who has no knowledge of cryptography algorithm can use it effortlessly without the requirement of any computation complexity. This technique divides the original image into a number of shares, which is called encryption. Each pixel of image is divided into 2 sub pixels. There are only four possible combinations in the pixel division, which result in the form of entire black or partially black and white pixel. Later it extracts the original image by superimposing the entire shares one over the other, which is called decryption.

The secret image becomes accessible to every individual member and there is an inherent risk of any one of the members in the group using the valuable information for illegal purposes as an intruder. To overcome this problem, the proposed algorithm Secret Image Enhanced Sharing using Visual Cryptography diligently facilitates any member in the group to retrieve either only a part or the complete secret image based purely on his access privilege rights only.

The proposed system uses predicate encryption technique for protecting secret information and Least Significant Bits (LSB) encoding algorithm is used to embed the encrypted data to avoid the data modification.

Predicate encryption is a special type of asymmetric encryption system and it was contributed by Dan Boneh. One of the main features of this algorithm is that the intended recipient can decrypt only part of the encrypted message received from the sender based on his privilege rights. In predicate encryption, an encrypted message is associated with feature and a private key associated with a predicate and the recipient who has a private key associate with this feature can decrypt an encrypted message.

The LSB encoding is a simple technique to embed the secret information into cover image. This technique replaces the position of bits in the cover image with secret image. In case of 24-bit color image, three bits of information in every pixel are replaced with information of secret image. The changes in the LSB cannot make much change in the appearance of the image. This encoding protects the integrity of the information.

This technique ensures total privacy, security, confidentiality, and integrity without the complication of pixel expansion or change in the quality of the image. The end-user has the benefit of retrieving the image with less computational effort [3].

Based on this research, it can be summarized that cryptography is used in different areas of activity, used for business processes, e-Governance, financial, health care, agriculture services, used for cryptocurrency, and for the implementation of digital signatures. By examining the algorithms from the articles, it is easy to notice that cryptography uses the simplest operations and a certain number of iterations to achieve high reliability and safety.

REFERENCES

1. Research of site authors Webroot. Automating Threat Defense. Using Machine Learning to Prevent Modern Cyber-attacks. – 2016. – Text: electronic. – URL: https://webroot-cms-cdn.s3.amazonaws.com/7914/8060/9397/Machine_Learning_Introductory_WP_us.pdf (Reference date 16.10.2020).

2. James Cannady. Artificial Neural Networks for Misuse Detection. – 1998. – Text: electronic. – URL: https://www.researchgate.net/publication/

2510350_Artificial_Neural_Networks_for_Misuse_Detection (Reference date 20.11.2020).

3. Tarem Ahmed, Boris Oreshkin, Mark Coates. Machine learning approaches to network anomaly detection. – 2007. – Text: electronic. – URL: https://www.researchgate.net/publication/234801644_Machine_learning_approaches_to_network_anomaly_detection (Reference date 18.12.2020).