A Review on Cryptographic Algorithms, Attacks and Key Management Techniques

Saima Iqbal[1] Mr.Ramlal yadav[2]
[1]Research Scholar [2]Associate Professor
[1,2]Kautilya Institute of Technology and Engineering, Jaipur

Abstract— In every organization security of data is the most vital aspect nowadays. Cryptography is the means of ensuring data integrity and confidentiality in order to enhance security. In this paper we have three basic cryptography algorithms, types of attacks on encrypted data and various key management techniques.

Key words: algorithm, cryptography, data integrity, encryption, security

I. INTRODUCTION

Cryptography is the practice or technique of communicating in the presence of malicious entities .It is a used in several fields: information security and [1] authentication, and access control. The main aim of Cryptography is encoding the messages and altering their meaning, not their existence. Cryptography is used in many areas examples: ATM cards, computer passwords[1], on-line shopping, stock trading, e-banking . Cryptography is the technique to convert the text message (Plain text) into coded form (cipher) by Sender and send it to Receiver who converts(decrypt) the message into original text format(Plain text) after receiving it in order to secure it from getting lost or damaged. Cryptography has been emerged as important tool for data transmission. A variety of algorithms of cryptography have been studied[2].

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

The encryption algorithms are categorized into two types: Symmetric key encryption and Asymmetric key encryption.

A. Symmetric Key Encryption (private key encryption algorithm):

In symmetric key encryption algorithm same key is used for encryption and decryption. The key is communicated between sender and receiver before data transmission. Strength of symmetric key algorithms depends on size of key[3]. Symmetric key cryptography algorithms include RC2, DES, 3DES, RC5, Blowfish, and AES, which use fixed- or variable-length key.[3]

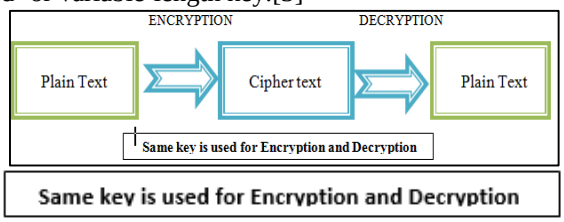

Fig. 1:

ALGORITHMS	KEY SIZE	BLOCK SIZE
DES	56	64
3DES	112 or 168	64
AES	256	128
BLOWFISH	32-448	64

Table 1: Types of Symmetric Key Cryptographic Algorithms

ADVANTAGES	DISADVANTAGES
It is simple to carry out . Users only have to share and specify the private key.	It needs a secure transfer medium for the exchange of private key.
It is faster than public key encryption algorithm and uses less computer recourses.	2. It requires too many encryption keys. For communication with every party a new shared key is required
For communication with each party a unique private key is required .If any key is compromised only messages between that party will be affected for other parties it is secure.	3. Message cannot be verified to have come from particular user since both parties uses same key for encryption and decryption[4]

Table 2: Advantages And Disadvantages Of Symmetric Key Encryption[4]:

B. Asymmetric or public key cryptography:

Asymmetric key encryption is used to solve the problem of key transmission. In Asymmetric key encryption, two keys are used namely private key and public key. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). However, public key encryption is based on mathematical functions, and is not very efficient for small mobile devices [3].

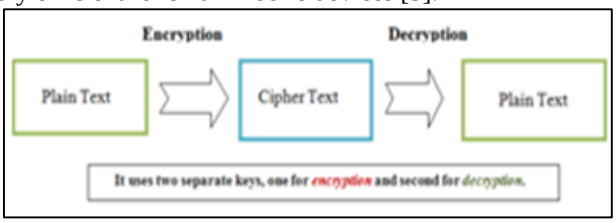

Fig. 2:

ADVANTAGES	DISADVANTAGES
1.It solves the problem of key distribution in symmetric keys encryption	1. It is slow as compared to symmetric key encryption.
2.It allows authentication of received message through use of digital signatures	2. It uses more computer resources[4].
3 Digitally signing[4] is way of acknowledgement of message and it cannot be denied by sender.	3 .If the private is lost all the received message can not be decrypted.

Table 3: Advantages and Disadvantages of Asymmetric Key Encryption [4]:

III. TYPES OF ATTACK

A. Brute Force Attack

It is an attempt to decrypt an encrypted message by trying with possible key. If the length of key used is long then brute force attack are not very efficient[5]. For example it is very difficult to break a key of length 128 bits.

B. Cryptanalysis

It refers to process of breaking encrypted codes. It refers to mechanism of exploring weakness in ciphers or cryptosystems that allow retrieval of plaintext from cipher text, without knowledge of the key or the encryption algorithm.

1) KKnown Plaintext attack

In this attack the attacker tries to deduce the key and recognize the algorithm involved in encryption by analyzing a block plaintext with corresponding block of cipher text[5].

2) CChosen plain text attack

In this attack the attacker encrypts any plaintext creating a cipher text[5] which cryptanalyst can analyze to deduce the encryption key used to decrypt message.

3) DDifferential cryptanalysis

In this attack many plaintext attacks which are slightly different are encrypted and results are compared to analyze the key.

4) DDifferential fault analysis

This attack are related to cryptosystem that are built in hardware[5].That device is exposed to factors (stress, radiation, heat)[5] to make the encryption and decryption process faulty. These faults are analyzed to know the internal state of device.

C. Security Threats

Security threats are those attacks that can begin the network security attack[5].Some of the security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares[5]

IV. KEY MANAGEMENT TECHNIQUES

Key management can be defined as process of generating keys and distributing them between authenticated users for encryption And decryption of information. These techniques are classified into two types.[6]

1) Static key management.
2) Dynamic key management.

A. Static Key Management

In static key management key is stable for whole process of encryption and decryption.

Since the keys remain same so chances of attacks on these system increases.[6]

B. Dynamic Key Management

In dynamic key management a new key is generated for each communication between sender and receiver .With the Dynamic key mechanism, the key and the system are changed for each new transmission. This is done by adding a dynamic encryption layer with standard encryption system.

The key management schemes can be categorized as:

1) Distributed key management

In this scheme there are number of key controllers instead of having a single controller for rekeying process to avoid failure at any single point.

2) Centralized key management scheme

In this scheme there is only a single controller e.g. base station or any third party[6] For rekeying process. It is further classified into three parts: [6]

a) Flat centralized Dynamic key management.[6]
b) Hierarchical centralized Dynamic key management.[6]
c) Heterogeneous Dynamic key management.[6]

In dynamic encryption algorithm each new data transmission is encrypted with new encryption key. This done by adding a encryption dynamic layer in with standard system of encryption.

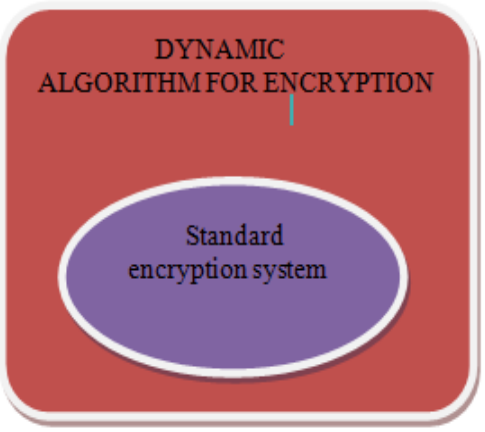

Fig. 3:

Cryptanalysis is hard to achieve due to dynamic key encryption algorithm.. It gives the confidence that information is secure.

V. SUMMARY

Cryptography is the process of assuring that the message has not been modified. Many cryptographic algorithm are used to provide data privacy to the data being transmitted considering all the attacks on cryptography. Key management techniques are used to enhance the privacy in transmitted data.

REFERENCES

[1] 1.Tanjyot Aurora, 2.Parul Arora, Blowfish Algorithm, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013
[2] https://en.wikipedia.org/wiki/Cryptography
[3] Tingyuan Nie, Chuanwang Song,,Xulong Zhi, Performance Evaluation of DES and Blowfish Algorithms, 978-1-4244-5316-0/10/$26.00 ©2010 IEEE.
[4] http://itchyfish.com/advantages-and-disadvantages-of-symmetric-and-asymmetric-key-encryption-methods/.
[5] Rajesh R Mane, A Review on Cryptography Algorithms, Attacks and Encryption Tools, International Journal of Innovative Research in Computer and Communication Engineering (An ISO

3297: 2007 Certified Organization) Vol. 3, Issue 9, September 2015

[6] 1.Deepika 2.Manpreet, A Review on Various Key Management Techniques for Security Enhancement in WSN, International Journal of Engineering Trends and Technology (IJETT) – Volume 34 Number 4- April 2016.

