Advances in Computer, Signals and Systems (2021) 5: 5-9
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2021.050202
ISSN 2371-8838

The Weakness of Traditional Cipher Technology and Quantum Cryptography's Superiority

Siyu Han

Jiangsu Tianyi High School, Wuxi, Jiangsu, China

Keywords: Quantum cryptography, Communication security

Abstract: Cryptography is the science to study ways to protect the communication security. At present, there are several ways of encryption methods, however, with the improvement of computer computing power, most of the encryption can already be cracked, though it will take much time. With the development of quantum physics, quantum cryptography has broken the limitations of traditional cryptography and it is becoming one of key directions to protect communication security in the future.

1. Introduction

In current modern society, with the rapid development of computer information technology, information exchange is becoming more frequent, there is much stricter requirement on information security. Therefore, cryptography attracts wide attention and concerns. Cryptography takes the objective law of cipher change as the research object, It consists of two parts, one is to establish cipher to keep communications secret, and another is to break the cipher to obtain communications information which is hidden behind the cipher.

2. Chapter 1 the History of Cryptography

2.1 Ancient Encryption Methods

From the creation of human society, people began to live in groups and communities, Thus, information exchange was needed among the different groups and communities. With the development of civilization, different groups and tribes started to emerge, which gradually generated different hierarchies, violence, and control in power among the groups or communities. Hiding some important information between different groups and individuals for some planning or action execution was required. Cryptography has played a mystical and important role in the long history of mankind.

Archaeological findings suggest that ancient people were already using codes to hind some information about 4,000 years ago. Around 1900 BC, the ancient Egyptians used a amended hieroglyph to hide their messages. In the 5th century BC, the Spartans in ancient Greece invented with a smart way of encrypting. They used a tape wrapped around a stick and then wrote messages on the tape. When the taps releasing from the stick, the letters on tape will become messy, and unavailable to understand its meaning, and achieve hiding the message. However, the message

recipient can rewind the tape around with a same diameter stick to show what is recorded on the tape.[2]

Long time ago, people also invented shift encryption which is relatively simple and easy to operate, Caesar cipher can be a typical representative, it was widely used in the Roman legions. The Caesar Cypher works by moving a letter three positions forward in the alphabet, for example, replacing A with D, B with E, C with F, and so on. The message recipient can decipher the message by moving the letters back with three positions.

However, as time goes by, people figure out that they can use Brute Force to find the right key. For instance, a programmer can use a programming language such as MATLAB to solve this problem[1], he can just loop all the circumstances until he find the right key. In the essay: Tonni Limbong, Parasian D.P. Silitonga used Matlab to decipher Caesar's Cypher: they use a 'for' loop and traverse every possible key.

Although ancient Greek and Roman encryption methods had contributed a lot during that history period, but it is easy to judge that they were not secure enough and to be easily cracked. Once you know how the Greeks used tape and stick, you just need to try again and again with more different diameters sticks, sooner or later, the message becomes readable. It's not difficult to crack its code. For a one-letter displacement cipher like the Caesar code, replace each letter with the letter that is three letters behind it.

2.2 Middle Age

Cryptography was further developed during the Middle Ages, and most cryptographic systems were based on transposition or substitution or combination of both. During the Renaissance, Leon Battista Albertip was an extraordinary talent. He was not only an artist, philosopher, or architect and composer, but also well-known as the "Father of Western Cryptography", since he pioneered a new technology of multi-letter substitution and open a new view for cryptography. It described a new cipher model in his manuscripts in 1467, which described a two copper plates joined together, one fixed and one rotatable, both engraved with letters, the outer plate in pure alphabetical order, and the inner plate with code replacements arranged in an irregular order, Every few words, the copper disc is rotated to alter the encryption logic, thereby improve the security.

However, people can decipher the message by finding the occur rate of the letters, since no matter how people try to encrypt one piece of English passage, the possibility of each letter to occur in the article is relative stable. In this method, the traditional encryption ways are all invalidated and is unreliable. For example, in most cases in a passage, the letter occur least is "z" and letter that occur is "e", people can directly find the most and least occur frequency letter and conclude the key.

With the technical development to 18th century, some more advanced methods have been developed to encrypt messages, such as Morse code and telegraph code. It is a kind of on and off signal code, it can express different English letters, numbers and punctuation marks through using different order. It was invented in 1837 by a controversial American named Samuel Morse or Elfield Weil. Morse code is an early form of digital communication, but unlike modern binary code, which uses only zero and one , it includes five types of code: dots, dashes, pauses between dots, short pauses between characters, medium pauses between words, and long pauses between sentences. The Morse code has played an important role in modern warfare.

2.3 Modern Encryption

In modern days, people developed two systems to encrypt messages, one is much faster but less secure -symmetric encryption, using one public key to encrypt message, the other is slower but more secure - asymmetric encryption, using one public key and one private key to establish secure

communication. [2]

2.3.1 DES

DES means Data Encryption standard, which was first introduced by the IBM[3], it is a symmetric encryption method, the message sender and the receiver shares one public key together as the figure 1.1 shown.

Fig.1 1 It is a Symmetric Encryption Method in Which the Sender and Receiver Share a Public Key

In principle, DES can ensure the security of the message if the key is longer than the message it has to encrypt. However, in reality, this type of encryption significantly reduces the efficiency of the communication. So people combined the symmetrical with the asymmetric encryption method.

However, this way to encrypt message is out of date now, since the attackers can easily Intercept the information, crack the key, eavesdrop on classified information and even change the information.

In practice, people use triple DES, which means the sender first encrypt the message then decipher it and then encrypt the message again. In this way, the information will be more secure than just encrypt the information once

2.3.2 RSA

RSA, named after the three mathematician Ron Rivest, Adi Shamir, Leonard Adleman, is another way to encrypt information in modern days, it is a asymmetrical method, the theory is largely based on two very large prime numbers, and the communication system is consisted of two types of keys, public key, which every one can access, and private key, which is kept among every personal computers.[4] . When sending the message, the sender using the public key of the receiver to encrypt the message and the receiver uses his own private key to decipher. The encryption method use nowadays use1024bit to encrypt information, which is hard for attackers to decipher using current technology. The principle is shown in the figure 1.2

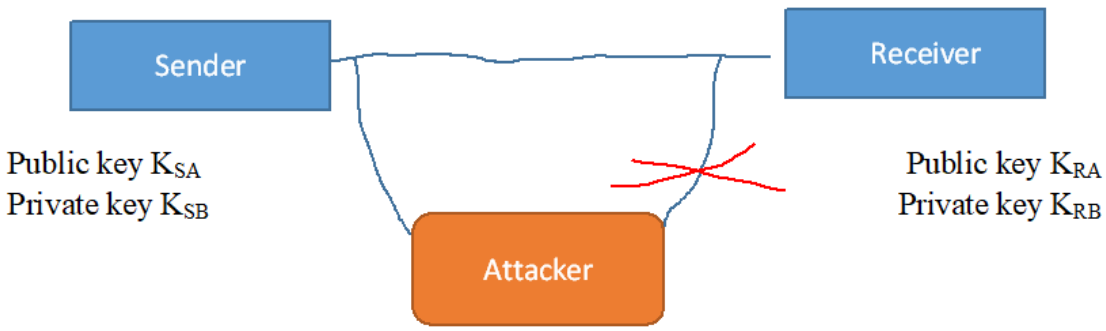

Fig.1.2 1024bit to Encrypt Information

By this way, Even the attacker knows the public key of the receiver, he can not decipher the

information

2.3.3 Digital Digest

This method cannot protect the message form being monitored by the third party, However, digital digest helps to keep the information from being changed, digital digest have a system such as MD5(MD Standards for Message Digest) and SHA(Secure Hash Algorithm)which compress the important information that extracted from the message. In the actual practice process. The website will have a qualified certificate given by SSL, and the user can compare the compressed information that they extract from the message they received with the information in the SSL certificate as the figure 1.3 shows.

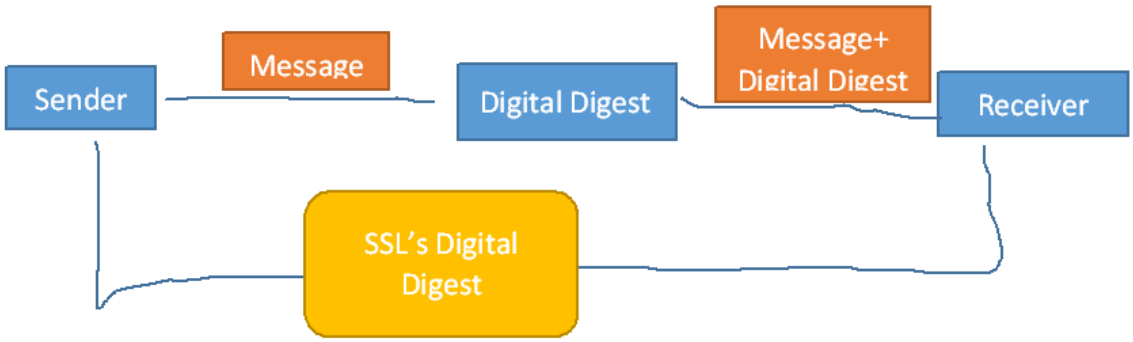

Fig.1 3 the Compressed Information Extracted from the Received Message is the Same as the Information in the Ssl Certificate

3. Chapter2 the Development of Quantum Computer and Quantum Communication

3.1 The Basic Principles of Quantum Mechanics

Quantum mechanics is different from classical mechanics because there is only one moving direction, however, in quantum mechanics, there are several possible moving direction and the possibility take effect, for the moving object will choose multiple least action paths simultaneously

3.2 The Invention of the Quantum Computers

In the late 20th century Benioff first introduced the concept of quantum computing and prototype Quantum computer. After that, physicist Feynman enhanced his theory and the system. Quantum Computing is largely based on gates that are different from traditional computers. Its basic unit is quantum-cubit. In 1998 Quantum- cubit is different from traditional cubits because these cubits can support superposition which derives several unique gates such as hardmord gate x gate. Quantum computers also support parallel computing, which greatly improves the computing performance of the computer and makes the reversible calculation feasible

3.3 Quantum Communication's Ability to Help Protect the Communication from Intercepting

Quantum mechanics has a fundamental theorem ---uncertainty theorem.Heisenberg's uncertainty principle can be applied to secure the communication because if there is a attacker that observe the message, then the message will immediately be invalidated. So it kept information from being monitored in the first place. The following graph shows one possibility of the attackers decipher

3.4 Quantum computers' Gates

Quantum computers are consisted of several different gates which can do more things than the traditional computers. For instance the Hadamard Gate Pauli-X and Y gate.

3.5 Shor's Algorithm's Impact on Modern Cryptography

Shor's Algorithm uses new Quantum techniques to solve the factor problem it threatens the traditional encryption method such as RSA, which is largely based on the difficulty to factor two large prime numbers' product, this means that the modern communication system is under threat. In RSA, the public key and the private key's product is more easy to access than accessing the private key, if the attacker use Shor's algorithm, then he can decipher the message and even change the message.

3.6 BB 84 Protocal

BB84, named after Charles Bennett and Gilles Brassard and 1984,is the first key distribution plan and the first Quantum cryptography protocol. It is proven to be completely secure. During the transmission, Alice (the message sender) will encrypt two n-long string and send to Bob(receiver), Both of the Strings are encodes as the tensor product of n-cubits.

4. Conclusion

Cryptography plays a very critical role in protecting the information security of government, financial, business and military etc.

References

[1] Limbong, T., & Silitonga, P. Testing the Classic Caesar Cipher Cryptography using of Matlab. International Journal of Engineering Research & Technology (IJERT) , no.02, pp.175-178, 2017.

[2] Donald Davies. A brief history of cryptography. Information Security Technical Report, no.02, pp.14-17, 1997.