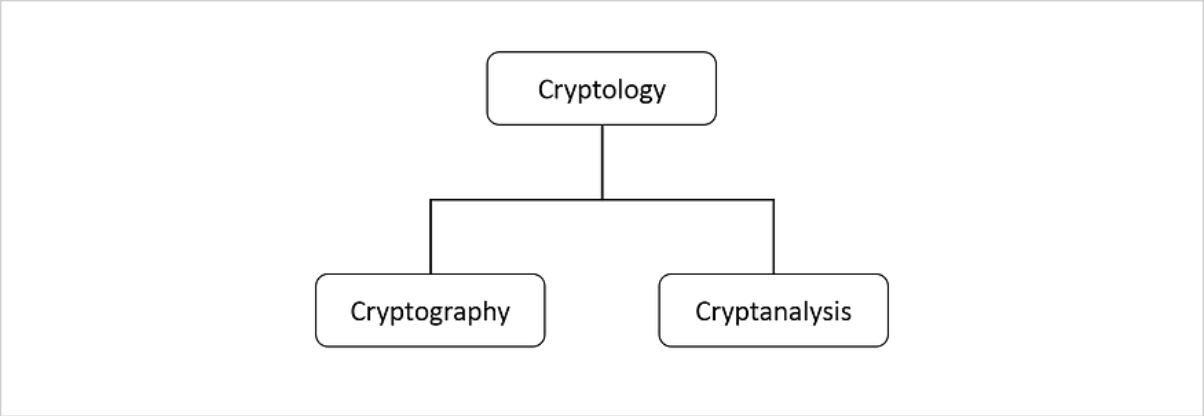
The Password War: From Classical to Modern, from Traditional to Quantum (Part 1)

Classified Information: A Key to Changing the Course of War

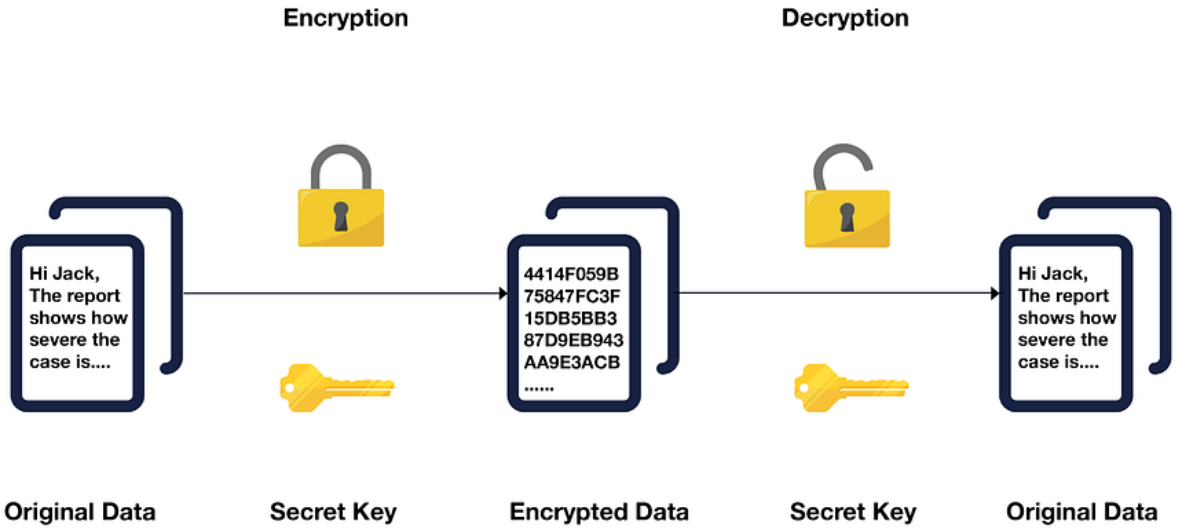
Throughout history, wars have never ceased. Emperors fought for their empires, generals for their power, and the key to victory has always been encapsulated in the classic phrase from The Art of War by Sun Tzu: “Know yourself and know your enemy, and you will never be defeated.” Knowing your enemy can lead to victory, so enemy intelligence has always been a crucial asset in warfare. Conversely, to prevent the enemy from acquiring our intelligence, it is necessary to employ methods to ensure that "the enemy does not know." To achieve this, we process the text in our intelligence before transmission, a practice known as "encryption" (encrypting). Even if the enemy intercepts it, they cannot discern its contents. On the other hand, to "know the enemy," we intercept enemy communications. If the information has been encrypted, to decode it, we must analyze the encryption method and identify flaws, a process known as "cryptanalysis" (cracking). Successfully cracking the encryption allows us to restore and interpret the message, known as "decryption" (decrypting).



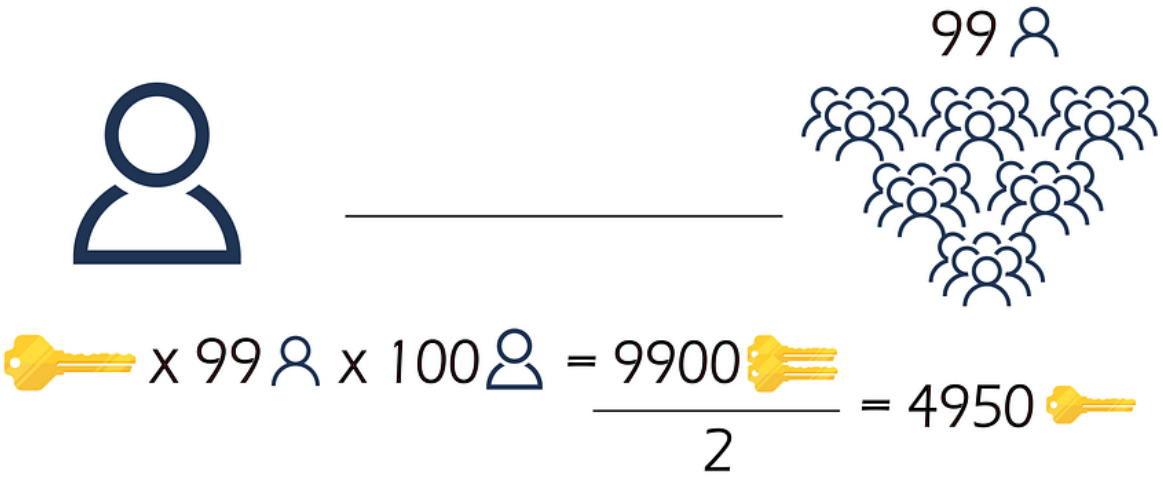
The study of encryption and decryption is referred to as "cryptography" and "cryptanalysis," respectively. In 45 BC, Roman Emperor Julius Caesar employed a simple substitution cipher to secure correspondence with his generals[1]. In the 16th century, Queen Mary I of Scotland used a substitution cipher to encrypt letters plotting the assassination of Queen Elizabeth I of England[2]. However, the encryption was eventually cracked, and the subsequent rumors led to Mary’s execution by Elizabeth[3]. In modern times, one of the most famous examples is during World War II when the Germans used the Enigma machine to encrypt their communications[4]. Even if the enemy intercepted the messages, they could not understand them[5]. British intelligence officer Alan Turing played a crucial role by developing the Turing-Welchman Bombe, a machine that analyzed the Enigma's encryption, significantly reducing decryption time and contributing to the end of the war[6].

From Classical to Modern: The Evolution of Military and Government Encryption

Technologies



In the past, ciphers like Caesar's, substitution ciphers, and Enigma required both parties to share the same "shared secret key" before transmitting messages. Only with this shared key could the messages be encrypted and decrypted. Both parties needed to manage and use the same key for encoding and decoding messages, and they could also establish methods for changing the key, such as the Germans' practice of issuing a codebook listing keys for each transmission. The major disadvantage of shared secret keys is the difficulty in key management. For example, if a group has 100 people, each person must manage 99 keys to communicate securely with others. This results in 4950 different keys to manage, whether individually or through a third party, leading to extremely high resource and management costs.



Another disadvantage is the key distribution problem. How can we ensure that a shared key is safely distributed to the intended parties? Even with a secure distribution method, why not directly send the secret message? The further apart two people are, the higher the risk of key

leakage during distribution. Due to these challenges, cryptographers have continuously sought solutions, leading to a significant breakthrough in the 1970s with the invention of the "public key cryptosystem."

The 1970s and 1980s marked a revolutionary breakthrough in cryptographic technology, opening the doors to modern cryptography[7]. Classical ciphers like Caesar's, substitution ciphers, and Enigma became part of history. How did cryptographic systems evolve from classical to modern? The next part of this article will explore public key cryptosystems and discuss the impact of future quantum computers on these systems.

Thank you for reading this article. Feel free to applaud, share, or reply. When sharing or reprinting, please credit the source: Quan'an Intelligent Technology (IKV-Tech). We will continue to unveil the mysteries of the field of cryptography and its applications in future articles. Stay tuned.

[1]: Luciano, D., & Prichett, G. (1987). Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. *The College Mathematics Journal, 18*(1), 2–17. doi:10.2307/2686311
[2]: Page of ciphers used by Mary Queen of Scots, c.1586 (SP 53/22 f.1) https://www.nationalarchives.gov.uk/education/resources/elizabeth-monarchy/ciphers-used-by-mary-queen-of-scots/
[3]: Historical Encryption: The Babington Plot https://www.thesslstore.com/blog/the-babington-plot/
[4]: Enigma — The International Museum of World War II https://museumofworldwarii.org/collection/enigma/
[5]: Enigma: Why the fight to break Nazi encryption still matters https://www.cnet.com/news/enigma-why-the-fight-to-break-nazi-encryption-still-matters/
[6]: The British Bombe — Turing-Welchman Bombe https://www.cryptomuseum.com/crypto/bombe/
[7]: Introduction to Modern Cryptography https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Introduction%20to%20Modern%20Cryptography.pdf