RSA encryption encounters quantum computer

劉東亮 201694005
張胤民 201694069
王宇晴 201694089

Before RSA: Symmetric encryption

The most widely known about symmetry encryption is the German cryptosystem "Enigma" in World War II. Each Sergeant has a password table (key). When receiving an encrypted message (Figure 1), the same password table must be used to translate the ciphertext. The enemy eavesdropper lacks a password list, and even if the signal is intercepted, the ciphertext cannot be solved. This cryptosystem was very successful, when the Germans relied on it to successfully defeat the surrounding countries through the blitz.

Asymmetric encryption

The Germans printed the password sheet on water-soluble materials and updated it once a month. If captured, the password list can be destroyed immediately. Even if the password list is really taken away, it can only be used for one month. But this is still not perfect. If there is a spy outflow password table in the group, the password system will be broken. The possible countermeasure is to have a unique password table between every two people. If there are n people in the group, the password table of a spy outflow will not affect other (n-1) people. However, in this case, the group needs a total of about n squares of the password table [Note 1], which is very inconvenient. Furthermore, to secretly communicate with a new member, how to safely pass the password list is also a big problem. In response to these challenges, asymmetric encryption has emerged.

The essence of asymmetric encryption is that encryption and decryption require different keys, public and private keys. Anyone with a public key can encrypt any message, but only the private key can unlock the ciphertext. In Figure 2, in order to send a message to the girl safely, the boy asks the girl for a public key for encryption. The girl decrypts the private message after receiving the encrypted message. If an eavesdropper intercepts the signal, he can only get the encrypted message and the public key for

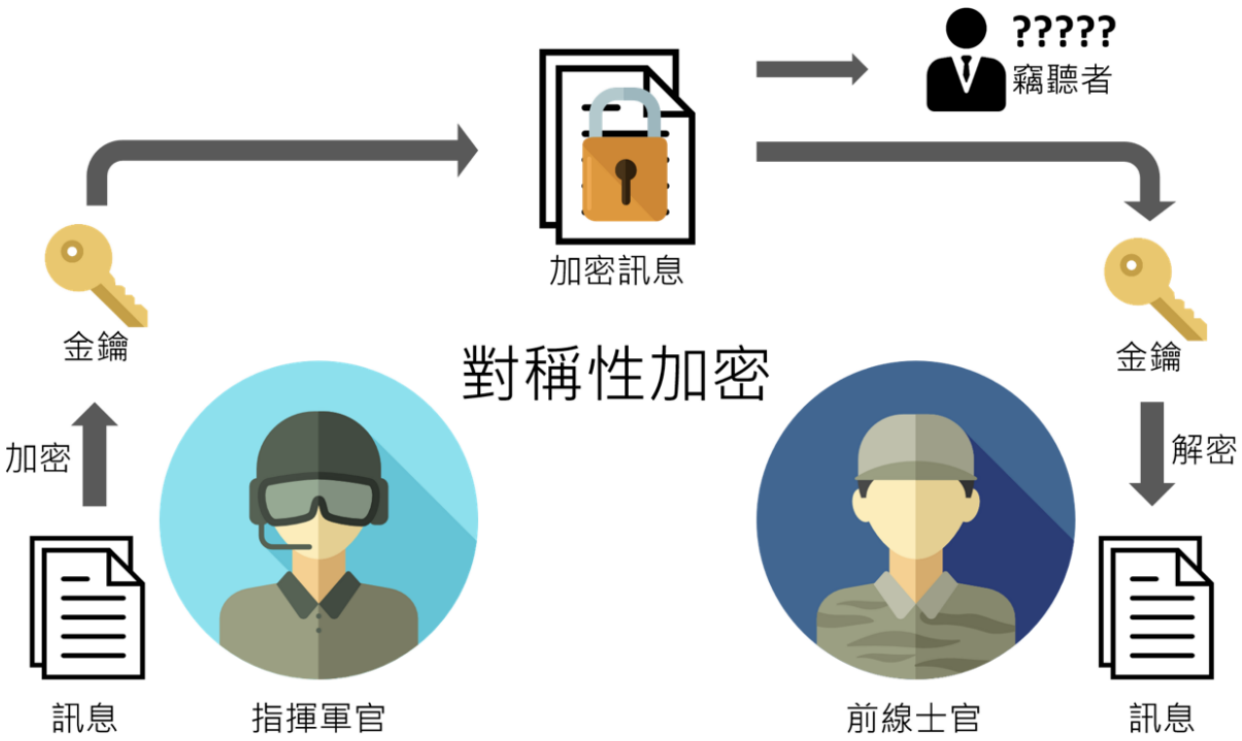

Fig 1. Schematic diagram of symmetric encryption. "Symmetric" in symmetric encryption means that the same key (password table) is used for encryption and decryption. His advantage is that the encryption process is simple and straightforward, and the security is high without the key being flowed out. But the downside is that once the key is out, the entire cryptosystem collapses. Whether it is past war or modern life, it is unrealistic to ensure that the key is never out, so the security of symmetric encryption is not really reliable.

encryption, which cannot be decrypted. It is worth mentioning that if a boy mistakenly deletes the original text of his message, he himself cannot restore the message through the public key, and his status becomes the same as that of the eavesdropper. Under such a password structure, although it takes time to obtain the public key in advance, the risk of transmitting the password table is eliminated, and the security is greatly improved.

Math and security behind the password

The most widely used asymmetric cryptography today is the RSA algorithm, whose name consists of the surnames of the inventors Ron Rivest, Adi Shamir, and Leonard Adleman. The concept is shown in Figure 3. The RSA algorithm is based on two prime numbers p and q, which make

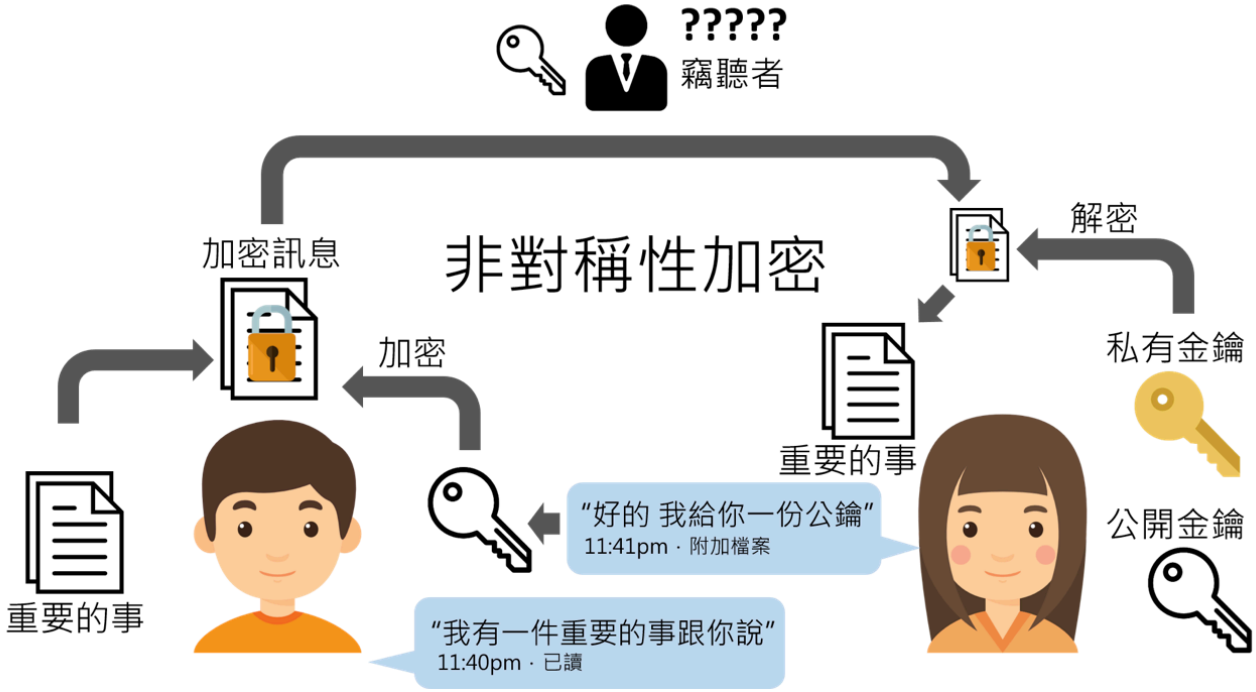

Fig 2. Schematic diagram of asymmetric encryption. "Asymmetric" refers to the use of different keys for encryption and decryption, so we can arbitrarily send public keys that can only be used for encryption. Before the boy sends a message like a girl, he must first obtain a public key. The message is a little longer, but the security is much improved. The eavesdropper can't get the private key for decryption because it never intercepts the signal, because it never exists in the communication. The only way to steal a private key is to hack into the holder's computer or home (but if he does succeed in the invasion, he simply steals the message and does not need to steal the key).

qualified public key (n, e) and private key (n, d). Encryption and decryption are to take the remainder of the message and take the remainder (mod) [Note 2]. For example, to use the public key (n=143, e=7) to encrypt the weight of "72" kilograms, the reader will get the pen (or computer) calculation will get Cipher text. When decrypting, a similar operation can be performed on the ciphertext with the private key.

For an eavesdropper who does not have a private key but wants to crack the message, his only information is the public key (n, e). One of the methods of cracking is to find the p and q for the prime factor decomposition, and then derive the private key d. But for the standard 2048-bit RSA encryption, even with the world's strongest supercomputer (Taihu Light, made in China), the time spent on Earth's age (4.6 billion years)

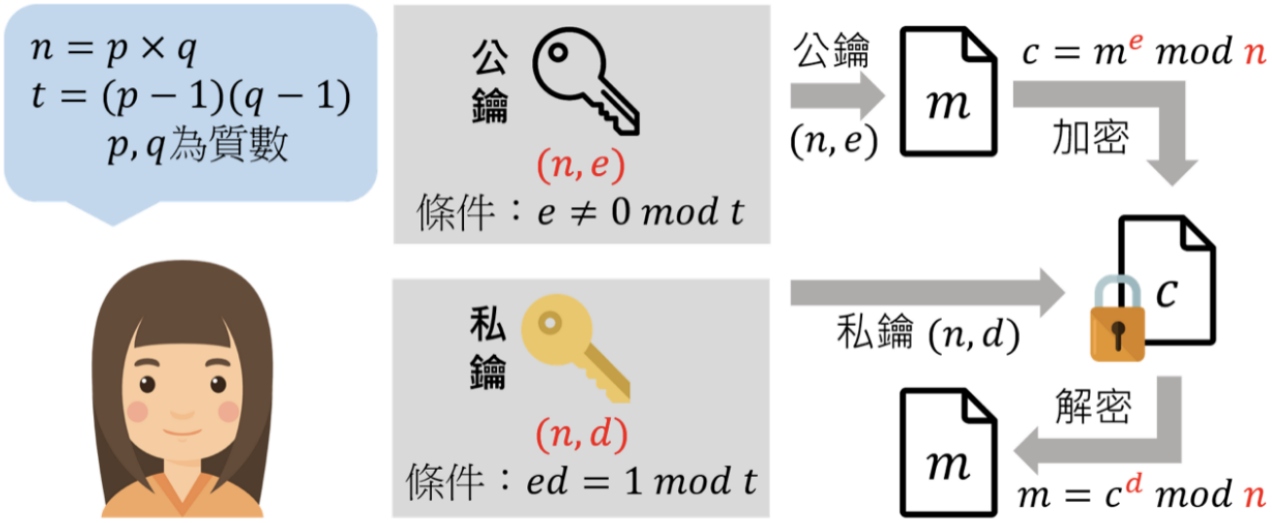

Fig 3. Behind the RSA algorithm, the public and private keys are actually two sets of numbers that match the mathematical conditions in the graph. To encrypt a message (m), you only need to do the power of the power and the remainder of the m, and decrypting a ciphertext (Ciphertext) c only needs to do similar operations, which is very convenient. In terms of security, in fact, the public key already contains enough information to crack the ciphertext, but to find the correct information needs to be calculated for a very long time, the general classical computer cannot effectively do.

cannot be cracked. The RSA algorithm is highly secure and only needs to share the public key, so it has its traces from social software to military communications. Our life can be said to be inseparable from RSA.

Quantum computer and periodicity

Quantum computers have far more computing power than classical computers for specific problems. Since quantum mechanics uses the concept of "fluctuation" to describe matter, the "cycle" of volatility is one of the fundamental properties of quantum mechanics. There is a conjugate between various physical quantities, and the physical quantities of these conjugates are like the relationship between fluctuations and cycles. For example, momentum can be thought of as a period in space, an energy like a period in time, or more abstractly, a particle number is like a period in phase.Because of these characteristics, quantum computers are particularly good at finding cycles.

In the above RSA algorithm, a core element is "remainder (mod)". This function has periodicity,

which is his advantage and his weakness. Because of its periodicity, he can be used efficiently for encryption and decryption. But if a machine can quickly find the periodicity of a function, the RSA algorithm can be easily cracked [Note 3]. Quantum computers happen to be such machines. Cracking the RSA algorithm is one of the goals of quantum computer development, and it is also one of the important reasons why academics, industry and government have invested a lot of money in research and development.

To break a set of 2048-bit RSA encryption, theoretically about 4000 qubits are needed. Currently, Google and IBM's quantum computers have about 20 qubits. Although the number is still far from enough, the two companies have doubled their numbers compared to the 9-bit and 5-digit in 2016. Whether we can use the quantum computer to revolutionize the existing cryptosystem in the future, let us continue to look at it.

Note:

[Note 1] There are n people in the group. Any two people with a unique password table need a total of n(n-1)/2, and the complexity is n square.

[Note 2] mod is the remainder. His format is "dividend = remainder mod divisor". For example, dividing 17 by 5 equals 3 or more 2 can be written as "17=2 mod 5".

[Note 3] The most well-known algorithm for cracking RSA is the "Shor's Algorithm". Readers who are interested in the details can refer to their Wikipedia entry.

Reference:

Eleni Diamanti et al., Best of both worlds, Nature Physics 13, 3–4 (2017)