The evolution of cryptography: From mechanical systems to quantum encryption.

From the start of human's history, we have been always wanting to keep our message secret that only the sender and the receiver can have access to it. In the early days, a long time before the appearance of transistors, computers, or even electricity, we had been wanting to protect oral communication, entries to castle, message between armies and their commanders, etc. Hence, cryptography had been used by humans in the very early days of civilization. Nowadays, in this modern world, where everything is moving to digital, we communicate and share information through internet, where everyone, good people, bad people have access to, we could not be perfectly sure that the emails that we sent to our professors, colleagues, or friends are hundred percent secret and were not be read by anybody except the sender and the receiver; therefore, the need of protecting data sent over the internet is greater than ever.

Many pieces of evidence of the existence of cryptography have been discovered across the development of human civilization history. The earliest sign of ancient cryptography was found in the main chamber of the tomb of the noble man Khnumhotep II in the ancient Kingdom of Egypt around 1900 BC, the scribe used some unusual hieroglyphic symbols was found carved into the wall of the tomb. Even though the purpose of it was not to hide a message, but to make the text appears dignified. Around 100 BC, Julius Caesar was the person to use a form of encryption to transfer secret messages to his army at the front line, the algorithms used is known as Caesar Cipher. Each letter in the original message is shifted by a constant amount to create a cipher text, in this case, Caesar shifted each letter by 3, so that letter "A" became "D", letter "B" became "E", 3 letters at the end of alphabet were shifted to the beginning of the alphabet, so "X" became "A", and so on. The needs of encrypting data became greater that ever during the World War II, when army commanders wanted to convey their command to their army without being known by the enemies.

As a result, a German engineer, Arthur Scherbius invented an encryption device called the Enigma Machine, this machine was mainly used by the German forces during the second world war. The Enigma machine uses 3 more rotors, each rotor rotates at a different rate, giving the output is the cipher letter, the key is the initial setting of the rotors. Nowadays, encryption is being used not only to transfer data over the internet, but also to protect data in our bank account, phones, televisions, cars, etc. (Sidhpurwala, 2023).

Symmetric ciphering is the method of encrypting text for centuries, these ciphers were the Caesar Cipher, Vigenere Cipher, and One-Time Pad, the common approach of these cipher is all ciphers encrypt the text by a single key, and to decrypt the cipher, the receiver must have the same key used for encrypting to decrypt the text (Bock, 2021). There are 2 types of symmetric ciphers, there are stream cipher and block cipher. In stream cipher, the bit from plain text will be combined with the bit from the key, the cipher bit is created by a bitwise XOR operation between plain text bit and key bit. In block cipher, the plain text will be split into chunks, the key size is equal to the chunk size. However, in block cipher, it requires every chunk must be filled before encrypting; as a result, in case that the plain text size is smaller than chunk size, padding must be added into the chunk, which makes it inefficient. However, these two types of symmetric cipher only ensure that the message will not be read by a third-party, they do not ensure that the message was not modified, and the message was really sent by the sender (data integrity and authenticity), that is when Authenticated Encryption is used to ensure both confidentiality, integrity and authenticity. Authenticated encryption encrypts the message and then adds

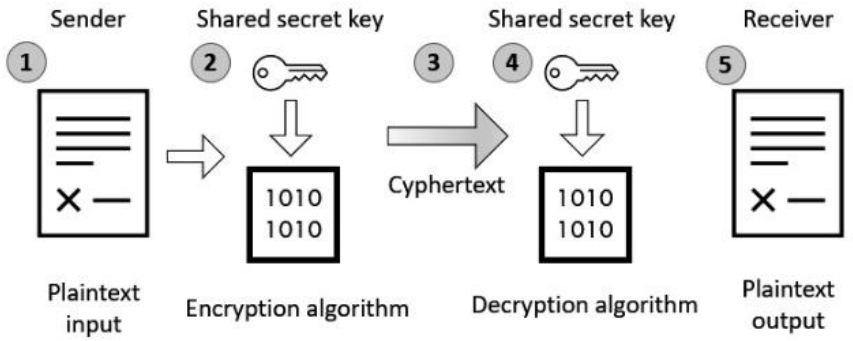

Figure 1: The process of symmetric cipher. From Bock, L., 2021.

authenticated encryption associated data (AEAD) along with the encrypted message to ensure the message has not been altered, an example of authenticate encryption is AES-GCM. (Thakur et al. 2024, pp. 29-30). There is a comparison between three symmetric algorithms between DES, AES and EB64 on nine factors, key size, block size, scalability, algorithm, encryption, decryption, power consumption, security, and key used (Logunleko et al., 2020, p. 47), but the figure 3 below is simplified to only key size, block size, algorithm, encryption, and decryption.

Factors	**DES**	**AES**	**EB64**
Key Size	56 bits	128, 192, 256 bits	Greater than or equal to 1
Block Size	64 bits	128 bits	Unlimited
Algorithm	Symmetric	Symmetric	Symmetric
Encryption	Moderate	Fast	Faster than both
Decryption	Moderate	Fast	Faster than both

Figure 2: Comparision table between DES, AES, and EB64. Adapted from Logunleko et al., 2020, p. 47. CC BY 4.0

As shown in figure 3, the AES algorithm gives the high security to encrypted messages; however, EB64 gives the fastest time in both encrypting and decrypting. However, the problem of symmetric cipher is key distribution, when only one key is used to encrypt and decrypt the message, so if a person has the key, they can decrypt the message.

Although symmetric cipher has been used for centuries, asymmetric cipher was first publicly introduced in 1976, there are 2 different keys, one is public key, the public key is shared with everyone who wants to encrypt the messages, the other key is private key, it is kept secret and

only the receiver knows the key, private key is used to decrypt the message that was encrypted by the public key. RSA is the most common asymmetric cipher algorithm, the RSA compute the public key and private key based on the mathematical fact that it is easy to multiply 2 prime numbers, but it is very hard (or impossible if the prime number is large enough) to find 2 prime numbers multiplied to get the product. The encrypted message is calculated by $c = m^e \ mod \ n$ where c is cipher text, e is public key and n is modulus, to decrypt the cipher text, $m = c^d \ mod \ n$ where d is the private key. With these formulas, people except the receiver know the public key e and modulus n, but it is very hard or impossible for them to find the private key. Another asymmetric cipher method is the Diffie-Hellman key exchange, it was developed by Whitfield Diffie and Martin Hellman in 1976. Even though Diffie-Hellman key exchange does not provide a ciphering algorithm, it allows sender and receiver agree on a shared public key without having to share their secret key (Rani & Kaur, 2017, p. 184).

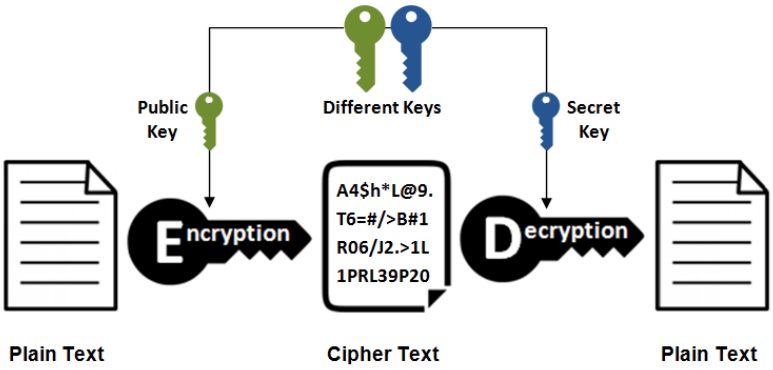

Figure 3: The process of asymmetric cipher. From Adsmurai, 2023.

After asymmetric cryptography, quantum cryptography is developed in the 1980s, there are 2 methods in quantum cryptography, the first method is Quantum Key Distribution (QKD), it was introduced by C. H. Bennett and G. Brassard in 1984. The main idea of QKD is sharing a secret key using protons, this method is not for sharing message due to the uncertainty of proton, when a slight disturb (noise) could cause change to the state of the proton, so that it is unreliable to share a large data such as message by proton, instead the sender and the receiver use protons to share a secret key, then they can use the secret key to encrypt and decrypt the message using symmetric

ciphering. However, QKD shows many disadvantages in the distance and the speed of transmission. QKD can only work with the length is below 100km, with the speed is around 100Kbit/s, due to the low speed of transmission. QKD can not be used to send the key for One-Time Pad cipher because OTP requires the key to be not smaller than the message (Li et al, 2022). Another method is Quantum Stream Cipher; it uses a common algorithm called Y-00. This method is used to transmit the entire message by a laser beam in a fiber cable, the laser beam will be transmitted in different angles, each range of angle represents for a value, and they key will tell the receiver what value that angle is representing. This method can avoid the message being altered because of the noise, because there are many protons used to transmit the message, it also offers high-speed and long-distance transmission, just like how we transmit network data worldwide through cables. However, this leads to the key distribution problem between the sender and the receiver (Sohma & Hirota, 2022, pp. 2-3).

Most of the asymmetric cryptography methods are based on the difficulty of mathematical computation to find the private key. For example, the private key is calculated by factoring very large prime numbers, with the computational performance of traditional computers, it will be very hard, or even impossible to find the private key if prime numbers are large enough. However, with the development of quantum computers with different way to process information based on the characteristics of quantum physic, it allows quantum computers to process calculations much more efficient than traditional computers (Radanliev, 2024, Review of the quantum threat, paras. 1-4; Gao et al, 2009, para. 2). This concern is a near-future possibility; therefore, the cryptography based on the difficulty of computations will be a vulnerability once powerful quantum computers are developed. To prevent from this threat, a new cryptography system to against quantum attack that is called “post-quantum” is being developed (Radanliev, 2024, Review of the quantum threat, paras. 1-4).

References

Adsmurai. (2023, July 14). How to generate secure SSH key. https://www.adsmurai.com/en/articles/how-to-generate-secure-ssh-keys

Gao, F., Wen, Q., Qin, S., & Zhu, F. (2009). Quantum asymmetric cryptography with symmetric keys. Science in China, 52(12), 1925-1931. https://doi.org/10.1007/s11433-009-0299-3

Li, Z., Kong, X., Zhang, J., Shao, L., Zhang, D., Liu, J., Wang, X., Zhu, W., & Qiu, C. (2022). Cryptography metasurface for one-time-pad encryption and massive data storage. Laser & Photonics Reviews, 16(8). https://doi.org/10.1002/lpor.202200113

Logunleko, K. B., Adeniji, O. D., & Logunleko, A. M. (2020). A comparative study of symmetric cryptography mechanism on DES and EB64 for information security. International Journal of Scientific Research in Computer Science and Engineering, 8(1), 45-51. https://ijsrcse.isroset.org/index.php/j/article/view/337

Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15(1). http://dx.doi.org.conestoga.idm.oclc.org/10.1186/s40543-024-00416-6

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*, *8*(4).

Sidhpurwala, H. (2023, January 12). A brief history of cryptography. Red Hat. https://www.redhat.com/en/blog/brief-history-cryptography

Sohma, M., & Hirota, O. (2022). Quantum Stream Cipher Based on Holevo–Yuen Theory. *Entropy (Basel, Switzerland)*, *24*(5), Article 667. https://doi.org/10.3390/e24050667

Thakur, I., Karmakar, A., Li, C., & Preneel, B. (2025). A survey on a transciphering and symmetric ciphers for homomorphic encryption. Paper 2025/093. https://eprint.iacr.org/2025/093.pdf