ISSN (Print) 2794-**7629** **Received** **18/04/2024**
ISSN (Online) 2794- **4549** Accepted 22/06/2024

FULL PAPER

Data Encryption

Prepared by

Researcher /Aouragh karim
Master of computers and Information technology
Cyber Security Management
Charisma University – UK
Aouragh.karim@yahoo.com

Abstract:

With the growing need for strong cyber security to safeguard the institutions systems and data from any incidents, whether from unintentional or deliberate cyberattacks, the methods used by institutions to improve their cyber security have changed. Our article will be devoted to one of the important data protection practices that institutions must pay great attention to data encryption

Key words: Cyber security, Enterprise systems, Data encryption

1-Introduction:

Cryptography, or encryption, has been known since 2000 BCE. Humans have used it to protect their secret messages, reaching its peak usage during wartime when battle plans and attack strategies were formulated. Most were sent as regular handwritten messages but were encrypted to prevent them from falling into enemy hands and thwarting those plans. It is noted that the first to use encryption in communication between army branches was the Pharaoh. The Chinese also used various encryption and cipher methods to send messages during wars so that if the message fell into enemy hands, it would be difficult to understand. The best method used in ancient times was the Caesar Cipher, named after Julius Caesar, one of the Roman emperors.

In our current era, the need for cryptography has become urgent due to the interconnectedness of the world through open networks. These networks are used for electronic information transfer, whether between ordinary people or between private and public organizations, whether military or civilian. Therefore, it is essential to have methods to maintain information confidentiality. As a result, significant efforts have been made worldwide to find optimal ways to exchange data without revealing it. Research in cryptography continues due to the rapid development of computers and significant advancements in networks, especially the World Wide Web and the Internet.

2-Problem Statement:

There are two types of encryption: symmetric and asymmetric. The fundamental difference between them lies in their algorithms. Symmetric encryption algorithms use one key, while asymmetric encryption uses two different but related keys. This seemingly simple difference explains the functional differences between these two encryption techniques and the methods used.

3-Hypotheses:

The main difference between symmetric and asymmetric encryption is that symmetric encryption uses one key to encrypt data, while asymmetric encryption uses two different keys: a public key to encrypt data and a private key to decrypt it.

4-Study Objectives:

1. To understand symmetric encryption.
2. To understand asymmetric encryption.
3. To identify the advantages and disadvantages of symmetric encryption.
4. To identify the advantages and disadvantages of asymmetric encryption.

5-Importance of the Study:

The theoretical importance of this study lies in maintaining the electronic transfer of information, whether between individuals or between private and public organizations, and protecting it from potential breaches, hacking, or sabotage, which can impact their strategies, future plans, and growth in their respective sectors.

6-Theoretical Framework:

6.1-Cryptography

6.1.1-Uses of Cryptography:

Cryptography originated from the need to send sensitive information between military and political figures. Messages could be encrypted to appear as random text to anyone except the intended recipient. However, original encryption techniques have now been entirely deciphered and are sometimes found in puzzle sections of newspapers. Fortunately, significant advances have been made in security, relying on precise analysis and mathematics to ensure the security of today's algorithms.

As security evolved, cryptography expanded its scope to include various security goals, such as message authentication, data integrity, and secure computing, among many others. Cryptography is foundational to modern society, underpinning countless internet applications, from HTTPS to secure text and voice communications, and even digital currencies.

6.1.2- Symmetric Encryption:

Symmetric encryption uses a single key for both data encryption and decryption. This means that the key must be shared with the person you want to communicate with, and it must remain secret. If anyone else knows the key, they can decrypt, read, or alter the data. It is akin to using a locked box with a padlock; you send it to your friend who has a copy of the key. Only you and your friend can open the box and read its contents.

Examples of symmetric encryption include:

- Data Encryption Standard (DES)
- Triple Data Encryption Algorithm (3DES)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- TLS/SSL Protocol

AES is a highly secure symmetric encryption technique that uses block ciphers of either 128, 192, or 256 bits to encrypt and decrypt data. Its effectiveness is well known, and it is commonly used to protect sensitive information in healthcare, banking, government, and other industries. Compared to other encryption techniques like DES, 3DES, and IDEA, AES is more secure. Breaking it would take billions of years, making it an ideal choice for data security.

The National Institute of Standards and Technology (NIST) no longer considers DES effective for protecting sensitive data from brute-force attacks and has fully withdrawn the

standard. Similarly, NIST is phasing out 3DES, which is more secure than DES, due to increasing security concerns. Although 3DES is still in use, it has been banned by NIST since 2023.

❖ **Advantages of Symmetric Encryption:**

- High speed in data encryption and decryption, making it suitable for large and sensitive data.
- Ease of use and implementation, requiring only one key for both parties.
- Strong reliability in protecting data from breaches and espionage.

❖ **Disadvantages of Symmetric Encryption:**

- Difficulty in distributing and storing the secret key between the sender and receiver, especially with a large number of users or sites.
- Risk of losing, stealing, or leaking the secret key, which puts data at risk.
- Lack of a mechanism to verify the identity of the sender or receiver or to ensure data integrity.
- Security is compromised if the key is hacked, lost, or stolen since anyone with the key can read or alter the encrypted data.

6.1.3-Asymmetric Encryption:

Asymmetric encryption uses two different keys for data encryption and decryption. One key is the public key, which can be shared with anyone and is used to encrypt data. The other key is the private key, which must remain secret and is used to decrypt the data. These keys are mathematically related in such a way that they complement each other. It is similar to using a locked box with a special padlock; anyone can lock the box, but only you can open it with your private key.

Examples of asymmetric encryption include:

- Rivest–Shamir–Adleman (RSA)
- Digital Signature Standard (DSS)
- Elliptic Curve Cryptography (ECC)
- Diffie-Hellman Key Exchange
- TLS/SSL Protocol

❖ **Advantages of Asymmetric Encryption:**

- Key distribution is unnecessary: The challenge of securing key distribution channels is a long-standing issue in encryption. Asymmetric encryption eliminates the need for key distribution entirely. This is achieved by exchanging necessary public keys through public key servers without compromising the security of encrypted messages since public keys cannot be used to derive private keys.
- Secure private key exchange is unnecessary: For asymmetric encryption, it is essential to keep private keys secure and accessible only to authorized entities. Using unsecured communication channels for private key exchange could lead to key compromise and decryption of sensitive information, which is why ensuring the security of encrypted messages is crucial.
- Digital signature verification: Asymmetric encryption allows senders to use their private keys to verify that the message or file indeed came from them and not from an untrusted third party.

❖ **Disadvantages of Asymmetric Encryption:**

Asymmetric encryption is slower compared to symmetric encryption due to its longer keys and more complex computations. The use of long key lengths in asymmetric encryption is necessary to make it nearly impossible to derive private keys from public keys, a task that is theoretically tied to complex mathematical problems. However, this could change in the future.

In summary, asymmetric encryption prioritizes security over speed, whereas symmetric encryption prioritizes speed over security. Although symmetric encryption is not inherently insecure, poorly managed symmetric encryption systems still pose certain information security risks that can be mitigated using the fundamentals and principles of asymmetric encryption.

7-Results:

We can conclude that both symmetric and asymmetric encryption have their pros and cons. Symmetric encryption is faster and more efficient than asymmetric encryption because it uses one key instead of two. However, symmetric encryption has more security weaknesses than asymmetric encryption because it relies on a single key for both encryption and decryption. If the key is compromised or stolen, the data becomes vulnerable. Asymmetric encryption provides more security than symmetric encryption because it uses different keys for each party. If the public key is compromised or stolen, the data remains secure. However, asymmetric encryption is slower and less efficient than symmetric encryption due to its complex calculations.

8-Conclusion:

Both symmetric and asymmetric encryption methods have their unique ways of ensuring the security of our digital communications. Symmetric encryption, with its efficiency and speed, is best suited for encrypting large amounts of data, while asymmetric encryption offers greater security. Understanding the strengths and weaknesses of each is crucial to utilizing them effectively in different security scenarios. A hybrid approach, combining the benefits of both, is commonly used to maximize efficiency and security. The best choice depends on the specific situation.

9-Recommendations:

Implementing encryption is a critical step in protecting sensitive data from unauthorized access. However, it is not enough to simply apply encryption techniques without considering best practices and potential challenges. To ensure effective encryption, organizations must carefully assess their specific needs and consider various factors from different perspectives.

10-References

[1] https://journals.asmarya.edu.ly/econ/index.php/epj/article/view/87/73

[2] Fouad, Hamza, Abd and Al-Sharifi: Science of Cryptography, publication of the College of Science at the University of Babylon, Babylon Open University Library

a. http://www.itl.nist.gov/fipspubs/

[3] https://aws.amazon.com/ar/what-is/cryptography/

[4] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cia.gov/library/abbottabad-compound/2F/2FC41064A148CBD737AF2EA1EB07DDB2_Cryptography.pdf&ved=2ahUKEwirltXTueiGAxU4hP0HHVmuBXkQFnoECCoQAQ&usg=AOvVaw1lZ3QCzC9MN1GCVGtn26R6

[5] (NIST) National Institute of Standards and Technology. FIPS-197: Advanced Encryption Standard, November 2001.

a. http://www.itl.nist.gov/fipspubs/.

[6] R. Al-Khatib: Degree Certificate Authentication using Cryptography, Digital Signature and QR Code Techniques,Journal of Hama University vol.2 No.6-2019, pp 1-18.