Research on Encryption Methods and Strategies for Cryptographic Attack

Yiming Ding[1,*]

[1]*Wenzhou Kean University, Wenzhou, Zhejiang, China, 325060*
**Corresponding author. Email: wku@wku.edu.cn*

ABSTRACT
Modern cryptographic technology has made great progress with the technological innovation of computers. In the face of more powerful cryptographic methods, traditional cryptographic methods cannot continue to protect the security of passwords. Based on improving the traditional encryption method, people try to put forward a new idea of cryptography. Through the method of logical reasoning, the research mainly refers to the relevant online literature and personal ideas. The data were obtained from online literature. We can take different measures to strengthen password security.

Keywords: *Cipher, Security, Method*

1. INTRODUCTION

"All human beings have three lives: public, private, and secret" -- Gabriel Garcia Marquez, Gabriel Garcia Marquez: A Life. [1] Marquez's words put secrets in the same position as public and private, which shows the importance of keeping secrets for a person. In this complicated modern society, the competition between people is more intense, and passwords are used to protect secrets. It's like a classic Caesar code that all you must do is substitute each letter in the alphabet by shifting it right or left by a specific number of letters. [2] The versatility of passwords lies in the number of areas in which they are most used. The battlefield can change rapidly, and the disclosure of a little military information can lead to the failure of the entire military plan. The example that the BND, to eavesdrop on adversaries and allies alike while earning millions of dollars from the sales, according to the Washington Post and the German public broadcaster ZDF, based on the agencies' internal histories of the intelligence operation.[3] Passwords are used to protect the existence of military secrets. The intrigue of business as well as war, and the existence of corporate espionage, are also driving some of the biggest names in the business to use passwords to protect their trade secrets. The status of science and technology in modern society is very important, the birth of science and technology may lead to earth-shaking changes in the whole society. As representatives of world leaders and scientists, passwords help them keep scientific secrets. But having a password alone is not enough to keep these secrets. The codebreakers who followed the birth of cryptography stared at secret documents in the shadows. People need more secure passwords to replace the ones that are easy to crack.

2. FOUR MAIN PASSWORD ATTACKS

People who work as cryptographers need to know what tools the breakers use to attack. Modern cryptography divides it into four main attack modes. "Cryptanalysis can be classified into ciphertext only attack, known plaintext attack, selected plaintext attack and selected ciphertext attack according to the amount of information the analyst knows." [4]

Ciphertext only attack refers to an exhaustive attack when the breaker only knows the encrypted text (ciphertext). The translator himself knows only ciphertext.

Known plaintext attack: the breaker obtains some given plaintext and corresponding ciphertext, which in this case can be any non-empty subset. The breaker knows the ciphertext pairs.

2.1 Ciphertext only attack

Ciphertext only attacks: the breaker knows only ciphertext and nothing else, which is the most difficult analysis.

2.2 Known plaintext attack

Known plaintext attack: the breaker knows both ciphertext and plaintext and deduces the encryption algorithm and key using the known plaintext and ciphertext. The analysis difficulty is lower than that of ciphertext only attack.

2.3 Selected plaintext attack

Select plaintext attack: In addition to knowing the encryption algorithm, the breaker can select plaintext messages and know the ciphertext corresponding to the encryption, that is, know the selected plaintext and the encrypted ciphertext.

2.4 Selected ciphertext attack

Select ciphertext attack: the breaker has access to the decryption machine and can construct the plaintext corresponding to any ciphertext. Among the four password attacks, the degree of decryption is from large too small.

Select plaintext attack: the breaker can not only obtain plaintext and ciphertext pairs, but they can also select these plaintexts and ciphertext pairs, to select those plaintexts and ciphertext pairs with more features, which is easier to analyse than the known plaintext attack. Selective ciphertext attack: the breaker can construct the plaintext corresponding to any ciphertext, and its difficulty. The difficulty of defending against cryptographic attacks is from large to small: choose ciphertext attack > Known plaintext attack > Known plaintext attack >Only ciphertext attacks are used. The most difficult cryptographic attack to defend against is the selective ciphertext attack.

3. SPECIFY THE ENCRYPTION MODE AND POLICY

3.1 Traditional methods of encrypting

The longer the password, the longer the brute-force attack is going to last. And the longer the brute-force attack is required, the more time-consuming and expensive it is to match the hash and discover the password.[5] people would trust that it is safe for long cipher. However, for these four methods, the plaintext is best with random values. Because the plaintext is orderly, it is easy for the breaker to decipher the cipher directly through the plaintext or deduce the relevant cryptographic rules according to the ordered plaintext, which leads to the cipher being deciphered. Second, the key needs to be one-time. The use of a key that is used repeatedly undoubtedly provides the time and material conditions for the breaker to carry out a series of selective attacks. The one-time key is destroyed immediately, leaving the breaker nowhere to be found. In addition, ciphertext should not be easily reversed back to plain text. A password that can go back from ciphertext to plain text minimizes security. Even if the plaintext design is extremely complex, once the cipher text is mastered by the breaker, a series of passwords will be cracked by the breaker.

In these cases, a secure password requires the following features. Strong randomness: indicates that the text itself is a random number. Ordered ciphertext or plaintext can be obtained only after the key is processed. The key has random numbers. The plaintext file will be automatically destroyed as the difficulty of password length and algorithm interpreter increases (encryption program, such as a set algorithm, the key is to correctly express right, the key is to clear errors). If the interpreter directs the algorithm to crack, it is difficult for others to use the key: The key can be decrypted only after it is processed. The operation of misplaced or random numbers is added to the key type, which increases the difficulty of decrypting the key. Strong deceptively: guide the breaker to make wrong attempts and use simple decoys to deceptively lure the breaker to decipher the wrong ciphertext, such as Caesar's password, which is easy to crack. Use similar encryption methods to confuse the breaker, but it is not actually Caesar's password. A good password can also be multiple encrypted. Multiply encryptions are performed based on original encryption to ensure the reliability of encryption.

3.2 Special methods of encrypting

But some of these traditional methods are not particularly useful given the computing power of computers. Complex calculations are useless in front of a computer and can be cracked in seconds. So, people also need special encryption for computer characteristics: the key is encrypted using material that computers and humans can't easily understand. For example, the key is the meaning of the expression of the person in a picture, and a smiley face can have many emotions as a decryption attempt, such as joy, happiness, friendliness, sincerity. However, if this type of password is set as a limited number of attempts, it can effectively prevent the breaker from forcibly cracking to a certain extent. Use personal history to hint at passwords. For example, the two people use the memory of ten years ago as the relevant password. In the case of no bystander or corresponding investigation, only the relevant parties know the content of the password, and the computer cracking method of the translator cannot crack the password. Related to this, human thinking and memory are beyond the control of computers, which will make computer decoding ineffective. In addition, people can use better computers to develop passwords.

Strengthening passwords with features that only these computers have mastered can reduce or prevent cracking. In more extreme cases, passwords can be contained in pseudo-viruses or pseudo-trojans. The false alarm and false alarm of the false virus, false Trojan horse program containing the password through the computer antivirus program of the crack, will achieve the effect of breaking the computer from the root.

3.3 Normal encryption strategies

In addition to designing strong passwords, people can use a variety of strategies to protect passwords. For example, use false keys as decoys. The password user and the password breaker are usually in the light and dark position, the user in the light, the password breaker in the dark. So often the code breakers can break the code without anyone knowing. A fake key can induce the decoder to give up the advantage of secret cracking and be tricked out by the user's fake key, to know the location of the decoder or protect the security of the real key. In addition, as technology advances, people can use personal fingerprints or facial recognition technology to insure. The unique nature of fingerprints and faces makes passwords harder to crack than ones that are easy to crack. In other cases, people can come up with similar patchy passwords. That is, the original password is incomplete, and the clue of the complete password can be known only after the corresponding patch is made, thus lengthening the password cracking time and increasing the password cracking steps in the process. Or, using a seemingly obvious fake password bait is actually the real password strategy, which requires a protection mechanism that limits the number of password attempts, so as to achieve the highest protection efficiency in the limited number of attempts, and protect the password from the flaw in the mind of the breaker.

Case analysis: “NSA control over setting of international encryption standards, the use of supercomputers to break encryption with "brute force", and – the most closely guarded secret of all –a collaboration with technology companies and internet service providers themselves. Through these covert partnerships, the agencies have inserted secret vulnerabilities – known as backdoors or trapdoors – into commercial encryption software. “[6] people are faced with a situation like this, such behavior is no doubt equivalent to the company has a mole. Therefore, in this case, people can adopt monitoring management, for authorized users to monitor rights. Or spread rumors about other important information, using it to focus on the accounts of individuals or businesses who are extremely active, in order to eliminate the mole and keep the password confidential. And for the situation that can't eliminate the mole but still need to protect the password, you can spread false information about the password or make a fake program using a fake password like the real password and run the fake program using a fake password in public. So that the mole to obtain fake news or fake password, and finally let the behind-the-scenes individuals or companies lose the trust of the mole, in order to protect the real password. There is a mole for those unable to confirm whether the internal of the company, can try to spread a private news value generally, by querying other platforms, to see if the news has been leaked to other individuals or companies, to roughly confirm whether there is a mole inside the company, but specific content already belong to the content of management, ceases to explore the specific content.

3.4 special encryption strategies

The idea of special encryption strategy is mainly from perspective-taking. People can do this by hiring some professional hackers. Learn what vulnerabilities still exist in your password during the test. In extreme cases. Relevant companies can legally organize and hire some cryptographers to try to decipher the passwords of some hostile companies, and gain experience and lessons from them, to modify their own passwords accordingly. If a password can be deciphered by a cryptographer hired by a person, it is not a secure password. Because it's possible that someone else could use the same idea to crack the code. In addition, people can offer a reward for decoding their passwords (testing nature) and gather the strength of private cryptographers to find out the flaws in their passwords. It is also a good way to strengthen passwords through computer calculation and artificial intelligence. There are even some big companies that are testing out rewards that can advance the historical trend or process of improving passwords, thereby increasing the strength of all passwords at a macro level, which is a boon to all password holders.

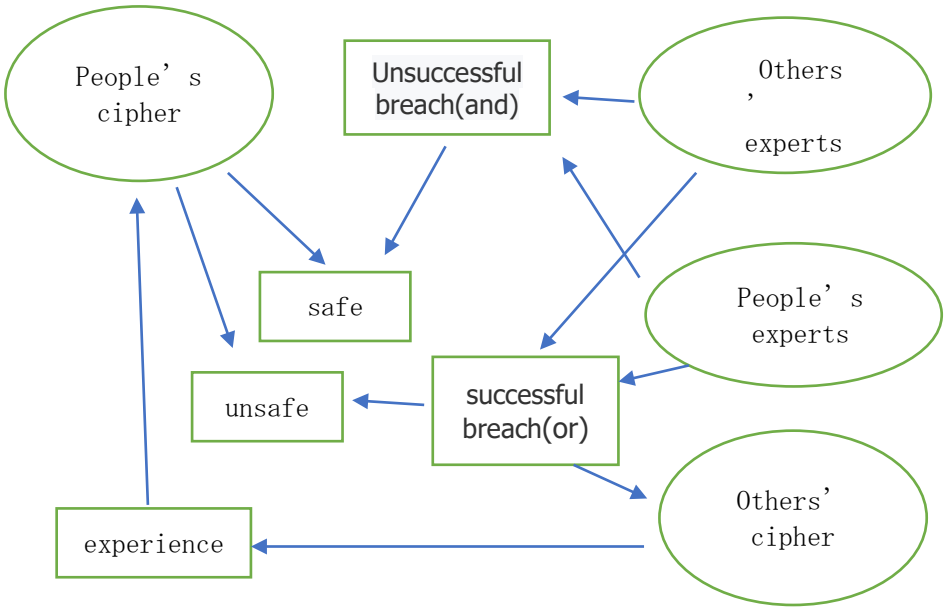

Figure1: Schematic diagram of password security process

4. CONCLUSION

People can improve password security.

Although this paper uses a lot of online literature, there are still many shortcomings in this paper. First, the personal thoughts section of this paper is limited by the cognitive bias caused by the lack of professional level. Secondly, the literature cited in this paper has uneven credibility, and there is no conclusive case on the spot. Secondly, there is no first-hand information in this paper, and most online literature focuses on timeliness. Despite the relatively new literature, password security issues are constantly evolving, and can change dramatically in just a few days. After that, the idea discussed in this paper remains purely theoretical applications, and its credibility is called into question. Finally, this paper discusses the problem of password secrecy relatively one-sided, and there is room for improvement to a certain extent. Passwords are infinitely variable. And a strong password should be so fickle that it's impossible for a codebreaker to get a handle on it. This will be our future research direction. What's more, future research can focus on computer force-cracking and the application of artificial intelligence in cryptography in the context of highly developed information technology. Keep passwords secret even if someone inside has leaked them. Encrypt passwords through personal private information. If the password is deciphered, it can automatically start a special program for data destruction, and after the destruction of private information as a password to reset the data method.

ACKNOWLEDGMENTS

This paper has received the help of Mr. Li and Mr. Huang, who have deep research in this field. In addition, I would like to thank Professor Goyal for his help and inspiration. Without their support, I couldn't finish such a paper. I'm very grateful for that.

REFERENCES

[1] Gabriel García Márquez in quotes. (2014, April 18). Retrieved from https://www.theguardian.com/books/2014/apr/18/gabriel-garcia-marquez-in-quotes

[2] Top 10 codes, keys and ciphers. (2015, September 10). Retrieved from https://www.theguardian.com/childrens-books-site/2015/sep/10/top-10-codes-keys-and-ciphers

[3] CIA controlled global encryption company for decades, says report. (2020, February 11). Retrieved from https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report

[4] Passwords and hacking: The jargon of hashing, salting and SHA-2 explained. (2016, December 15). Retrieved from https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2

[5] Plaintext Attack. (n.d.). Retrieved from https://www.sciencedirect.com/topics/computer-science/plaintext-attack#:~:text=With a known

plaintext attack, the attacker has, key, and has access to the resulting ciphertext.

[6] Revealed: How US and UK spy agencies defeat internet privacy and security. (2013, September 06). Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security