On Key Authentic Degree of Cryptosystem

WANG Yong WANG Huangdeng
(School of Computer and Control, Guilin University of Electronic Technology, Guilin 541004, China)
hellowy@126.com

Abstract： Against such attacks as rubber-hose attack, key authentic degree of cryptosystem is expatiated in detail, and the important significance of key authentic degree of cryptosystem is pointed out. And the key authentic degrees of modern cryptosystem under different conditions are given. Research shows that under most realistic situations, the key authentic degree of modern cryptosystem is high, this means that modern cryptosystem is threatened by such as rubber-hose attack and so on. Feasibility of low key authentic degree reliability is analyzed, and the implementing of low key authentic degree algorithm is studied.

Keywords: key; probability; rubber-hose; redundancy; cryptology

1. Introduction

Rubber-hose attack is a kind of attack without technique, but it is very effectual. The cryptanalysts obtain the key via threatening, extorting or afflicting the key holder until he gives it out. The kindred attack is key purchase based on bribery. These all are very effective attacks and they are often the best approaches of breaking a cipher [1]. The holder has to give the key to someone who want the key not only for being controlled, but also sometimes for fear of hurting somebody's feelings, even for being stressed by power or interests. Assume a ciphertext may have a meaning using more than one key. The wrong keys are called spurious key (pseudokey). There are mostly few spurious keys for the common modern cryptosystems, what’s more, it is difficult to find the spurious keys. According to Shannon's theories, when the lengths of the keys are fixed, the amount of the spurious keys will gradually decrease along with the increase of the ciphertext length. The modern cryptographic algorithms are all based on the fixed length keys, the amount of the spurious keys will be decreased along with the increase of the ciphertext, and the authentic plaintexts decrypted from the spurious keys may be eliminated because possibly they entirely don't correlate with the communication background at that time, so the spurious keys that can be trusted by the cryptanalysts are very few. The most modern cryptographic algorithms use bits or chars of the data as the computational unit, and after complicated computation, the spurious keys are difficult to find out even though they are existent. This means that in the condition of modern cryptographic algorithms, if a key holder randomly offers a key when facing the rubber-hose attack, obviously the cryptanalyst can easily find that the key is wrong, because the plaintext can be found to have no semantic meaning in most situations. If the key holder cannot withstand the rubber-hose attack, finally he will have to surrender and provide the real key. Because of these reasons, designing encryption algorithms whose spurious keys can be easily found out is very significative, especially in military fields. The concept of the key authentic degree was proposed in [3]. The key authentic degree of cryptosystem means the difficulty of finding out the spurious keys which we can decrypt to obtain semantic meaning plaintexts without flaws under a certain conditions. Essentially it is used to weigh the degree of the trustworthiness of the key provided by a key holder who is intimidated but not willing to leak the plaintext under the condition that the ciphertext and the algorithm are known, assuming that the key holder tries his best to provider a spurious key without flaws to misguide people who intimidate him. The key authentic degree is high if the spurious keys of the cryptographic algorithms are hard to find out. The reason why we named it as authentic degree is that when the algorithm whose spurious keys are hard to find, then a key that can decrypt the ciphertext to a meaningful text is mostly authentic. If what we get is not a real key, the plaintext decrypted from the key is mostly meaningless code. On the contrary, if the plaintext has semantic meaning, the key is the right key in most cases.

2. The significance of the research of key authentic degree

In cryptography, Kerckhoffs' law (also called Kerckhoffs' assumption or Kerckhoffs' principle) was stated by Auguste Kerckhoffs in the 19th century: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge that means all the security must lie in the choice of key. Now the protection of the keys still relies on such passive measures as encryption, multistage encryption, or even hardware protection. But there is no effective methods for the direct rob of the keys and the intimidation to the key holders. Many existent attacks under rigorous conditions are studied in the modern cryptanalysis, but there are still no precautionary measures for the rubber-hose attacks and the rob of the keys. The spurious keys of most current cryptographic algorithms are very few, moreover there is no effective method to find out spurious keys, and these increase the risks of the intimidation and interception of key. Under this situation, it is very difficult to find out a spurious key to educe a semantic meaning plaintext, therefore to a great extent we can estimate whether a key is the real key according to whether the plaintext educed from the key has semantic meaning. Namely, the key is authentic if the plaintext educed has semantic meaning. For a cryptosystem which is difficult for us to find out the spurious keys, the plaintext can be directly decrypted from the key, and then we can estimate whether the key is the real key according to whether the plaintext has semantic meaning. Hence it is necessary to establish and consummate the concept the key authentic degree of cryptosystem. We should also study the corresponding influencing factors and design a low key authentic degree cryptosystem whose spurious keys is easy to be found out.

Moreover, many modern cryptosystems or algorithms such as DES and RSA can be broken by quantum computers in very short time. With the increased speed of computers, modern cryptosystem is also threatened by high performance computer. Even under the ciphertext-only attack, because the spurious keys are very few and the semantic meaning plaintexts we obtained may be eliminated by the cryptanalyst according to background information, and then finally very few keys or one key may be at the waiting list of the right key. This also may cause the leakage of part or all of the information.

The security of modern cryptosystems relies entirely on the security of key. But in the situation that the key authentic degree is high (namely the spurious keys are very few and difficult to find out), we can exclude large numbers of keys only according to whether the plaintext decrypted from the ciphertext has semantic meaning. This influences the security of the cryptosystem. And in some situations, we can reduce the uncertainty of the key and even can directly certain the key in conjunction with other conditions. Even in the situation that the computing power is finite, the cryptanalysts also may possibly obtain the key of a semantic meaning plaintext by chance through brute force. And if luckily they find no flaws and the plaintext matches the context of the communication, to a great extent we can believe that the key is the real key.

This consideration is not hairsplitting. Modern cryptosystems have proposed complete analyses for many attacks whose precondition is hard to appear, for example the conditions of chosen message attack is that the cryptographic machine is captured and the key inside it is not destroyed, or the cryptanalysts can momentarily use the cryptographic machine. The current cryptanalysis mainly considers the situations of finite computing power. Now the computational security of the algorithms is studied in depth, not only the algorithms, but also the realization of the algorithm and other factors are considered. The analysis technologies of ciphers are unprecedentedly developed, and now there are many analysis technologies of block ciphers such as brute force attacks(including exhaustive searches attack, dictionary attack, look-up table attack and time-storage balance attack),differential cryptanalysis and its generalization, differential linearity cryptanalysis, interpolation attack, correlational key attack, multi-set attack, reflection attack, self similarity attack, energy analysis, error attack, timing attack and so on. The main attacks of stream ciphers are differential cryptanalysis, linearity consistency testing cryptanalysis, divide-and-conquer (DAC) attack, algebraic attacks, and so on[4]. The analysis methods of public key cryptosystems mainly decrease the difficulties of the intractable problems. Many of these analysis methods are put in practice under conditions of small probability (such as the interceptions of cryptographic machine, the cryptanalysis is near to the cryptographic machine and so on), and these researches are very intensive. But in our consideration, if cryptanalysts get enough ciphertext and know the cipher algorithm, the wrong key can be excluded by redundancy, but these two preconditions generally are necessary to the modern cryptanalysis, because according to Kerckhoff's assumption, the encryption algorithms may be public, and the ciphertext is indispensable for the cryptanalysis.

3. The key authentic degree of modern cryptosystem under different conditions

In 1949, C.E.Shannon published "Communication Theory of Secrecy Systems"[2], and it transformed cryptography from an art to a science. Shannon's paper introduced the information theory into cryptography, and from the view of statistics to make a mathematical description and a quantitative analysis for the information source, the cipher and others. Shannon made a very penetrating analysis and research of the problem of spurious keys. He defined the spurious key (pseudokey), ideal secrecy, the unicity distance and the perfect security according to the information theory and redundancy. But most cryptosystems cannot approach ideal secrecy, the number of spurious keys (except the right key) will finally reduce to 0 along with the increase of the length of the ciphertext, and this will intimidates the security of cryptosystems. Shannon studied on the cryptanalysis under the conditions of ciphertext only attack, he pointed out that the number of spurious keys will gradually reduce along with the increase of the length of the ciphertext. Although the above analysis of Shannon is of great value, but cryptanalysts seldom do research from this aspect.

The measurements of the key authentic degree of cryptosystems can also refer to Shannon's theories. But in reality the measure of the key authentic degree of cryptosystems will differ because of the restriction of conditions and background information. We define the key authentic degree of cryptosystem as the probability of the correctness of key that the key holder gave cryptanalyst under the restriction of conditions although the key holder tries his best to find out a wrong spurious key. We think the cryptanalyst estimate whether the key is reliable according to whether the plaintext has semantic meaning and whether there are flaws in the plaintext, if there are any flaws in the plaintext or the plaintext has no semantic meaning, the cryptanalyst will continually intimidate the key holder into surrendering the real key, so finally the key holder either surrender the real key or surrender a spurious key without flaws.

We will discuss the following situations:

Firstly, when a cryptanalyst knows nothing about the content of communication and the communication background, and he have infinite computing power, and that the key holder has infinite computing power to use, the key authentic degree is closely related to the redundancy of encoding. When the number of spurious keys is 0, if ciphertext may have a meaning using a key, then the probability that the key is the right key is 1, so key authentic degree will be 1 at that condition.

When the length of ciphertext greatly exceeds the unicity distance of some kind of encoding of the corresponding language, statistically there is no spurious key, then the key holder has to surrender the real key and the key authentic degree will be 1. It is easy to obtain the corresponding length ciphertext in reality. For example, for a message with a 56 bit key and represented with ASCII characters, the unicity distance of DES are about 8.2 ASCII characters(about 66 bits)[5]. For the ciphertext less than the unicity distance, it was pointed out that the approximate number of spurious keys N should be averagely $2^{H(k)-nD}$-1 according to the corresponding redundancy of language[6,7]. We have pointed out that N would averagely be between $2^{H(k)-nD}$-1 and $2^{H(k)-nD}$, as the right key will exist for ever and its existence is almost not affected by the redundancy of language. In most cases, N would averagely be more near $2^{H(k)-nD}$. Here D is redundancy rate of language, H(k) is the entropy of cryptosystem, generally amounts to the length of the key. If N is equal or greater than 1, on average we can find out a right key and a spurious key at least. And then because of the infinite computing power, the key holder can figure out all the keys which can be used to obtain semantic meaning plaintexts. The key holder can rationally give a spurious key to the cryptanalyst. When there is a spurious key without flaw, the key authentic degree will be 0. What we discuss is an ideal situation, in reality the semantic meaning plaintext is also restricted by the background information and other conditions. Sometimes because of inconsistent factors or antilogy, the spurious key can be found out to have flaws and be excluded. Sometimes a meaningful plaintext is totally unrelated to the background information, the corresponding spurious key will be excluded, so the spurious key without flaw would be very few. In most cases, there is no spurious key without flaw and the key authentic degree will be 1. In fact the cryptanalysts are impossible to have infinite computing power, and they also impossibly allow the key holder to compute spurious key for a long time. Therefore the situation that the key authentic degree is 0 is purely ideal.

Secondly, considering practical conditions, for example the cryptanalysts generally know something about the communication, and the computing power is finite, and the key holder can beforehand figure out a spurious key to prevent being intimidated, under such conditions, the key authentic degree is related to the redundancy of the language encoding, the length of the ciphertext, the computational time, the number of the keys, the context of the communication and the complexity of the algorithm. Theoretically speaking, the spurious keys without flaws and match the communication context are few. There are two situations: 1)If the number of spurious keys which match the conditions is 0,and there is only one right key, well then the key authentic degree is 1,because the cryptanalyst cannot found out any flaws only when the key holder surrender the key. Because of finite computing power, the cryptanalysts may cannot decrypt and test the keys one by one to find out all the spurious keys and the real keys, then they can preliminarily estimate whether the number of spurious keys is 0 according to the unicity distance and the amount of background information, under these situations the key authentic degree is higher if the background information is more and the key authentic degree approximates 1. 2) If there are more than one spurious key without flaws and match the communication background, we need to estimate whether the key holder can find out effective spurious keys according to the computing power which the key holder can user. If the probability of finding out effective spurious keys is r, the key authentic degree is 1-r. Modern cryptosystem such as AES is designed based on many rounds of complex operations on the data, the design criteria of modern cryptosystem can ensure that the cryptosystem is secure under known plaintext attack and chosen plaintext attack, so it is computational infeasible to get keys for given plaintext-ciphertext pairs. If the key holder design a ‘plaintext’ to mislead the cryptanalysts, it is hard to get the corresponding spurious key even if the spurious key is existent. Therefore under these conditions, the key authentic degree is mostly 1.

Thirdly, if we cannot compute in reality, as long as the length of the ciphertext is not very short, all the key authentic degrees of general modern cryptosystems approximate 1. It is very difficult for almost all of modern cryptosystems to find out the spurious keys because of the complicated operations. So if the key holder doesn’t prepare a spurious key beforehand, once he is controlled under duress and the cryptanalyst don't allow the holder to compute, the key holder will have to surrender the real key.

According to the above analyses, we can find that for modern cryptosystems, if other conditions are the same, the more powerful the computing power, the more possible the spurious key is to be found out and the lower the key authentic degree. And the more background information the cryptanalyst holds, the higher the key authentic degree, even though the key holder cheats, it is easier to be found out and he will continue to be grilled. The longer the ciphertext is held, the higher the key authentic degree, and as long as the unicity distance is exceeded, then the key authentic degree will approximate or be 1. In fact the unicity distances of most modern cryptosystems are very short. For example, for 256-bit-key block cipher algorithm, the unicity distance of ASCII text encryption algorithm is only 37.6 characters, obviously it is easy to obtain the ciphertext with more than 37.6 characters, and because of the finite computing power, the restriction of background information and so on, the key authentic degree of modern cryptosystem under most conditions approximates 1. Thus it can be seen, for modern cryptosystems, the key authentic degree generally reaches the upper limit 1, and this brings very great hidden theat.

4. The feasibility analysis of algorithm with low key authentic degree

The above researches indicate that the key authentic degree of modern cryptosystem is very high. But whether it really cannot be lowered? In fact it is possible. As is mentioned above, the approximate number of spurious keys N should be gained by

$$N=2^{H(k)-nD}-1$$

From this formula we can know that if we want to increase the number of spurious keys, H(k) must increases with the increase of n, which means the length of the key will increase. One-time system in classical cryptography is such a cryptosystem. In one-time system, if we casually give a plaintext with a same length as the ciphertext (the real plaintext), then we can get a corresponding spurious key according to the XOR operation of the plaintext and the ciphertext. The question in one-time system is that the key and the ciphertext are of the same length, and the increase of the length of keys is mostly unpractical, unless QKD (Quantum Key Distribution) is used.

Whether there are any other methods to reduce the key authentic degree? The lack of spurious keys is because of the redundancy of languages, and we can reduce redundancies by many ways, for example, data compression can reduces data redundancies and increases the number of spurious keys, but modern cryptography cannot provide effective methods to find out spurious keys. Furthermore we can anew encode all possible messages, for example, we can sequentially encode all the messages with a fixed length binary number, but the workload of encoding is heavy and it is very unpractical.

The redundancy of languages has to do with lingual characteristics such as grammar, so we hopefully realize low key authentic degree algorithms from this aspect. Tremendous developments of modern natural language processing are also helpful for corresponding encryptions and decryptions. But because of the complexity of natural language, some measures should be taken to ensure reliable decryption of ciphertext.

We designed a cryptosystem with low key authentic degree via an extension method like multiple-choice. The cryptosystem with low key authentic degree can effectively solve the above problems, and the plaintext obtained from the spurious key entirely accords with the communication background. These plaintexts we obtain perhaps are opposite or similar to primary meanings, and such spurious keys are easier to believe compared with general spurious keys. Because of the need of low key authentic degree, our algorithm is comparatively complex and the encryption progress is also more complex than traditional encryption. When encrypting with our method, we fill in the keywords in original texts, for example, for "sunny", we can append "cloudy", "rainy" and so on to extend, and mark them according to the key to ensure the recovery. The original right plaintext is "Today is Sunday ", but the ciphertext may be decrypted as "Tomorrow is Monday" using a wrong key, and this will misguide the cryptanalysts. This kind of algorithms has limitations, and they can be used in conjunction with traditional cryptosystems.

5. Conclusions

In this paper, we expatiated on the origin and concepts of the key authentic degree of cryptosystem, pointed out the significance of the research of key authentic degree, analyzed the key authentic degree under different conditions in modern cryptosystems, and pointed out that the key authentic degree is high in most practical situations, this means that the modern cryptosystems can be intimidated by rubber-hose attacks. We also analyzed the feasibility of the cryptosystems with low key authentic degree, and illustrated it with several examples. The cryptosystems with low key authentic degree are not only used when one is intimidating, but also can be used to mislead the cryptanalysts or attackers, and we can consciously use spurious keys to misguide the cryptanalysts who attempt to obtain sensitive messages. Of course the similar algorithms are not only used for encryption but also can be effectively applied in special situations such as steganographic method and so on. As a new research field, more cryptosystems of low authentic degree and more applications remain to be found out, and the limitations of these algorithms also remain to be found out and improved.

ACKNOWLEDGMENT

This research was supported by Guangxi Natural Science Foundation (0640171).

References

[1]. Bruce Schneier，Applied Cryptography Second Edition: protocols, algorithms, and source code in C，John Wiley &Sons, Inc，1996

[2]. C.E. Shannon, Communication theory of secrecy systems, Bell System Technical journal, v.28, n.4, 1949, 656-715.

[3]. Yong Wang，Study of Some Problems of Quantum Cryptography and Theoretical Security of Cryptosystem [D]，Southwest Jiaotong University，2005(in Chinese)

[4]. Dengguo Feng. Cryptanalysis. Beijing: Tsinghua University Publishing House, 2000(in Chinese)

[5]. C. A. Deavours. Unicity points In cryptanalysis," Cryptologta v.1, n.1, 1977, 46-68

[6]. M. E. Hellman, An extension of the Shannon theory approach to cryptography, Information Theory, IEEE Transactions on, May 1977, Volume: 23, Issue: 3: 289- 294

[7]. Beauchemin P, Brassard G A, Generalization of Hellman s extension to Shannon s approach to cryptography , Journal of Cryptology; 1988