International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 1, July 2014)

# Security Algorithms in Cryptography and their network Attacks

Jitender Singh[1], Monika[2]

*[1,2]M. Tech Scholars in RPSGOI Mohindergarh, Haryana, India.*

***Abstract*–Cryptography algorithms can be divided in to two groups that are Symmetric key (also called as Secret key) algorithms and Asymmetric algorithms (also called as Public key). In Symmetric key same is used at both sides that is at sender side as well as receiver side .that is sender encrypt the message with same key as the receiver uses to decrypt the message . Where as in Asymmetric key two different keys are used by sender and receiver to encrypt or decrypt the message. Sender uses the Public key to encrypt the message whereas receiver uses the private key to decrypt the message. Public is used as publically but private key is used by individually. Hence three keys are used in cryptography that is public key, secret key and private key [1]. Cryptanalyst studies the algorithm, finding its pattern and weakness while cryptographer set to try to secure the message by applying the algorithm. Various technologies are used to secure the message like AES, DES, DSS, Encryption, and RSA. Symmetric key also uses the Traditional cipher, Substitution cipher, Mon alphabetic cipher, poly alphabetic cipher, Shift cipher, Transposition cipher, Simple modern cipher, Xor cipher, Rotation cipher, Substitution cipher s-box, transposition cipher p-box, including expansion permutation, compression permutation, straight permutation, modern round cipher, Data Encryption standard (DES), triple DES, Advanced Encryption standard (AES) other ciphers like IDEA, BLOWFISH, RC-5, CAST-128,while Asymmetric approach use RSA and Diffie-Hellman algorithms in cryptography.**

***Keyword*- Cryptanalyst, cryptographer, computational complexity, OSPA protocol, Cryptosystem, field theory, transposition.**

## I. INTRODUCTION ABOUT CRYPTOGRAPHY

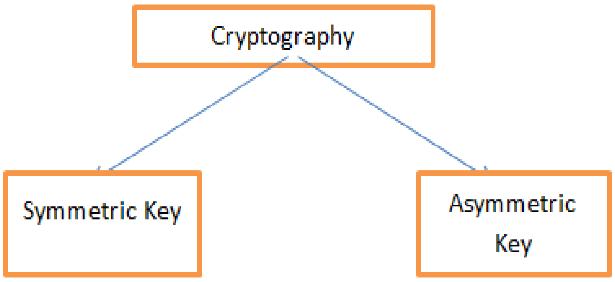
Cryptography is a technique of encoding and decoding a message so that no other can access the message. Cryptography is used in network security. Cryptography was firstly developed by Department of Defence in U.S.A. Cryptography is the science of using mathematics to encrypt or decrypt the data. Cryptography enables you to store secure information [2] or transmit it across in-secure networks like internet so that it cannot be read by anyone except the intended recipient. Cryptography is an art of secret writing or cryptography is a science of encrypting or hiding secrets. When a message is transferred through the network, many attacks occurred on network. Some important attacks are like Trojan horse attack, brute force attack salami attacks, timing attacks, man- in-the middle attacks.

The most famous way to protect the message is unique Id and password. In practical unique password and Id is given to energy user by two factor of authentication (E.g. debit card, mobile phone, cordless phone etc.). There are three factor of authentication are also present like retina scan, heart scan, finger print scan. Many attacks when occurred on networks can be removed by using the anti-virus, window defender. Cryptography uses various technologies to protect [5] messages like AES, DES, DSS, Encryption, and Decryption. As encryption uses the plain text message, encrypted, and output in the form of decryption. Decrypted message send over the network then at receiver side message is in the form of cipher text. Symmetric and asymmetric keys are used in encryption. Where symmetric key is also known as public key and asymmetric key is called as private key. Cryptography uses plain text which is called as original message. Cipher text is the encoded message. Conversation of plain text to cipher text called as encryption algorithm and vice versa is called as decryption algorithm. Conversation is done by the secret key, public key or private key.

There are two categories of the cryptography algorithms:-

1. Asymmetric [6] key.
2. Symmetric key.

Diagram for categories are as above:-



Symmetric key uses only secret key whereas asymmetric key uses both public and private keys.

There are difference between secret key and public or private key with their characteristics:-

| Sr. No. | Characteristics | Secret Key | Public Key |
|---|---|---|---|
| 1. | Number of Keys | 1 | 2 |
| 2. | Protection of Key | Must be kept secret | One Key must be secret but other cannot |
| 3. | Key Distribution | Must be out of band | Public key can used to distribution other keys |
| 4. | Speed | Fast | Slow |
| 5. | Best Use | Block of Data, Message, Files | Key Exchange, authentication |

Cryptosystem is based on the hard problems. Knapsack problems can not solved out cryptography because it takes too much time for solution. We discuss here only asymmetric key algorithm that is RSA [3] and Diffie-Hellman [4] and attacks occurred on both algorithms and how these attacks can be removed.

## II. Related Survey

The most common public key algorithm is RSA. Suggested by Rivest, Shamir, Adleman. It has two numbers that is e and d as the public and private key. Let sender is represented by A and receiver is represented by B.

*Selecting Keys:-*

B uses the following steps to select the public and private keys.

1. B uses two very large prime numbers like p and q. Prime number can be divided only by 1 or itself.
2. B multiplies the prime numbers i ,e p and q to find the n. I, e n=p*q.
3. B calculates another number Ø= (p-1)*(q-1).
4. B selects a random integer e and calculates d i, e d*e=1mod Ø.
5. B announces e and n to public i, e B keep Ø and d secret.
6. Here e and n are public and d and Ø are private.

Encryption can be done by this method i, e
C= $p^{e}$ mod n

And decryption can be done by this method i, e

P=$c^{d}$ mod n

If p is larger than n, p can be divided in to blocks.

For Example:-

Let B selects 17 and 11 as p and q. Then finding n=p*q or
n=17*11 i, e n=187

And value of Ø = (p-1)*(q-1) i, e Ø=160. Then finding the two keys

d*e=1mod n.

23*7=161=10*160+1

So, d=23. For C=$88^{7}$ mod 187

$88^{7}$ mod 187= ($88^{4}$ mod 187)* ($88^{2}$mod 187)* ($88^{1}$ mod 187).

$88^{4}$ mod 187=132,
$88^{2}$mod 187=77,
$88^{1}$ mod 187=88,

$88^{7}$ mod 187= (88*77*132) mod 187

$88^{7}$ mod 187=894432 and
894432 mod 187=11, And for

Decryption:-

M=$11^{23}$ mod 187, P= $c^{d}$ mod n.

($11^{1}$ mod 187)=11,
($11^{2}$ mod 187) =121,
($11^{4}$ mod 187)=14641 mod 187=55,
($11^{8}$ mod 187)=214358881 mod 187 =33.
($11^{1}$ mod 187)=79720245 mod 187=88.

Hence the plain text 11 is send by B is received by A is 88.

But RSA algorithm is very slow in very long messages. It is very useful for short messages. It is used in Digital signature which is also a type of cryptosystem. RSA is also used for authentication.

Diffie-Hellman method is designed for key exchange. In Diffie-Hellman two parties create a symmetric session key to exchange data. Let A wants to communicate B, then both parties need to choose to numbers i, e p and g. The first number p is large prime number in order to 300 decimal digits (1024 bits). The second number is random number. These two numbers are not necessary to secret. They can be public.

*Selection Process of Keys:-*

Step1. If A choose a large random number x and calculates $R_1=g^{x}$ mod p.

Step2. B choose another large random number y and calculates $R_2=g^{y}$ mod p.

Step3. A sends $R_1$ to B, not x.

Step4. B sends $R_2$ to A, not y.

Step5. A calculates K= $(R_2)^x$ mod p. And B calculates K= $(R_1)^y$ mod p.

For Example:-

Let g=7 and p=23, According to Steps:

A choose x=3 and calculates $R_1=7^3$ mod 23 i, e

$7^2$ mod 23=3 and
$7^1$ mod 23=7, OR
$7^3$ mod 23=21 mod 23=21,

B choose y=6 and calculates $R_2=7^6$ mod 23 i, e

$7^4$ mod 23=9 and
$7^2$ mod 23=3, OR
$7^6$ mod 23=27 mod 23=4,

Now A sends 21 to B and B sends number 4 to A.
A finds the public key k=$4^3$ mod 23.

$4^2$ mod 23=16 and $4^1$ mod 23=4 OR $4^3$ mod 23=64 mod23=18.

B finds the public key:

K=$21^6$ mod 23 i, e $21^4$ mod 23=16 and $21^2$ mod 23=4 OR $21^6$mod 23=64 mod 23=18.

Hence both keys are same i, e $g^{xy}$ mod p= $7^{18}$ mod 35=18.

Hence Diffie-Hellman algorithm is very important because keys are very large to find. But one problem with Diffie Hellman is intruder.

Let A choose x and find $R_1=g^x$ mod p and send to B.

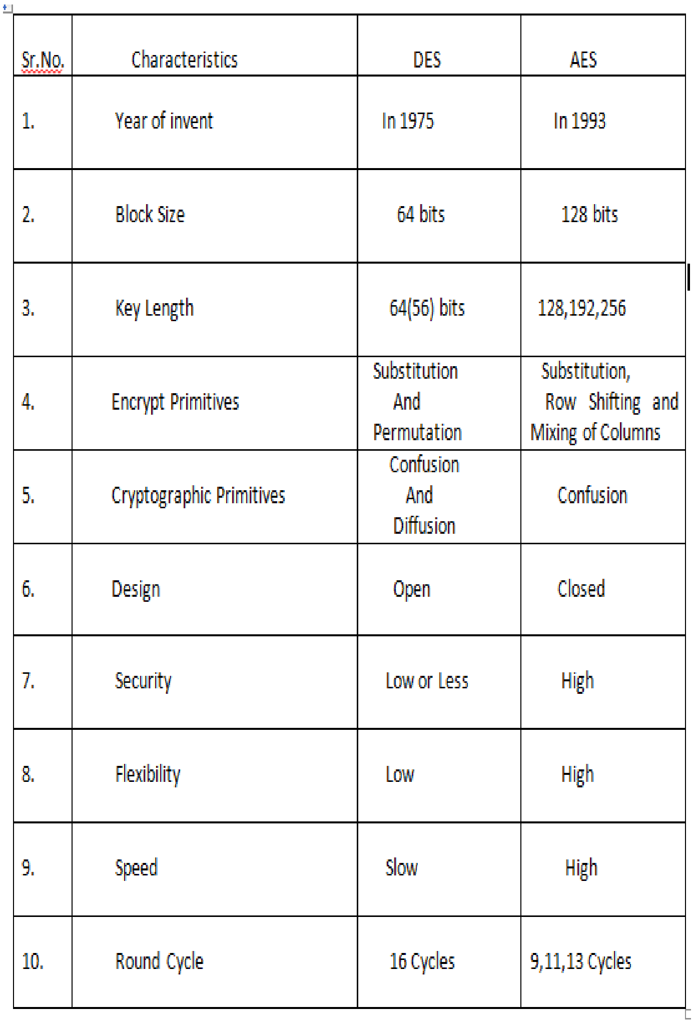
Let C is intruder, it accept it and choose $R_2=g^z$ mod p and send $R_3$ to A and $R_3$ is intercepted by C and never reaches to A.

Hence two keys are produced instead of one. This situation called as Man-In-Middle, because C comes in between A and B, and also called as bucket bridge attack.

Whether in RSA four possible attacks can occur:-

1. *Brute Force attack:*-This tries all possible private keys.
2. *Mathematical attack:*-These are many approaches like factoring the product of two primes.
3. *Timing attack:*-This depends on run time of decryption algorithm.
4. *Chosen Cipher Text attack:*-This type of attack exploits the properties of RSA algorithm.

The comparisons [7] between the AES with DES with their characteristics are as above.



| Sr.No. | Characteristics | DES | AES |
|---|---|---|---|
| 1. | Year of invent | In 1975 | In 1993 |
| 2. | Block Size | 64 bits | 128 bits |
| 3. | Key Length | 64(56) bits | 128,192,256 |
| 4. | Encrypt Primitives | Substitution And Permutation | Substitution, Row Shifting and Mixing of Columns |
| 5. | Cryptographic Primitives | Confusion And Diffusion | Confusion |
| 6. | Design | Open | Closed |
| 7. | Security | Low or Less | High |
| 8. | Flexibility | Low | High |
| 9. | Speed | Slow | High |
| 10. | Round Cycle | 16 Cycles | 9,11,13 Cycles |

## III. Various Attacks On Network

*Layered Attack-*

Network layered attack, Warm whole layered attack, black hole layered attack, sink hole layered attack, IP hijacking layered attack, IP snooping, Routing table layered attack, Grey hole layered attack.

*Transport Layer Attack-* Session hijacking, Slip deprivation attack.

*Application Layer attack-* Cryptanalysis, password, virus,

Physical Layer Attack- Wiretapping.

*Other Attacks-* Man- in –middle attack, replay, modification, packet dropping, tracker, flow analysis, selfishness, Daniel of service attacks [8]. Zhang et al focused on application layer attack.

That now the packet hijacked and replaced by the false one like Trojan horse attack, virus attack, malware attack. These can be removed by the updating of the anti-virus and window defender [9]. Chang -chi –Lee, Chia-Hsin-Liu and Min-Shiang-Hwang gives the information in his research about the guessing of attacks on strong password authentication protocol. They focused on his research to guess on attacks by OSPA protocol. OSPA protocol is vulnerable to guessing attacks. OSPA protocol consists two phase

1. Registration phase.
2. Authentication phase. [10]

## IV. Review Of Paper

We have studied here categories of cryptography i, e Symmetric and Asymmetric. But our main focus is on Asymmetric key cryptography also. We have also studied the RSA algorithm, Diffie-Hellman algorithm and their problems with examples.

Cryptography is most important part of securing a message before delivery. We have studied about various cryptographic techniques, to defend the attacks on the security of the message. We have also studied about the various attacks occurs on the Node, Network and Transmissions packets.

## REFERENCES

[1] Stalling William on ,” cryptography and network security”.

[2] Behroaz A.Forouzan on,” Data Communication and networking”.

[3] Paul C. Kocher “Asymmetric algoritms and other systems using various timing attacks”.

[4] Charles P.Pflegger, Shari Lawerence Pflegger “security in computing” 2007.

[5] Sumedha Kaushik and Ankur Singhal “network security using cryptographic techniques” International journal of advanced research in computer science and software engineering. Vol. 2 ISS-12, Dec. 2012.

[6] Punita Meelu and sitender Mali ”AES asymmetric key cryptographic system,” International journal of information technology 2011.

[7] Sanchez- Avila, C.Sanchez-Reilllol, R ”comparison between AES and DES,” 35th International conference on security technique 2001.

[8] Pflegger and lawerence “various attacks” 2007.

[9] Zhang et al “Detection for Application on Level Attacks” proceeding of 2007.

[10] Cheng-Chi-Lee, Chia-Hsin-Liu and MinShaiang Hwang “guessing of attacks on strong password and authentication protocol”.