Exploring Symmetric and Asymmetric Cryptosystems

Name: Eduard Korotkihs K-Number: K2200500

Executive Summery

This report explores the fundamental concepts and provides an overview of cryptosystems, their types, and recommendations for securing patient records in private healthcare organisations. The report will cover symmetric and public key cyphers, including their strengths and weaknesses. In the end, recommendations will be given to private healthcare organisations.

Introduction

Cryptosystems, also known as cryptographic systems, are computer systems that use cryptography to protect information and communications between devices over a network. The cryptosystem consists of different algorithms that convert plaintext, known as data, to cypher text, which is unreadable data. The goal is not to hide information but to make it inaccessible to unauthorised people.

The simplest way to do it is to use classical cypher methods; while it's historically significant, it's easy to break them. The first one is Caesar cypher, a simple substitution cypher involving shifting each letter of the plaintext by a fixed number of positions (for example, with the shift of 3, meaning that letter 'A' becomes 'D', letter 'B' becomes 'E' and so on) (Simmons, no date). The second example is the Vigenère Cipher, a polyalphabetic substitution cypher. It works by having a keyword that determines the shift for each plaintext letter—making it more robust than Caeser Cipher. The last example is the Transposition cypher. This cypher method rearranges all the letters instead of substituting them. The letters can be written down on a grid, then read column to column or row to row, which will rearrange all the letters (Geeksforgeeks, 2024a).

The classical methods mentioned above became very insecure as technology improved. They can be easily cracked using brute force methods or by finding patterns in cipher texts. Therefore, it is important to use stronger cipher methods to protect data, which involve complex mathematical equations and logic behind them.

Symmetric Ciphers

A symmetric cypher is a cryptographic algorithm that has one key that is used for encrypting and as well as decrypting. One person will share the key between both parties to communicate securely. The Advance Encryption Standard (AES) is the most widely used symmetric cypher known for its strength and efficiency. AES is a block cypher that has a block size of 128 bits. One of the benefits of using symmetric cyphers is that it’s generally faster than using asymmetric cyphers; this makes them most suitable for encrypting high volumes of data. Another benefit is its simplicity because having one key to encrypt and decrypt is very straightforward to implement (Cooper, 2024).

However, the cryptosystems key distribution may create some challenges. If a hacker intercepts the key, the entire security of encrypted data is compromised. In addition, it has another scalability as the number of users using the communication increases, managing and distributing unique keys for each communication becomes complex.

Public Key Ciphers

Asymmetric cyphers, or public key cyphers, use two pairs of keys. The public key is used for data encryption, and the private key is used for decryption. The public key is shared with everyone who wants to communicate, and the private key is kept secret. You cannot decrypt this cypher using your public key, so it is secure.

The RSA algorithm is one of the examples of asymmetric cyphers. It is a widely used public key cryptosystem. It works by choosing two large prime numbers; the numbers must be different. For this example, our prime numbers are p = 13 and q = 17. Once we have the prime numbers, the next step is to calculate both public and private keys. Both keys consist of two numbers, and the n number is the same in both keys:

Private key: (n, d) | Public key: (n, e)

To calculate n, multiply two prime numbers (p and q). In this case, it will give the result of 221; this means that the length is 8 bits. Moreover, e and d values must be calculated. The Euler phi function is used to calculate those values.

$$phi(n) = (p - 1) \times (q - 1)$$

If n equals 221, it will return 192. Once it's done, the e value can be chosen freely, but it needs to be a coprime number. For this example, it will be 17. To check if 17 is a coprime number, the gcd function can be used.

$$\gcd\big(e, phi(n)\big) = 1$$

This function will return one if e is a coprime number. If e is 17 and n is 192, it will return 1, which means that 17 is a coprime number. The last step is calculating the d value using the extended Euclidean algorithm. Once the d value is computed, it must be checked using the following formula:

$$(d \times e)\ mod\ phi(n) = 1$$

If this formula returns one, the d value can be used for decryption, and the e value can be used for encryption. The resulting keys will be:

Private key: (221,113) | Public key: (221,17)

To encrypt, you get any number you want to encrypt, for example, 88. You need to perform 88 roots of 17 and, after applying the modulus of 221, give us the results of 121. For decrypting, you need to do 121 roots of 113, and using a modulus of 221 will provide us with the original number, 88.

However, RSA may be a secure cryptosystem. Still, it's computationally intensive, requiring a lot of resources and may decrease speed when dealing with large prime numbers and large amounts of data. This leads to another point: RSA may not be suitable for some applications requiring encrypting and decrypting large amounts of data, making it incompatible with that

application. In addition, it's vulnerable to quantum computing as it has enough power to have the ability to attack the RSA algorithm and decrypt the data.

Recommendation and Conclusion

Based on organisations' needs, a cryptosystem that combines symmetric and public key encryption is recommended. A proposed system involves AES, RSA and HMAC algorithms. AES is efficient and firmly secure; it's suitable for encrypting large amounts of data and doing actual time encryption (Cooper 2024), so private healthcare organisations can use it to encrypt patients' records. The private healthcare organisation can use the RSA key to exchange AES keys securely between parties, as it will ensure that only authorised users, such as doctors and nurses, can access the symmetric encryption key. HMAC can be combined with AES and RSA to ensure that data haven't been modified during the transmission or storage (Geeksforgeeks, 2024b).

When implementing the cryptosystem, ensure that a proper key management system has been implemented. Also, it is crucial to update the cypher algorithms and key size regularly so you can adjust to new emerging threats. In conclusion, this hybrid system provides confidentiality, integrity, scalability and performance for private healthcare organisations.

References

Bernstein, C.B. (2023) *Cryptosystems*. Available at: https://www.techtarget.com/searchsecurity/definition/cryptosystem (Accessed: 10th November).

Simmons, G.J.S. (No Date) *Substitution Cipher*. Available at: https://www.britannica.com/topic/substitution-cipher (Accessed: 10th November).

Geeksforgeeks (2024a) *Transposition Cipher Techniques in Cryptography*. Available at: https://www.geeksforgeeks.org/transposition-cipher-techniques-in-cryptography/ (Accessed: 11th November).

Cooper, V.C. (2024) *AES Encryption Explained: How It Works, Benefits, and Real-World Uses*. Available at: https://www.splashtop.com/blog/aes-encryption (Accessed: 14th November).

Geeksforgeeks (2024b) *HMAC Algorithm in Computer Network*. Available at: https://www.geeksforgeeks.org/hmac-algorithm-in-computer-network/ (Accessed: 20th November).

Scheider, J.S. (2024) *Cryptography use cases: From secure communication to data security*. Available at: https://www.ibm.com/think/topics/cryptography-use-cases (Accessed: 22nd November).