Volume 2, Issue 10, October 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Various Techniques of Cryptanalysis

Mr. Vinod Saroha
CSE,SES,BPSMV
India

Suman Mor
CSE,SES,BPSMV
India

Jyoti Malik
CSE,SES,BPSMV
India

Abstract -***This talk will present a perspective on various techniques which are currently used for cryptanalysis purpose.This paper mainly focuses on various types of attacks which are mainly in use,in particular attacks on symmetric cipher,asymmetric cipher,hash system.Also on classification of attacks and side channel attacks. Aim a brief description of all available types of cryptanalysis techniques.***

Keywords— cryptology,cryptanalyst,attacker,cryptography, cipher,cryptanalysis.

I. INTRODUCTION

Cryptology is an art and science of hidden or secret writing.It has two main areas:cryptography and cryptanalysis[4]. Cryptography is basically related with converting data to make them secure and immune to attacks where cryptanalysis is related with breaking of codes[2].There are two categories of cryptography.

1.Symmetric key cryptography
2.Asymmetric key cryptography

In symmetric key,there is only single key which is used by sender for encryption and receiver for decryption.In this type the key is shared between both the parties[4].In asymmetric key,there are two keys:a private key and a public key.Private key is kept by receiver for decryption and public key is announced to public and used for encrypt the data[3]. Now various new techniques are developing for encryption of data as well as various tcechniques are also evolving in order to hack that data.This paper holds various methods of cryptanalysis which are used in these days.

II. CLASSIFICATION OF ATTACKS

The main goal of a cryptanalyst is to obtain maximum information about the plaintext(original data).Classification of attacks can be done on following basis[4]:

A. *Amount of Information Available to Attacker*

The main objective of attacking is to access the encryption key in place of simply decrypt the data.Attacks can be classified on the basis of information available to attacker.

- Ciphertext Only:In this type of attack an attacker can access only cipher text or decrypted data but can not access plaintext.This type of attack is done on simple cipher like caesar cipher where frequency analysis can be used to break the code.
- Known Plaintext:In this type a cryptanalyst have plaintext and their corresponding ciphertext.Attacker tries to find out the relation between these two.
- Chosen Plaintext:The attacker obtain the various ciphertext corresponding to an arbitrary set of plain text.
- Chosen Ciphertext:The attacker obtain the various plaintext corresponding to an arbitrary set of cipher text.
- Adaptive Chosen Plaintext:This is similar with the Chosen Plaintext,except in this attacker chooses subsequent set of plaintext which is based on the information obtain from previous encryption methods.
- Adaptive Chosen Ciphertext:This is similar with the Chosen Ciphertext,except in this attacker chooses subsequent set of ciphertext which is based on the information obtain from previous encryption methods(previous results).
- Related Key Attack:Like the chosen plaintext,attack in which attacker can obtain only cipher text encrypted with the haelp of two keys.These keys are unknown but the relationship between these keys is known.example two keys differ by a single bit.

B. *On the Basis of Computational Resources Required*

Attacks can also be classified on the basis of resources they require.Those resources are:

- Time :the number of computation steps(like encryption) that must be performed.
- Memory:the amount of memory required to perform the task.
- Data:the amount of plain text or cipher text required.

Actually it is very difficult to find out all these resources very precisely,specially when the attack isn't practical to actually implement for testing.But academic cryptanalst tend to provide atleast estimated order of magnitude of their attacks difficulty.For example SHA-1 collisions are 2^{52}.

C. *On the Basis of Partial Breaks*

The result of cryptanalysis also varies in terms of usefulness of that data.Cryptographer Lars Knudsen classified various types of attacks on the basis of amount and quality of secret information that is discovered.

- Total Break:In this attacker find out the secret key.
- Global Deduction:In this attacker find out equivalent algorithm for encryption and decryption without knowing secret key.
- Instance Deduction:Attacker find out some additional cipher text or plaintext without previously known.
- Information Deduction:Attacker find out some Shannon information about plaintext or ciphertext not previously known.
- Distinguishing Algorithm:Attacker differentiate various ciphertext from random permutation.

In academic cryptography,it is very difficult to specify break or weakness so it is define quite conservatively.It usually require unknown or impractical amount of time,money and ciphertext.The attacker may be able to do various things the real world attacker can't do.Furthermore,itmight only reveal a very small information in order to specify that cryptosystem is imperfect but this information is not that much useful for attacker.Finally attacker may attack only on the weakened version of cryptographic tools,like a reduced robin block cipher,as a step towards break the full system.

III. CRYPTANALYSIS OF SYMMETRIC CIPHER

There are various types of attacks done on symmetric cipher.The explaination is given below:

A. *Boomerang Attack*

This is a method of cryptanalsis of block cipher based on differential cryptanalsis.This attack provide various avenues of attack on various cipher which are deemed safe from differential cryptanalsis.

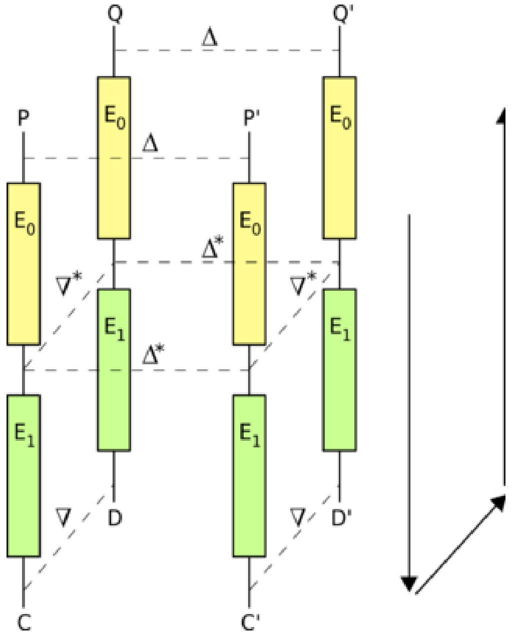

Fig. 1 Example of Boomerang attack

In differential cryptanalsis,an attacker exploits how difference in the input to a cipher can affect the resultant change in the cipher.A high probability "differential" is needed that covers all or nearly all of the cipher.This attack allows differentials to used which covers only part of cipher.

This attack is used to generate so called"quartet" at the point halfway through the cipher.For this purpose an encryption action E is split into its two consecutive stages E_0 and E_1 so that $E(M)=E_1(E_0(M))$,where M is plaintext message.Suppose we have two differentials for this stage:

$\Delta \longrightarrow \Delta^*$ for E_0 and

$\nabla \longrightarrow \nabla^*$ for E_1^{-1}(decryption of E_1)

The basis attack proceeds as follows:

- Choose a random plain text P and calculate $P' = P \oplus \Delta$
- Request the encryption of P and P' to obtain $C = E(P)$ and $C' = E(P')$

- Calculate $D = C \oplus \nabla$ and $D' = C' \oplus \nabla$
- Request the decryption of D and D' to obtain $Q = E^{-1}(D)$ and $Q' = E^{-1}(D')$
- Compare Q and Q',when differentials holds $Q \oplus Q' = \Delta$

B. Brute Force Attack

Brute force attack or exhaustive key search is a type of strategy which can be applied on any type of encrypted data.In this type of attack all possible keys are tried systematically until correct key is found.This method is used when any other weakness is not useful.The key length used in the encryption process specifies the practical feasibility of brute force attack,with longer keys exponential more difficult to crack as compared to smaller keys[1].One of the measure strength of the encryption system depends on theoretically how much time is taken to mount a successful brute force attack.The resources required for brute force attack grow exponentially with increase in key size,not linearly.

C. Davies' Attack

This attack is dedicated statistical cryptanalysis method for attacking Data Encryption Standard(DES).This attack was originally created by Donald Davies in 1987.It is a Known PlainText Attack which is based on non uniform distribution of output of pairs of adjacent S-boxes[3].It works by collecting various plaintext/ciphertext pairs and calculating empirical distribution of its characterstics.Various bits of keys are find out from plaintexts,leaving remaining bits to be find out through brute force attack.There is tradeoff between number of plaintext,keys found and probability of success.

D. Differential Cryptanalysis

This attack is a chosen plaintext attack in which relationship is find out between the cipher text produced by two related plaintext.It focuses on the statistical analysis of of two inputs and two outputs of cryptographic algorithm[4].This scheme can successfully crack DES with an effort on the order of 2^{47} chosen plaintext.In the method,the difference can be specified in several ways but eXclusive-OR(XOR) operation is mostly used.The cryptanalyst then encrypts plaintext and its XORed pairs using all possible subkeys,and it seeks the signs of non- randomness in each pair of intermediate ciphertext pairs.

E. Integral cryptanalysis

This attack is applicable on block cipher based on substitution-permutation networks.Unlike differential cryptanalysis,it uses sets or even multisets of chosen plaintext of which part is held constant and other part varies with all possibilitiesIt is commonly known as Square attack[1].

F.Linear Cryptanalysis

This is a known plaintext attack that require access to large amount of plaintext and ciphertext pairs which are encrypted with unknown keys.It focuses on statistical analysis against one round of decryption on large number of ciphertext.the attacker decrypts each cipher text using all possible subkeys for one round of encryption and studies the resulting intermediate cipher text to seek the least random result.A subkey which generate the least random intermediate cipher for all ciphertexts becomes a candidate key(most likely subkey)[2].

G.Man-in-the-Middle Attack

This type of attack can be used in those cases in which multiple keys are used for encryption[4].This attack is known plain text attack,the attacker has access to both the plaintext and resulting ciphertext.Example is attack versus Double DES.To improve the strength of 56-bit DES,Double DES (two rounds of DES encryption using two different keys,of total key length of 112 bits)was suggested.The attacker wants to recover two keys (key1 and key2) used for encryption.The attacker first apply brute force attack on key1 using all 2^{56} different single keys to encrypt the plaintext and saves each keys and cipher text ant analyst again brute force for key2 by using 2^{56}.The brute force attack is complete when both keys are known to attacker.The attack takes 2^{56} plus atmost 2^{56} attack,or maximum 2^{57} total attempts.This is far easier than 2^{112} attempts.

IV. CRYPTANALYSIS OF ASYMMETRIC CIPHER

Asymmetric cryptography is a type which relies on two keys,one private key for decryption and one public key for encryption.Such kind of cipher rely on the "hard" mathematical problem for their security.So the main point of attack is to develop methods to solve such problems.The security of two key cryptography depends on mathematical questions in a way that one key cryptography doesn't,conversely links to wider area of mathematical research in a new way.Asymmetric techniques are designed around of solving various mathematical problems.In case any improved algorithm is found to solve the problem then system is weakened.For example the security of Diffie-Hellman key exchange depends on calculating the discrete logarithm[2].RSA's security depends on difficulty of integer factorization-a breakthrough in factoring would impact security of RSA.Another main feature of asymmetric over symmetric cipher is that cryptanalst has an opportunity to make use of knowledge obtained from public key[3].

V. .CRYPTANALYSIS OF HASH SYSTEM

The attack which is apply on hash system is called as Birthday Attack.Actually birthday attack is an attack which can discover collisions in the hashing algorithm.It is based on birthday paradox,according to which if there are 23 people in a room,the odds are slightly greater than 50% that two will share the same birthday.The key to understanding the attack is that it is odds of any two people(out of 23)sharing a birthday. It is not odds of sharing birthday with the same person.This type of attack is mostly used on hash algorithm specially,SHA1 or MD5[4].

.

VI. .SIDE CHANNEL ATTACK

The side channel attacks basically based on some additional information based on some physical implementation of cryptographic algorithm including the hardware used to encrypt or decrypt the data.All cryptographic attacks above described assume that attacker has access plaintext or ciphertext pairs or cryptographic algorithm.A side channel attack basically used additional information like CPU cycle used, memory used, time consumed to perform calculation, voltage used etc[4].There are many practical example of side channel attack.One example of side channel attack is network based versus OpenSSL.

OpenSSL uses two type of multiplication:one type is called karatsuba,for equal sized words and normal multiplication for unequal sized words.Karatsuba is faster and the difference in speed can be detected via a network using an SSL TCP/IP connection.Attacker leaks information from the multiplication methods.

VII. CONCLUSION

In this paper we discussed about all type of cryptanalysis techniques.If we know about all type of attacks then it is very useful to improve the cryptographic algorithm or encryption techniques.The knowledge of all type of attacking techniques helps to make our system safe from any cryptographic attack.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Mr. Vinod Saroha who guides us to pursue this topic and help us to complete this topic.

REFERENCES

[1] William Stalling”Network Security Essentials(Applications and Standards)”,Pearson Education,2004

[2] Atul Kahate (2009), *Cryptography and Network Security*, 2nd edition, McGraw-Hill.

[3] Stallings W (1999), *Cryptography and Network Security*, 2nd edition, Prentice Hall.

[4] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education .