International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(1), pp.190-196
DOI: http://dx.doi.org/10.21172/1.91.29
e-ISSN:2278-621X

FAULT ANALYSIS IN CRYPTOGRAPHY

Shipra Saraswat[1], Tanisha Shangari[2] & Neetu Faujdar[3]

Abstract- Cryptographic mechanism is a major security component of operating system in securing its communication paths and its system. In maximum cases cryptography is only tool that can solve some problems like network level security. Usually cryptography also does not give guarantee for its security by itself, when applied in a correct manner it may improve overall security. This research paper covers an introduction on cryptography, Understanding of goals, how cryptography works, faults in symmetric algorithm, faults in asymmetric algorithm, Research issue and problem, latest trends and analysis

Keywords - Cryptography; Network Security; Encryption; Decryption; Active and Passive Attacks

1. INTRODUCTION

1.1 Define

The study of mathematical techniques which are related to some aspects of information security like data integrity, data authenticity and confidentiality is called cryptography.

1.2 Goals-

- Privacy or confidentiality
- Data Integrity
- Authentication
- Non-repudiation

1.3 Types-

- Symmetric
- Non Symmetric

In Symmetric cryptography, same secret key is shared between two parties to enable secure connection.

In Asymmetric cryptography, two secret keys are shared between them one is public key which is used for encryption and other is secret key which is used for decryption [1].

Cryptography is very useful in solving security issues as: (Figure 2)

- Network Security
- Secure storage facilities
- (Pseudo-)Random Number Generators

B.

As our goal is to provide strong security, we have introduced number of protocols and services to keep our mechanism such as IPsec, SSL etc. unaffected.

Supporting these mechanisms is not sufficient; we are trying to make their use easy and transparent to end user [2].

[1] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*
[2] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*
[3] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*

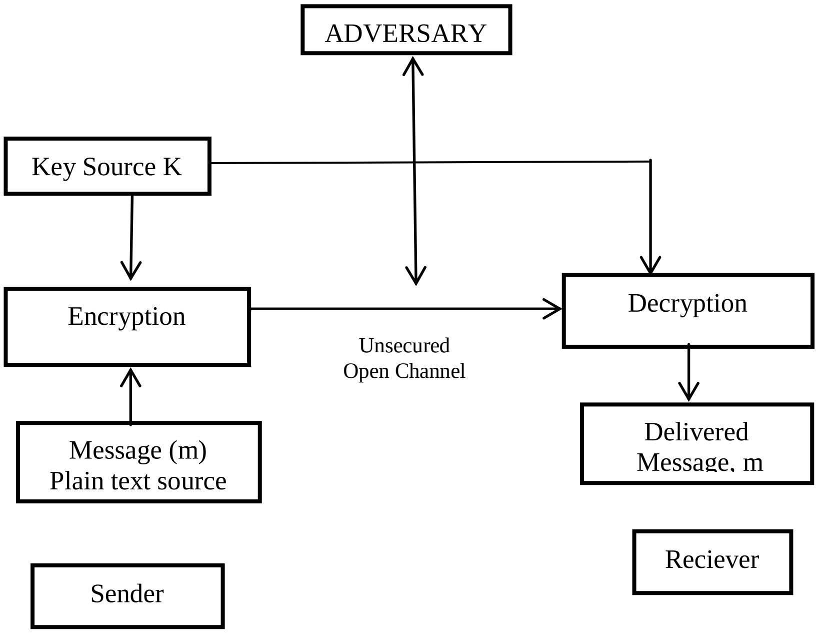

Figure 1. Symmetric encryption using same key

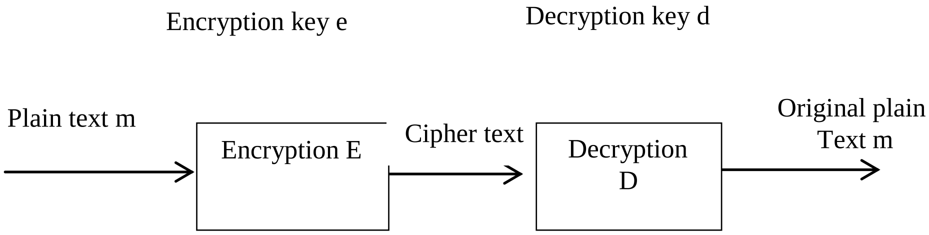

Figure 2 Asymmetric encryption using different keys

2. UNDERSTANDING OF GOALS

2.1 Privacy or confidentiality

Confidentiality and privacy are synonyms. It used to keep the content of information secret from all but only the authorized once can know it and use it.

2.2 Data Integrity-

The unauthorized manipulation of data such as addition subtracting the data. It detects the unauthorized change in its data [3]

2.3 Authentication-

This service is related to identification. Parties entering into communication should identify each other.

2.4 Non-repudiation-

It is the service preventing an entity from denying any commitment. If any dispute arises due to denying of entity, there should be a means to resolve the situation [4].

3. HOW CRYPTOGRAPHY WORKS

Consider that our data is very important and if we need to save it from hacker we need some important criteria to encrypt the data so that it becomes impossible for the hacker to decrypt the data and after doing so much things he would not able to decrypt it and the data he requires will not be delivered to him.

The encryption technique is used as suppose your data is someone's name. This name has to be hidden and have to be kept secured. Now this name is Naira. Now cryptography encrypt the data the name Naira in the form that A=Z B=Y an so on as in the algorithm and will encrypt the data so that if the hacker reach till information, he will not be able to read it or understand it and this cryptography technique is used by using cipher [5].

4. FAULTS IN SYMMETRIC ALGO

Symmetric encryption is one of the best and oldest techniques. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Issue using this algorithm is exchanging of key. Other issue is the trust between parties sharing symmetric secret key. Problems regarding trust will be faced when encryption will be used for authentication and integrity checking. This symmetric key is used to verify the identity of the other communicating party, but this is required that parties must trust each other [6].

4.1 The Key Exchange Problem-

This problem arises when the communicating parties have to share secret key before communicating and both parties have to keep it secret Direct exchange is not possible due to risk and cost factors. Then this question arises how to securely share key before communication is started The exchange of direct key is important in some situations. But in commercial data exchange the parties who never met each other and are dealing for the first time or the parties having some trust issues and still have to final a deal hesitate to trust each other for sharing their secret key. Due to this they will like to communicate to in a authenticated & secures manner. This problem can be resolved by use of asymmetric algorithm [7].

4.2 The Trust Issues-

Confirming the honesty of the data received and rechecking the source of data is very important

For example-

If data might be regarding any business deal then it has to be given more importance as it might be on higher risk .These problem are legally important and is investigated often about who and when is information being shared. Herein symmetric key can be used to verify the identity of the source and destination in which the data is being shared. But with the introduction of new concept there arises some more problems with it related to trust

In this technique the data is hashed, and the resulting hash is encrypted using a shared secret key with a symmetric algorithm. The recipient, who also knows the secret key, is sent the data along with the encrypted hash value. The recipient then decrypts the hash using the shared key, and the result is verified against a fresh recalculation of the hash value on the data received. This works because only someone who knows the secret key is capable of correctly encrypting the hash of the original data such that it will match the recalculated hash value computed by the recipient. This verifies the identity of the data source. As an added bonus, this technique verifies data integrity in that any individual who is ignorant of the secret key could not have tampered with the data [8].

This is great if you have the luxury of establishing the shared secret beforehand, but there is an additional problem here. What if you cannot trust the other party with whom you have shared the secret key? The problem is that this scheme cannot discriminate between the two individuals who know the shared key. For example, your pen pal may fraudulently send messages using your shared key, pretending to be you. This would allow your friend to write IOUs to himself in your name, making this scheme useless in any trust-lacking relationship. Other problems could arise if your partner shared the secret key with others without telling you about it. Suddenly, you would have no leg to stand on if certain disputes were to arise. For example, your partner could renege on a contract by claiming that someone else must have obtained the key from you and signed off on a deal in his name. This problem is known as repudiation, and we often need a way to enforce nonrepudiation between untrusting parties. The basic problem with all this is that any symmetric algorithm scheme requires that one party can safely trust the other party, which often is not realistic.

Asymmetric algorithms can be used to solve these problems by performing the same basic operations but encrypting the hash using a private key (belonging to an asymmetric key pair) that one individual and only one individual knows. Then anyone can use the associated public key to verify the hash. This effectively eliminates the problems of trust and repudiation. This technique is called a digital signature

5. FAULTS IN ASYMMETRIC ALGO

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair . A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message [9].

6. RESEARCH ISSUES AND PROBLEMS

There is a need of high computing power processors for creating diversifies circumstances in order to achieve symmetric encryption that works for the small length of the key because of the distributed computational methods that can broke the small key easily.

Also, DES (Data Encryption Standard) has given a 56 bits symmetric key that was already been cracked by the Electronic Frontier within 3 days. 56 bits symmetric key of Data Encryption Standard (DES) has already been cracked practically by Electronic Frontier Foundation in 1998 within the duration of less than 3 days other problem of symmetric encryption is the key exchange because without secret and secure key exchange, symmetric encryption becomes unconfident. Origin authentication and group based secure information exchange under symmetric approach are the big issues. It cannot be assured at the time of exchanging secret key, either the received key is not falsely modified by hacker or it is really send by the authentic sender from whom we are expecting? Similarly, if a person P wants to send 50 different secret messages to 50 group members then P required to generate 50 secret keys for completing this task under symmetric encryption scheme which is difficult to remember moreover, in this case if each user wants to communicate with each other user of the same group then the total no. of key(s) required to exchange for whole group can be calculated as follows

Let G is the no. of group members So G = 50

Total Key(s) required for mutual communication of whole group = G (G-1) / 2

= 50(50-1) / 2

= 50 (49)/2

= 1225 keys

It means for mutual communication of all group members; one two two five secret keys will be required to exchange.

This situation will result extra load on the network. Asymmetric scheme is 100 times slower than symmetric one. It deals with large key(s) and involvement of third trusted party which may be risky from country to country communication due to spy attacks or political reasons. Issuing and renewing of certificate requires cost and extra penalty of time consumption. In case of large data it is not feasible due to laziness of encrypting process that requires more Random Access Memory (RAM) and electric power. Certification Authority behaves like a central server so the central point of failure is another notable issue that may leads the situation to large penalty of waiting time due to load or failure.

Furthermore, the increasing demand of public key cryptosystem is creating problem for managing and storing of large no. of certificates. Natural disasters, security threats and vulnerabilities may lead the Certification Authority to a critical situation. It means sufficient backup and enhanced security plans are required for central point authority. Origin authentication is necessary for security and this objective can be achieved with digital signature but the minimum key size is 1024 bit for digital signature that is the greatest hurdle in processing speed . Hash functions are fast in processing but hash function did not provide origin authentication. Message authentication codes are quite fast and based on symmetric key, so these are required to share and agreed on single key as a prerequisite of encryption; moreover, key is small as compared to public key that makes the user unconfident due to large computation power processors that can act in distributed fashion with parallelism to break the security of small length key.

For a very disorganized image encryption there is no standard criteria to measure performance as different authors have different opinions. Quantum cryptography does not provide reliable signature scheme for authentication and integrity; furthermore, it associates the possibility of man-in-middle attack and Denial of Service attack. Elliptic Curve Cryptography is slow in signature verification and enciphering process than symmetric encryption. NIST and ISO do not recommend quantum cryptography and elliptic cryptography. Steganography itself is just process of hiding information but it cannot provide required security objectives and concealing process with image results the large size of message. The critical issue with steganography is the implementation of statistical and Radiofrequency methods like Measurement and Signature intelligence (MASINT) to realize the inter–bit delays for cracking the information [10].

7. LATEST TRENDS AND ANALYSIS

Smmetric scheme associates probability of happening many things for the cracker where the asymmetric scheme is based on factorization of large no. with large mathematical functions but it can be determined mathematically that means asymmetric technique is just increasing the processing time but lacked to confuse the cracker with randomness. A study conducted in 2007 that claims; the practical encryption scheme should be probabilistic like symmetric encryption rather than deterministic scheme like a symmetric encryption . In 2009,

Perlner. R. A. and Cooper. D. A. said, there is no particular need to replace symmetric encryption with quantum cryptographic methods. In 2007 study reported that the International Standard Organization ISO 9564-1 recommends that the minimum key length for symmetric scheme should be 112 bits for sufficient security. In 2008, Cryptographic Key Injection Facility: Auditor's Guide Version 1.0 reported the following key lengths for following cryptographic algorithms [11].

Cryptographic Schemes	**Minimum Key Length**
Symmetric Cipher(DES)	112 bits
Asymmetric Elliptic Cryptography	160 bits
Asymmetric RSA and DSA	1024 bits

In today’s time all the things related to human life are filled with some kind of information. Because of which it is compulsory to keep the information safe from attacks attempted by attackers.

Attacks can be determined o the process attempted by attackers.

Passive Attacks-The main goal of a passive attack is to obtain unauthorized access to the information. For example, actions such as intercepting and eavesdropping on the communication channel can be regarded as passive attack.

They do not affect information as well as don’t disrupt the communication channel, such actions are passive in nature .A passive attack is often seen as stealing information. The only difference in stealing physical goods and stealing information is that theft of data still leaves the owner in possession of that data. Passive information attack is thus more dangerous than stealing of goods, as information theft may go unnoticed by the owner [12].

Active Attacks-In this attack attacker does some process on information so that he can change some information In For example,

- Modifying the information in an unauthorized manner.
- Initiating unintended or unauthorized transmission of information.
- Alteration of authentication data such as originator name or timestamp associated with information
- Unauthorized deletion of data.
- Denial of access to information for legitimate users (denial of service).

Cryptography gives many methods and equipment’s for implementing cryptosystems capable of preventing most of the attacks described above.

Assumptions of Attacker- Let us see the prevailing environment around cryptosystems followed by the types of attacks employed to break these systems [13].

Environment around Cryptosystem-As we are learning about possible attacks n cryptosystems, it is must to have knowledge about cryptosystems environment. The knowledge of environment of cryptosystems of attacker reflects his capabilities

In cryptography, the following three assumptions are made about the security environment and attacker’s capabilities.

Details of the Encryption Scheme- The design of a cryptosystem is based on the following two cryptography algorithms −

- Public Algorithm details of algorithm known to everyone
- Proprietar Algorithm details of the algorithm are only known by the system designers and users.

In proprietary algorithms, security is ensured through obscurity. Private algorithms may not be the strongest algorithms as they are developed in-house and may not be extensively investigated for weakness.

Secondly, they allow communication among closed group only. Hence they are not suitable for modern communication where people communicate with large number of known or unknown entities. Also, according to Kerckhoff’s principle, the algorithm is preferred to be public with strength of encryption lying in the key.

Thus, the first assumption about security environment is that the encryption algorithm is known to the attacker.

Availability of Cipher text-We know that once the plaintext is encrypted into cipher text, it is put on unsecure public channel for transmission. Thus, the attacker can obviously assume that it has access to the cipher text generated by the cryptosystem [14].

Availability of Plaintext and Cipher text-This assumption is not as obvious as other. However, there may be situations where an attacker can have access to plaintext and corresponding cipher text. Some such possible circumstances are − The attacker influences the sender to convert plaintext of his choice and obtains the cipher text .

- The receiver may divulge the plaintext to the attacker inadvertently. The attacker has access to corresponding cipher text gathered from open channel.
- In a public-key cryptosystem, the encryption key is in open domain and is known to any potential

Attacker. Using this key, he can generate pairs of corresponding plaintexts and cipher texts.

Cryptographic Attacks-The aim of attacker is to attack (break) the cryptosystems and use cipher text and obtain plaintext from it. To find plaintext, attacker needs to get secret description key as the algorithms are already a public domain

So he gives maximum of his time to obtain secret key which is used in particular cryptosystems. As he obtains the key that system is said to be broken or compromised

Based on the methodology used, attacks on cryptosystems are categorized as follows −

7.1 Cipher text Only Attacks (COA)-

Herein the attackers know the cipher text and can access it but do not know the plain text regarding it. This attack can said to be successful when the attacker will be able to know the plaintext from the cipher text he knows. Mainly encryption key can be known with the help of this attack Morden cryptosystem are guarded against COA [15].

7.2 Known Plaintext Attack (KPA)-

Herein the attacker has some information about the cipher text .Now he needs to find (decrypt) complete information about that particular cipher text using that particular info. This can be achieved by finding the key by some method
Best example linear cryptanalysis against block ciphers.

7.3 Chosen Plaintext Attack (CPA)-

In this method, the attacker has the text of his choice encrypted. So he has the cipher text-plaintext pair of his choice . This simplifies his task of determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.

7.4 Dictionary Attack-

Many variants in this attack are involved in compiling of a dictionary. In simple terms attacker learns some cipher text and information in some time and forms a dictionary of it. So whenever in life he gets a cipher text he can refer that dictionary and check related information about that cipher text.

7.5 Brute Force Attack (BFA)-

Herein the attacker knows the algorithm and the cipher text and through which he will try to determine the key by applying the entire possible key. If the key will be 8 bit in size then the probability will be 2^8.This makes 256 possible attempts that can be tried to decrypt. The time to decrypt will be very long and will depend on the perfect probability figure

7.6 Man in Middle Attack (MIM)-

It targets mostly public key cryptosystems because here key exchange is done before communication o Suppose party 1 wants to communicate to party 2 then party 1 will ask for public key from party 2

- Attacker detects this process of request and sends its own public key o Then he is able to read everything that party 1 is sending to party 2. o In order to maintain the communication and not get caught the attacker re-encrypts the data and sends it to party 2
- The attacker sends it in a way that arty 2 will believe that the data has come from party 1 and not from the attacker

7.7 Side Channel Attack (SCA)-

This type of attack is not against any type of cryptosystem or algorithm. It is launched to exploit the weakness in physical implementation of the cryptosystem.

7.8 Timing Attacks-

They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out.
For example, if the secret key is long encryption will take longer time.

7.9 Power Analysis Attacks-

These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.

7.10 Fault analysis Attacks-

These attacks induce errors in cryptosystem so that attacker can study it and gather useful information

7.11 Practicality of Attacks-

The attacks on cryptosystem which are described here are academic because maximum of them belongs to academic community. However many of them involves unrealistic assumptions regarding environment and capabilities of the attackers For example, in chosen-cipher text attack, the attacker requires an impractical number of deliberately chosen plaintext-cipher text pairs. It may not be applied over all however the detail that some attack happens should be reason of fear mainly if the attack method has chances for development [16].

8. CONCLUSION

This technique of cryptography is moving towards another level of success. Despite of many hindrances being getting by the hackers and failures it has shown a very resilient behavior towards its growth.

9. REFERENCES

[1] Zhang, X., Parhi, K.K, Implementation approaches for the advanced encryption standard algorithm, IEEE Circu. Syst. Mag. 2(4), pp. 2446, 2002.

[2] Yen, S.M., Kim, S., Lim, S., Moon, S.J, RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis, IEEE Transac. Comput. 52(4), pp.461472, 2003.

[3] Yen, S.M., Joye, M, Checking before output may not be enough against fault-based cryptanalysis, IEEE Transac. Comput. 49(9), pp. 967970, 2000.

[4] Yen, C.H., Wu, B.F, Simple error detection methods for hardware implementation of advanced encryption standard, IEEE Transaction Computing, 55(6), pp. 720731, 2006.

[5] Wang, Z., Karpovsky, M.G., Kulikowski, K.J, Replacing linear Hamming codes by robust nonlinear codes results in a reliability improvement of memories, IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 514523, 2009.

[6] Takahashi, J., Fukunaga, T, Differential fault analysis on the AES key schedule, Improved version of DFA mechanism on the AES key schedule, 2007

[7] P. Kocher J. Jaffe B. Jun P. Rohatgi ,"Introduction to differential power analysis" ,J. Cryptograph. Eng., vol. 1 no. 1 pp. 5-27 Mar. 2011.

[8] J. Heyszl S. Mangard B. Heinz F. Stumpf G. Sigl "Localized electromagnetic analysis of cryptographic implementations" ,Proc. CT-RSA,pp. 231-244 Feb. 2012.

[9] Y. Li K. Ohta K. Sakiyama "New fault-based side-channel attack using fault sensitivity" ,IEEE Trans. Inf. Forensics Security, vol. 7 no. 1 pp. 88-97 Feb. 2012.

[10] H. Bar-El H. Choukri D. Naccache M. Tunstall C. Whelan "The sorcerer's apprentice guide to fault attacks" ,Proc. IEEE,vol. 94 no. 2 pp. 370-382 Feb. 2006.

[11] D. Karaklajić J.-M. Schmidt I. Verbauwhede "Hardware designer's guide to fault attacks" ,IEEE Trans. Very Large Scale Integr. (VLSI) Syst.,vol. 21 no. 12 pp. 2295-2306 Dec. 2013.

[12] R. Leveugle et al. "Laser-induced fault effects in security-dedicated circuits" Proc. 22nd Int. Conf. Very Large Scale Integr. (VLSI-SoC), pp. 1-6 Oct. 2014.

[13] X. Guo R. Karri "Recomputing with permuted operands: A concurrent error detection approach" ,IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.,vol. 32 no. 10 pp. 1595-1608 Oct. 2013.

[14] H. Tupsamudre S. Bisht D. Mukhopadhyay "Destroying fault invariant with randomization" ,Proc. Cryptograph. Hardw. Embedded Syst. (CHES),pp. 93-111 Sep. 2014.

[15] B. Gierlichs J. M. Schmidt M. Tunstall "Infective computation and dummy rounds: Fault protection for block ciphers without check-before-output" Proc. Progr. Cryptol. LATINCRYPT,pp. 305-321 2012.

[16] J. G. J. van Woudenberg M. F. Witteman F. Menarini "Practical optical fault injection on secure microcontrollers" Proc. Workshop Fault Diagnosis Tolerance Cryptography (FDTC) pp. 91-99 Sep. 2011.