15. ASYMMETRIC VS. SYMMETRIC ENCRYPTION: A COMPARATIVE ANALYSIS OF DATA SECURITY METHODS

Kadushko R.A

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Ladyjenko M.V. – Senior Lecturer

The information about the two encryption methods, symmetric and asymmetric, is presented. The differences between these two algorithms are considered. Speed, safety, and other critical criteria are analysed.

With the rise of Internet utilisation across all aspects of life, safeguarding the security and privacy of information has emerged as a foremost concern. Today, encryption is a cornerstone of the digital world. It secures personal conversations on messaging platforms, safeguards business communications, and protects financial transactions. It has become an essential component of people's daily interactions. However, the landscape of encryption changed dramatically in the latter half of the 20th century when a significant cryptographic challenge was solved.

Cryptography, which works by transforming plaintext into an illegible encrypted format, has been declared the most outstanding method of ensuring data privacy. Cryptography is the technique of obfuscating or coding data, ensuring that only the person who is meant to see the information and has the key to break the code can read it. The word is a hybrid of two Greek words: "kryptós", which means hidden, and "graphein", which means to write. Literally, the word cryptography translates to hidden writing, but in reality, the practice involves the secure transmission of information. To date, cryptographic systems are divided into two major fields of study: symmetric and asymmetric cryptography.

Symmetric key encryption or symmetric encryption is a type of encryption that employs a singular secret cryptographic key for both encoding and decoding data. Such a method of encoding information has been largely used in the past decades to facilitate secret communication between governments and militaries. Nowadays, symmetric key algorithms are widely applied in various types of computer systems such as file encryption software, payment processing, and communication software to enhance data security. Symmetric encryption schemes rely on a single key that is shared between two or more users. The same key is used to encrypt and decrypt the so-called plaintext (which represents the message or piece of data that is being encoded). The process of encryption consists of running a plaintext (input) through an encryption algorithm called a cipher, which in turn generates a ciphertext (output). If the encryption scheme is strong enough, the only way for a person to read or access the information contained in the ciphertext is by using the corresponding key to decrypt it. The process of decryption is basically converting the ciphertext back to plaintext. The security of symmetric encryption systems is based on how difficult it is to randomly guess the corresponding key to brute force them. A 128-bit key, for example, would take billions of years to guess using common computer hardware. The longer the encryption key is, the harder it becomes to crack it. Keys that are 256-bits length are generally regarded as highly secure and theoretically resistant to quantum computer brute force attacks. Two of the most common symmetric encryption schemes used today are based on block and stream ciphers. Block ciphers group data into blocks of predetermined size and each block is encrypted using the corresponding key and encryption algorithm (e.g., 128-bit plaintext is encrypted into 128-bit ciphertext). On the other hand, stream ciphers do not encrypt plaintext data by blocks, but rather by 1-bit increments (1-bit plaintext is encrypted into 1-bit ciphertext at a time) [1].

Asymmetric encryption, also known as public-key encryption, operates on the principle of using two distinct keys: the public key and the private key. The public key is employed for encrypting data, while the private key is utilised for decryption. This method presents a fundamental departure from symmetric encryption, which relies on a single secret cryptographic key shared between communicating parties for both encryption and decryption processes. Asymmetric encryption offers a key advantage in facilitating secure communication without the need for a shared secret key This obviates the logistical complexities associated with securely distributing keys prior to initiating communication channels. The public key can be disseminated openly without compromising the integrity of the encryption process. Consequently, any party can access and utilise the public key without posing a security risk. The generation of these two keys is achieved through the utilisation of one-way functions, specialised mathematical functions designed to render it computationally infeasible to derive the original input from the output. Such functions leverage intricate mathematical operations such as the multiplication of large prime numbers. The security of asymmetric encryption relies on the strength of these one-way functions, which render brute force attacks computationally prohibitive for deriving the private key from the public key. Moreover, asymmetric encryption plays a crucial role in digital signatures, providing a secure method for verifying the authenticity and integrity of digital documents and messages. By combining

encryption with cryptographic hashing algorithms, digital signatures enable individuals and organisations to securely sign and authenticate electronic transactions, contracts, and communications [2].

The basic aspects of symmetric and asymmetric encryption methods are provided in Table 1 [3].

Table 1 – Main aspects of encryption methods

Symmetric	Asymmetric
One key used to encrypt and decrypt the message	Different keys for encryption and decryption
Very fast	Complex and slower
Usually uses 128 or 256 bits keys	Uses key which are at least 1000 bits long
Isn't used in digital signatures	It is used in digital signatures
Ciphertext size don't differ much from the original plaintext	Ciphertext is bigger than plaintext
Scalability is an issue	Easily scalable
Single key is shared among all participants decreasing security	Public key is shared only to message senders. Recipient stores private key secretly

Symmetric algorithms provide a fairly high level of security while at the same time allowing for messages to be encrypted and decrypted quickly. The relative simplicity of symmetric systems is also a logistical advantage, as they require less computing power than the asymmetric ones.

Another functional difference between symmetric and asymmetric encryption is related to the length of the keys, which are measured in bits and are directly related to the level of security provided by each cryptographic algorithm. While a sufficiently long key can make a brute force attack mathematically impossible, errors in implementation made by programmers often create weaknesses that open up the way for cyber attacks. In addition, the security provided by symmetric encryption can be scaled up simply by increasing key lengths. For every single bit added to the length of a symmetric key, the difficulty of cracking the encryption through a brute force attack increases exponentially.

Furthermore, while symmetric encryption offers a wide range of benefits, there is one major disadvantage associated with it: the inherent problem of transmitting the keys used to encrypt and decrypt data. When these keys are shared over an unsecured connection, they are vulnerable to being intercepted by malicious third parties. If an unauthorised user gains access to a particular symmetric key, the security of any data encrypted using that key is compromised [4].

In contrast, asymmetric encryption offers a distinct approach to secure communication by utilising two separate keys. Furthermore, the security of asymmetric encryption relies on the complexity of mathematical operations employed in key generation, rendering brute force attacks computationally prohibitive. However, asymmetric encryption tends to be computationally intensive and less efficient than symmetric encryption, particularly for large-scale data encryption.

Thanks to its relative speed, simplicity, and security, symmetric encryption is used extensively in applications ranging from securing Internet traffic to protecting data stored on cloud servers. Although it is frequently paired with asymmetric encryption in order to solve the problem of safely transferring keys, symmetric encryption schemes remain a critical component of modern computer security.

To address the limitations of both symmetric and asymmetric encryption, many web protocols adopt a hybrid approach, combining the efficiency of symmetric encryption with the secure key exchange mechanisms of asymmetric encryption. This hybrid model leverages the strengths of both encryption methods to establish secure connections while mitigating vulnerabilities associated with key transmission [5]. It should also be noted that all types of computer encryption are subject to vulnerabilities due to improper implementation. For example, weak key generation or flawed algorithm implementation can compromise the security of encrypted data. Both symmetric and asymmetric encryption play important roles in keeping sensitive information and communications systems secure in today's digitally dependent world. However, though both methods can be useful, they each have their own advantages and disadvantages and so are put to different applications.

In conclusion, as the science of cryptography continues to evolve to defend against newer and more sophisticated threats, both symmetric and asymmetric cryptographic systems will likely remain relevant to computer security. Additionally, advancements in quantum computing pose both challenges and opportunities for encryption techniques, prompting ongoing research into quantum-resistant cryptographic methods.

References:

1. Types of Encryption: Symmetric or Asymmetric? RSA or AES? [Electronic resource]. – Mode of access: https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes. *– Date of access 22.02.2024.*

2. Symmetric vs. Asymmetric Encryption: What's the Difference? [Electronic resource]. – Mode of access: https://www.trentonsystems.com/en-us/resource-hub/blog/symmetric-vs-asymmetric-encryption. – Date of access 22.02.2024.

3. Symmetric Cryptography vs Asymmetric Cryptography? [Electronic resource]. – Mode of access: https://www.baeldung.com/cs/symmetric-vs-asymmetric-cryptography. *– Date of access 22.02.2024*

4. The Ultimate Difference between Symmetric and Asymmetric Encryption [Electronic resource]. – Mode of access: https://www.nwkings.com/differentiate-symmetric-and-asymmetric-encryption - Date of access 22.02.2024.

5. Analysis and Comparison of Symmetric and Asymmetric Cryptography [Electronic resource]. - Mode of access: https://secuxtech.com/blogs/blog/symmetric-vs-asymmetric-encryption-in-cryptography. – Date of access 22.02.2024.