International Journal of Advanced Education and Research
ISSN: 2455-5746, Impact Factor: RJIF 5.34
www.newresearchjournal.com/education
Volume 1; Issue 5; May 2016; Page No. 55-58

Role of cryptanalysis

Priya Arora

Assistant Professor, Department of Mathematics, S.D. (P.G) College, Panipat, Haryana, India

Abstract
In Mathematical Science Group Based Cryptography and other forms of cryptography are present. In this paper, we discuss the insecurity factors of various schemes on which cryptographic systems are built. Various attacks are discussed which can be made on these systems.

Keywords: cryptanalysis, mathematical science, cryptosystems

1. Introduction

Cryptanalysis is a broad concept that refers to the study of ciphers, ciphertext or cryptosystems i.e to secret code systems with a view to tracing weakness in them that will permit getting of the plaintext or original message from the ciphertext without having the knowledge of the key or algorithm. This concept is known as breaking the cipher, ciphertext or cryptosystem. An approach related to cryptography is cryptanalysis. The cryptographer's goal is to provide security for information by developing strong cryptosystems, while the cryptanalyst's goal is to discover weakness or flaws in cryptosystems and the break the security provided by those systems. In fact, a good cryptanalyst can even determine plaintext from samples of ciphertext without even knowing the cipher that was used to produce it. When properly implemented, standard cryptography based security technologies can provide lot of protection against a wide range of attacks, including common cryptanalyst attacks. Cryptosystems come in 3 kinds:

1. Those that have been broken (most).
2. Those that have not yet been analyzed (because they are new and not yet widely used.
3. Those that have been analyzed but not broken. (RSA, Discrete log cryptosystems.

There are three most common ways to turn cipher text into plaintext:

1. Steal/purchase/bribe to get key
2. Exploit sloppy implementation/protocol problems (hacking/cracking). Examples are some- one used spouse's name as key, someone sent key along with message
3. Cryptanalysis

2. Types of Cryptanalysis

To study the cryptanalysis it can be broadly classified into the following three categories

2.1 Cipher text only attack

The enemy has intercepted cipher text but has no matching plain-text. You typically assume that the enemy has access to the cipher text. Two situations:

a) The enemy is aware of the nature of the cryptosystem, but does not have the key. True with most cryptosystems used in U.S. businesses.
b) The enemy is not aware of the nature of the cryptosystem. The proper users should neverassume that this situation will last very long. The Skipjack algorithm on the Clipper Chipis classified, for example. Often the nature of a military cryptosystem is kept secret as longas possible. RSA has tried to keep the nature of a few of its cryptosystems secret, but they were published on Cipher punks.

2.2 Known plaintext attack (KPA)

In the KPA System it has been assumed that the enemy has some matched cipher text/plaintext pairs. The enemy may well have more cipher text also. The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books. Here the basic concept behind a crib is that cryptologists were looking at incomprehensible ciphertext, but if they had a clue about some word or phrase that might be expected to be in the ciphertext, they would have a "wedge," a test to break into it. If their otherwise random attacks on the cipher managed to sometimes produce those words or phrases, they would know they might be on the right track. Under such circumstances when those words or phrases appeared, they would feed the settings they had used to reveal them back into the whole encrypted message to good effect. Modern ciphers such as Advanced Encryption Standard are not currently known to be susceptible to known-plaintext attacks.

The older versions of the zip format specification have chances of this attack by using PKZIP stream cipher. Consider an example, an attacker with an encrypted ZIP file needs only one unencrypted file from the archive which forms the "known-plaintext". After that there are some publicly available software by using them they can quickly calculate the key required to decrypt the entire archive. To obtain this unencrypted file the attacker could search the website for a suitable file, find it from another archive they can open, or manually try to reconstruct a plaintext file armed with the knowledge of the filename from the encrypted archive. However, the attack does not work on AES-encrypted zip files.

2.3 Chosen plaintext attack (CPA)

The CPA model, appears to be an unrealistic model at first instance because it is unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. However, modern cryptography is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and so attackers can encrypt any plaintext they choose. Here we assume that the enemy can choose the plaintext that he wants put through the cryptosystem. Though this is, in general, unrealistic, such attacks are of theoretic interest because if enough plaintext is known, then chosen plaintext attack techniques may be useable. However this is an issue with smart cards.

The various forms of CPA are as follows

- **Batch chosen-plaintext attack**, where the cryptanalyst chooses all of the plaintexts before seeing any of the corresponding ciphertexts. This is often the meaning of an unqualified use of "chosen-plaintext attack".
- **Adaptive chosen-plaintext attack** (CPA2), where the cryptanalyst can request the ciphertexts of additional plaintexts after seeing the ciphertexts for some plaintexts.

CPA Relation to other attacks

A CPA is more powerful than known-plaintext attack (KPA), because the attacker can obtain many pairs of plaintexts and ciphertexts, instead of only one pair, and therefore has more data for cryptanalysis. Therefore, any cipher that prevents chosen-plaintext attacks is also secure against known-plaintext and ciphertext-only attacks. However, a chosen-plaintext attack is less powerful than a chosen-ciphertext attack, where the attacker can obtain the plaintexts of arbitrary ciphertexts. A CCA-attacker can sometimes break a CPA-secure system.

3. Insecurity of Group based schemes

Now, we briefly outline some techniques that have been developed to demonstrate the insecurity of group-based schemes.

3.1 Differential Cryptanalysis

In the year of 1990 Biham and Shamir developed the concept of Differential Cryptanalysis. The basic concept or idea behind the Differential Cryptanalysis is to compare the differences exist between ciphertext and plaintext. The basic purpose is to get the value of the Key. It can be found out with the help of XOR operation that is also used in the digital electronics. The first concept in this regard was introduced known as Differential Cryptanalysis for three rounds. For example assume that we have input XOR equal to 1011 and we are waiting for the output of XOR equal to 100. Then we can run through the input pair (1011,0000), (1010,0001)... each of which has XOR equal to 1011 and look at the output XORs. In the same way differential Cryptanalysis can be used for four round also. Assume that we have to access a four round device. Everything is known about the internal workings of the algorithm but the key is not known.

3.2 Braid based Key Exchange

The encryption scheme generally used in the cryptography uses the braid based key exchange scheme. To describe the braid based key exchange protocol assume that A;B be two commuting subgroups of the braid group Bn. In the protocol g 2 Bn is assumed to be public. The equation comes to be Kab=gba Kab=gab. Initially when it was presented it appears to produce the weak keys. In other words the group element gab could be efficiently distinguished from a random conjugate of g the output key should rather be defined by means of an ideal hash function. The main issue with braid based key exchange protocol is conjugacy problem in which it has to be find out whether two braids or in other way we can say that two elements of the braid group are conjugate or not. First of all to solve the conjugacy problem Garside given an algorithm. The main problem arises by the algorithm given by Garside is regarding its efficiency that algorithm will represent during its implementation. Ko-et al also described an efficient algorithm to solve the problem with great accuracy. This algorithm is the common basis for all existing braid-based signatures. The basic reason behind it is that the verification algorithm need to determine whether two given braids are conjugate or not. Although some other algorithms related to braid based key exchange were are also proposed but none of them has been proven implementable with a polynomial time complexity. At present we can say that up to this time Gebhard algorithm which was proposed in 2005 and published, is the most efficient method for solving the problem related to braid groups. This algorithm has not yet been proven implementable with polynomial time. If at any time someone is interested to break a braid-based cryptosystem for the purposes of cryptography, then he need not require to efficiently solve the conjugacy problem. He is free to use the specifics of the protocol being employed. Under such circumstances even heuristic algorithms are also useful and may work properly.

3.3 Length-based attacks

Length based attack generally known as LBA based on the concept of Anshel-Anshel Goldfeld commutator key exchange protocol was initially proposed by Tannenbaus and Hughes. In this algorithm attempts has been made through the heuristic search procedure to find the A's private key with reference to B. No one can say that all the successful experiments has been performed of the Length based attack and hence what will be the real threat that is not evaluated at all. On the basis of these facts one can say that Anshel-Anshel-Goldfeld protocol is invulnerable to length based attack. Now it is common faith that successful attacks on Anshel-anshel-Goldfeld were proposed. But it is common believe now that AAG with original parameters is not secure. However the scaleability of attacks has not been completely realized. This leads to speculations that AAG protocol may still be secure with a different set of parameters such as longer private keys. On the other hand Length based attack can be modified so it breaks AAG protocol with a very high rate of success. Length based Attack and Braid Groups information is necessary for AAG protocol to be immune to the length based attack. Therefore, we say that security of AAG protocol is partially based. Even in the Braid Group there are various length function available for such type of attack. Length based attack are of various categories such as

Summit set attack where as this method starts by reducing conjugate to the minimum level. Linear attack which uses presentation of braids. Hofheinz attack where as the heuristic is used to get the solution in the minimum level.

3.4 Attacks based on Linear Algebra

Linear cryptananlysis is a general form of cryptanalysis. It is based on the concept of approximations to the action of cipher. Various types of attacks have been developed. These attacks can be implemented on block ciphers and stream ciphers. Out of these two attacks, the linear cryptanalysis is widely used attack on block ciphers. Time to time a number of efforsts has been made for the refinements, including multiples linear approximations. Now the question arises how the linear cryptanalysis is performed. It is performed in two phases. In the first phase linear equation is constructed with reference to plaintext, ciphertext and key bits. The second phase is to use these constructed linear equations in conjuctions with known plaintext-ciphertext pairs to get the key bits. While constructing the linear equation binary variables 0 and 1 are used and the operation XOR is carried out. On the other hand the method for developing approximation is carried out. The approximation method is different for each cipher. To solve the conjugacy search problem a linear representation of the braid group is taken and solution is reached by using linear algebra in a matrix group.

4. Key exchange scheme based on stickel

Key exchange scheme in cryptanalysis idea was proposed by Stickel popularly known as Stickel's key exchange scheme. Basically Stickel's protocol is based on the well known Hellman protocol. The choice of base used by Stickel's while using the Key exchange scheme makes the protocol vulnerable to linear algebra attacks. While doing so, the major problem arises in front of Stickel to find out the secret key. To solve any discrete logarithm type problem instead can solve the decomposition search problem. Stickel's protocol can be designed with improved performance as – Assume G b e public non-abelian group, a;b 2 g public elements such that ab=ba. The key exchange protocol runs as follows. Assume that N and M be the orders of a and b, respectively.

1) A picks two random natural numbers n<N, m<M sends u=arbm to A
2) B picks two random natural numbers r<N, s<M and sends v=arbs to A
3) A Computes KA=anvbm=an+bm+s
4) B computes KB=arubs=an+bm+s

Thus A and B end up with the same group element K=KA=KB which can serve the shared secret key. When it comes to implementation details, exposition in becomes somewhat foggy. It is in the general practice that author actually prefers the following general version of the above protocol. Assume that w 2G be a public then the above protocol in the modified form can be presented as follows:

1) First of all A chooses two random natural number n<N, m<M, as well as one of the element c1 from the center of the group G and transfer u=c1anwbm to B.
2) B pick up two random number such that r<N, s<M, as well as an element c2 from the center of the group G, and transfer v=c2arwbs to A
3) A computes KA=c1anvbm=c1c2an+rwbm+s
4) Finally B calculate KB=c2arubs=c1c2an+rwbm+s

On the basis of the above facts A and B ends with the same group element K=Ka=KB. There are several key exchange protocols that directly uses the alleged hardness of the decomposition search problem in various groups. Up to now no particular group has been recognized as providing a secure platform for any of these protocols. On the other hand we can say that matrics semigroups can generally make good platforms too.

5. Logarithmic signatures

There are various schemes of logarithmic signatures, but in these schemes, the signature is at least as long as the message. Of course it apparent a major weakness. The situation appears to be worst in the case when the message is long. To find the solution, a hash function is used. After it the signature scheme is put up to the hash message not on the message itself. Under the present circumstances, the hash function h is made public. Starting with a message m, A computes the hash h (m). This output h (m) is of course smaller and appears to the solution of the problem prescribed above. The main advantages of it is that it is faster to create and also the requirement of resources is also less. Now the question arises whether this method for signature is secure or not. Assume that A has signed a document electronically by using one of the signature schemes to sign the hash of the document. Here assume that the hash function produces an output of 40 bits. Although there is a fear regarding signing an additional contract but still it is safe because the chance of fraudulent contract having the same hash as the correct document is 1 out of 2 raise to power 50 which is approximately 1 out of 10 raise to power 15. Although one can try several fraudulent contracts, but it is very unlikely that he can find one that has the right hash. The major problem associated with logarithmic signatures is to specify how this should be done. How can secure logarithmic signatures be generated?

6. Conclusion

Cryptanalysts can use powerful computing equipment and a variety of procedures, processes, and techniques to launch attacks against cryptosystems. In fact, a good cryptanalyst can even determine plaintext from samples of ciphertext without even knowing the cipher that was used to produce it. Knowledgeable intruders can use cryptanalysis techniques as part of their attacks against your cryptography-based security systems. When properly implemented, standard cryptography-based security technologies can provide a lot of protection against a wide range of attacks, including common cryptanalysis techniques. However, to obtain highly valuable information, skilled intruders or trained espionage agents with access to powerful computing resources might have the incentive to launch expensive and highly sophisticated cryptanalyst attacks. Stopping sophisticated cryptanalyst attacks requires highly secure systems that use strong cryptography-based security technologies. From the above discussion we are in a position to point out that group-based

cryptography motivates some beautiful and natural questions for the pure group theorist. Most obviously, the cryptosystems above motivate problems in computational group theory, especially combinatorial group theory. But we would like to highlight two more problems as examples of the kind of questions that can arise. Despite ten years of strong interest in group-based cryptography, a well studied candidate for a secure, well specified and efficient cryptosystem is yet to emerge.

7. References

1. David Garber, Shmuel Kaplan, Mina Teicher, Boaz Tsaban and Uzi Vishne, Probabilistic solutions of equations in the braid group, Adv. Appl. Math, 2005; 35:323-334.
2. James Hughes. A linear algebraic attack on the AAFG1 braid group cryptosystem, in Information Security and Privacy G. Goos, J. Hart-manis and J. van Leeuwen, eds, Lecture Notes in Computer Science 2384 Springer-Verlag, Berlin, 2002, 176-189.
3. David Garber, Shmuel Kaplan, Mina Teicher, Boaz Tsaban, Uzi Vishne. Probabilistic solutions of equations in the braid group, Adv. Appl. Math, 2005; 35:323-334.
4. Ryan D, Budney. On the image of the Lawrence-Krammer representa-tion, J. Knot Theory and its Ramifications, 2005; 14:1-17.
5. Mar´ıa Isabel Gonzalez Vasco, Martin Rotteler, Rainer Steinwandt. On minimal length factorizations of finite groups, J. Exp. Math, 2003; 12:1-12.
6. Mar´ıa Isabel Gonz´alez Vasco, Rainer Steinwandt. Obstacles in two public-key cryptosystems based on group factorizations, Tatra Mt. Math. Pub., 2002 25:23-37.
7. Holmes PE. On minimal factorisations of sporadic groups, J. Exp. Math, 2004; 13:435-440.
8. Aviad Kipnis, Adi Shamir. Cryptanalysis of the HFE public key cryptosystem, in Advances in Cryptology - CRYPTO ’99 M. Weiner, ed., Lecture Notes in Computer Science 1666 Springer, Berlin, 1999, 19-30.
9. McEliece RJ. A public key cryptosystem based on algebraic coding theory, DSN Progress Report 42 - 44 Jet Propulsion Lab, Pasadena, 1978, 114-116.
10. Sean Murphy, Kenneth Paterson, Peter Wild. A weak cipher that generates the symmetric group, J. Cryptology, 1994; 7:61-65.