ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Public Key Cryptosystems (Research Paper)

Prof. Saroj Singh
Dept. Computer Science & Engineering
Delhi Engineering College
Ladiyapur, Faridabad, India

Abstract: Public key cryptosystems came into force because of the problems associated with symmetric encryption. Plaintext, encryption algorithm, public and private key, decryption algorithm and ciphertext are five components of a public key cryptosystem. The more likely way for the world to be destroyed. Most experts agree is by accident. There is where we come in; we are computer professional: we cause accidents, by Nathaniel Borenstein

Keywords: symmetric; algorithm; cipher; message; cryptosystems; decryption; encryption;

I. INTRODUCTION

Public key cryptosystems came into force because of the problems associated with symmetric encryption.[1] There are :

- Key distribution requires that the two communication parties should already share a key which has been distributed to them.
- It provides no protection against forgery.

Components of public key cryptosystems: there are five components of a public key cryptosystem:

1. Plaintext: It is readable form of the data and is fed into an algorithms input.
2. Encryption algorithm: These algorithms perform various computations on the plaintext data.
3. Public and private keys: These are the selected pair of the keys which are used for encryption and decryption process. One is used for encryption process and another is used for decryption process.
4. Ciphertext: This is the encrypted form of plaintext which is provided as output. It depends upon the key used. Two different keys will give you different two outputs.
5. Decryption algorithm: It takes as input the ciphertext and matching key and produces plaintext as output.

A. Encryption Process

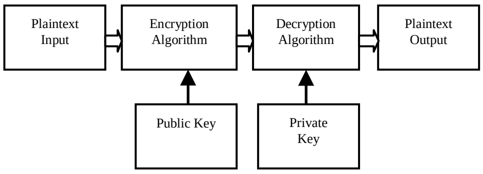

Fig: 1

B. Authentication Process

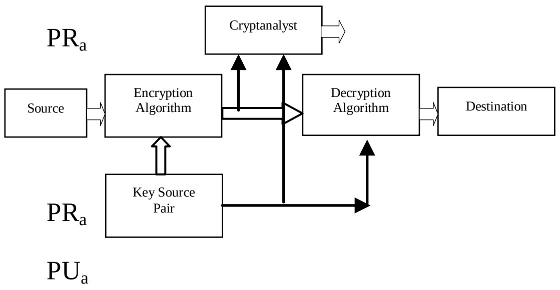

Fig: 2

C. Authentication and Secrecy

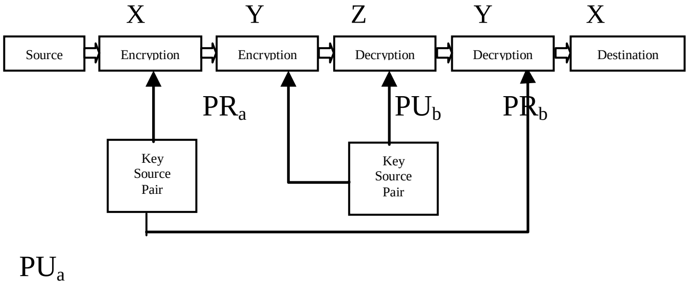

Fig: 3

D. Applications:

Depending upon the applications the user sender either:

- Sender's private key
- Receiver's public key
- Both the Sender's private key and Receiver's public key

The applications can be summarized as follows:

1. Encryption/Decryption: sender encrypts the message with the receiver's public key.
2. Digital signature: Sender signs a message with the private key. Cryptographic algorithms are applied.
3. Key exchange: Session key is exchanged with the help of different approaches.

E. Advantages:

•

nly the private key must be kept secret.

•

epending upon the mode being used private – public key pair can be remaining unchanged for a large amount of time.

•

fficient digital signature mechanism

•

n a large network less number of keys are used

F. Disadvantages:

- Public key scheme is not secure.
- Large key sizes.

II. DIFFIE HELLMAN KEY

Diffie Hellman key exchange was developed by Diffie and Hellman[2] in 1976. This method is one of the earlier methods of exchanging keys in the field of cryptography.

Definition: it allows two parties to exchange the secret key over an insecure medium. The two parties may not have any prior knowledge about each other.

A. Key Exchange Protocols:

- User A wishes to set up a connection with user B.
- User a uses a secret key to encrypt the messages that are to be send on the network connection.
- User A can generate one time key X_A and calculate Y_A and sends to user B.
- User B responds by generating a private value X_B and calculates Y_B and sends it to the user A.
- Both users can now calculate the key.

B. Algorithm: Suppose that there are two users to exchange a key namely A and B.

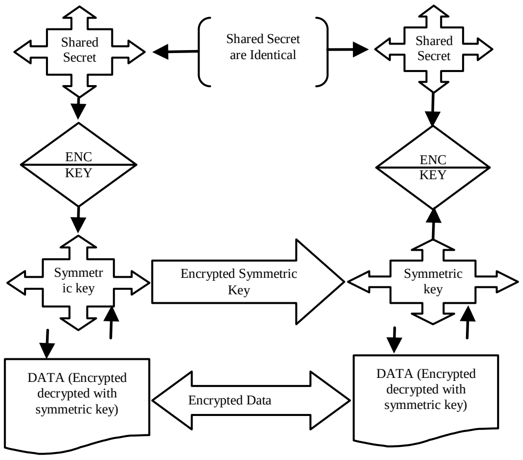
Shared Secret
Shared Secret are Identical
Shared Secret
ENC KEY
ENC KEY
Symmetric key
Encrypted Symmetric Key
Symmetric key
DATA (Encrypted decrypted with symmetric key)
Encrypted Data
DATA (Encrypted decrypted with symmetric key)

Fig: 4

- P and G are both publicly available numbers and P is at least of 512 bits.
- Users pick private values A and B and performs the following actions:

1. Compute public values
$x = g_a \bmod p$ and
$y = g_b \bmod p$
2. Public values x and y are then exchanged.
3. Compute shared private key
$k_a = y_a \bmod p$ and
$k_b = x_b \bmod p$
4. Algebraically it can be shown that $k_a = k_b$.

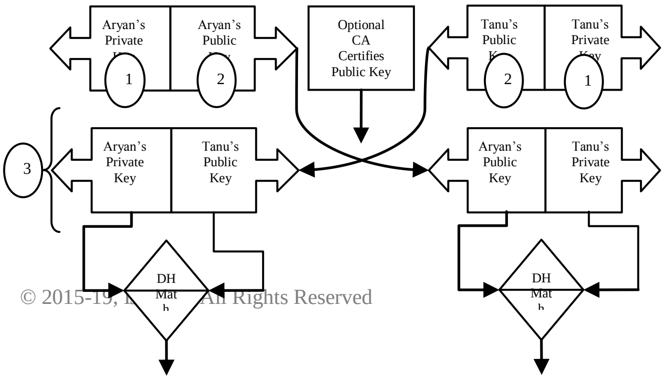

Fig: 5

C. Example

Two internet users namely Aryan and Tanu wish to have a secure conversation and decide to use the Diffie – Hellman protocol.

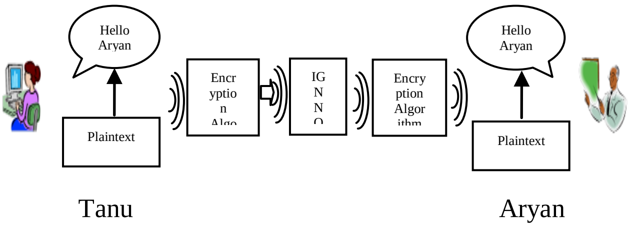

Fig: 6

- Aryan and Tanu gets public numbers
P=23 and G=9
- Aryan and Tanu compute Public values
X=94 mod 23=6561 mod 23=6
Y=93 mod 23=729 mod 23=16
- Aryan and Tanu then exchange public numbers.
- Aryan and Tanu compute symmetric keys.
$k_a = y_a \bmod p = 164 \bmod 23 = 9$
$k_b = x_b \bmod p = 63 \bmod 23 = 9$
- Aryan and Tanu can now talk in a secure manner.

D. Advantages:

- It provides a medium for variety of authentication protocols.
- It provides secrecy in transport layer security.

E. Disadvantages:

Diffie Hellman is used in many protocols like:

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Secure Shell (SSH)
- Internet Protocol Security(IPSec)
- Public Key Infrastructure (PKI)

III. KNAPSACK SYSTEMS

The Merkle-Hellman knapsack system is one of the earliest public key cryptosystems. This earliest public key cryptosystems was invented by Ralph Merkle and Martin Hellman in 1978.

A classic knapsack cryptosystem is constructed in the following ways:

- Find an easy knapsack problem.
- Transform this easy knapsack into a hard knapsack problem.
- Publish the hard knapsack.
- Construct the cryptosystem such that decryption is essentially different for the cryptanalyst and receiver.

A. Charactristics of a Knapsak System:

There are different characteristics of a knapsack system which makes them different from each other:

- Trapdoor one way function: it allows someone in possession of secret information to go backwords and compute the one-way function in inverse. Different knapsack cryptosystems use different one-way functions.
- Density of the cryptosystem: A cryptosystem density has a great effect on its vulnerability and decides whether it can be used to generate digital signatures for data origin authentication purposes or not
- Use of knapsack: these can be used for additive and multiplicative purposes.

B. Properties:

- Merkle-Hellman knapsack systems is an asymmetric key cryptosystem.
- Two Keys: Public and private keys are required for communication process.
- It is one way that means that the public key is used only for encryption process and private key is used only for decryption process.
- It is not used for authentication processes.

Merkle-Hellman knapsack systems is based on the subset sum problem.

C. Problem: NP-Complete

Given a set of numbers A and a number b. Find a subset of A which sums to b. If the set of numbers known as knapsack is super increasing then the problem is easy and can be solved in polynomial time.

a)Key generation in Merkle-Hellman Knapsack System: In Merkle-Hellman Knapsack systems the keys are known as knapsacks:

- Public key is a hard knapsack.
- Private Key is a super increasing knapsack.

The super increasing knapsack is combining with two additional numbers:

- Multiplier
- Modulus

Role of Modulus and Multiplier: Modulus and Multiplier has two functions-they are used to conert the super increasing knapsack into hard knapsack. They are used to transform are used to transform the sum of the subset of the hard knapsack into the sum of the subset of the easy knapsack.

D. Encryption:

Encryption is performed in the following steps:

- A subset of the hard knapsack is chosen by comparing it with the plaintext which is equal in length to the key.
- Each term in the public key that corresponding to a "1" in the plaintext is made an element if the subset.
- The terms corresponding to "0" in the plaintext are ignored.
- The elements of this subset are added together and the resulting sum is the ciphertext.

E. Decryption:

Decryption is performed in the following steps:

- Multiplier and modulus are used transform the number that represents the ciphertext into a sum of corresponding elements of the super increasing knapsack.
- Greedy algorithm is then used to solve the simple greedy algorithm. O(n) arithmetic operations are used to decrypt the message.

Advantages:

- Merkle – Hellman knapsack systems offers high speed.

Disadvantages:

- It is not suitable for generating digital signatures.

F. Graham-Shamir Cryptosystem

It is used to remove the disadvantages of the Merles-Hellman Cryptosystem. Here structured numbers whose low-order parts are in a super increasing sequence and whose higher order parts are random bits of strings are used[3].

G. Mori-Kasahara Cryptosystem:

- Morii-Kasahara cryptosystem is similar to Merkle-Hellmanscheme that uses an easy multiplicative knapsack.
- The Morii-Kasahara cryptosystem uses two multiplicative knapsacks respectively. These are easy and hard knapsacks.

H. Chor-Rivest Cryptosystem:This is the most popular cryptosystem that has withheld attacks for many years. The major disadvantage of this system is that it requires much time for generating large keys.

Evaluation of knapsack cryptosystems

Knapsack cryptosystems are evaluated in two terms:

- Security
- Efficiency

The NP completeness of the general knapsack problem offers high speed.

IV. Elliptic curve based systems

Elliptic curve systems were suggested by Neal Koblitz and Victor S Miller in 1985[4].

Definition: Elliptic curve cryptography is an approach to public key cryptography. This approach is based on the structure of elliptic curves. These are analog of existing public key cryptosystems in which modular arithmetic is replaced by operations defined over elliptic curves.

Elliptic curves are mathematical constructions from the number theory and algorithmic geometry. These are defined over a field. The field may be real, relational or complex field.

A. Elements of an Elliptic Curve

Elliptic curve consists of elements (x,y) and must satisfy the equation:

$$Y^2 = x^3 + ax + b$$

A single element 'O' known as the point of infinity is also denoted. This point of infinity can be visualized as a point at the top and the bottom of every vertical line.

B. Security of an elliptic curve systems:

The attacks on elliptic curve systems brute-force attacks.

Applications: Used in integer factorization algorithms.

C. Disadvantages:

Similar key sizes and better performance.

Elliptic curve systems with a 160 bit key offers the same security like RSA systems and discrete algorithm systems which makes use of 1024 bit key.

They are faster than corresponding discrete logarithm based systems.

They are faster than RSA systems in signing and decryption.

Disadvantages:

-

hey are slower than RSA systems in signature verification and encryption process.

-

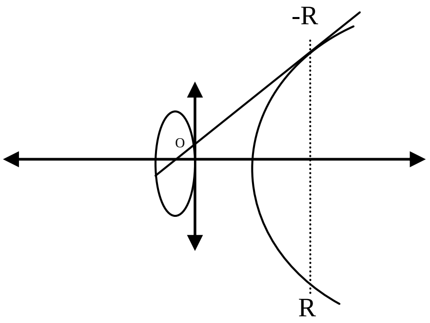

Fig:6

V. MAN IN THE MIDDLE ATTACK

Man in the middle attack < MITM>is also known as bucket bridge attack or Janus attack.

Definition: In this attack, an attacker makes independent connection with victims and relay message between them[5]. The attacker makes them believe that they are talking directly to each other over a private connection but the whole conversation is control by the attacker.

A. MITM Attacks MITM attack INCLUDE

- IP address of the server
- DNS name of the server
- X.509 certificate of the server
- Is the certificate self signed?
- Is the certificate signed by a trusted certification authority?
- Do other clients have the same certificate?
- Financial transaction systems

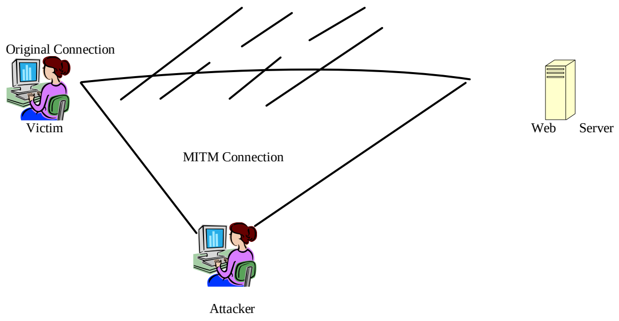

Fig: 7

A. Defenses Against the Attack:

Defenses against the MITM make use of authentication scheme. These are:

- Public key infrastructure
- Strong mutual authentication like secret keys and passwords
- Use of cryptographic hash function
- Secure channel verification
- Carry forward verification.

A. Non cryptographic man in the middle attack.

It would take over the HTTP connection periodically. Thus the traffic will not reach its destination and will itself respond to the intended server. The reply is sent in place of the web page that the user has requested.

B. Example

- Public key exchanging: MITM attacker may intercept the public key being exchange between the client and server. The attacker than modifies the key for malicious purpose
- Command injection: .MITM attacker hijacks and already authenticated session and then inject commands to the server and emulate fake replies to the clients.
- Malicious code injection: MITM attacker injects code into mails, SQL statement and web page.

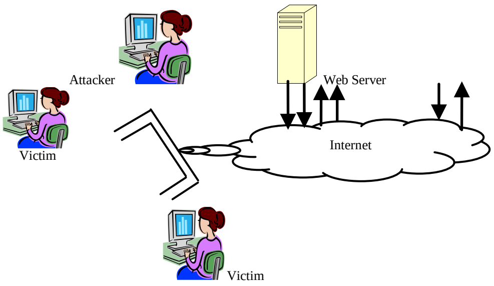

Fig: 8

- Downgrade attacks- SSH V2 TO VI: MITM attackers may force the clients to initiate a SSH 1 connection instead SSSH2. It forces the victim to use less secure feature and functions.
- Downgrade attacks- IPSEC failure: MITM attackers may obstruct the key material exchanged on UDP port 500 and the victim thinks that the IPSEC connection cannot be started on the other side.
- Down grade attacks-Point to Point Tunneling Protocol (PPTP): MITM attackers may force victim to use less secure PAP authentication. They can also steal passwords and repeat the attacks.

VI. MITM TECHNIQUES

MITM uses three techniques:

a)Local Area Network: it consists of:

- Address resolution protocol spoofing: Attackers uses ARP spoofing to shuffles data frames on LAN and then modify the packets.
- DNS Spoofing: The attacker starts sniffing the ID of any DNS server.
- IP Address Spoofing: the attacker creates forged source IP address to hide the identity of the packet sender.
- Spanning tree Protocol managing: Attacker is elected as the new root of the spanning tree.

b) From Local to Remote through a gateway:

- ARP Poisoning
- DNS spoofing
- Gateway spoofing
- ICMP redirection

c)Remote:

- DNS poisoning
- Traffic Tunneling
- Route Change

VII. MESSAGE DIGEST ALGORITHM(MD5)

Message digest algorithm designed by Ron Rivest in 1991 is a cryptographic hash function that produces 128 bit hash value.

A. MD5 algorithm: b bit message is provided as input.

- A message is padded so that its length is congruent to 448 modulo 512[6].
- Single "1" bit is appended to the message and the "0" bits are appended so that the length in bits equal 448 modulo 512.
- Length is appended. A 64 bit representation of "b" is appended to the result of the previous step.
- The result obtained has a multiple length of 512 bits.
- A four word buffer is used to compute the message digest. Let us say buffer is (A, B, C and D). This buffer is now initiated. Note that A, B, C and d are 32 bits registers.
- These registers are now initiated to the following values in hexadecimal:

i. word A: 01 23 45 67
ii. word B: 89 ab cd ef
iii. word C: fe dc ba 98
iv. word D: 76 54 32 10

- Process the message in 16 word blocks.

i. F (X,Y,Z): XY v not (X) Z
ii. (X,Y,Z): X v Y not (Z)
iii. H (X,Y,Z): X xor Y xor Z
iv. I (X,Y,Z): Y xor [X v not (z)]

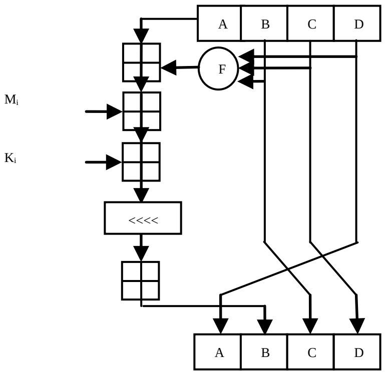

Fig: 9

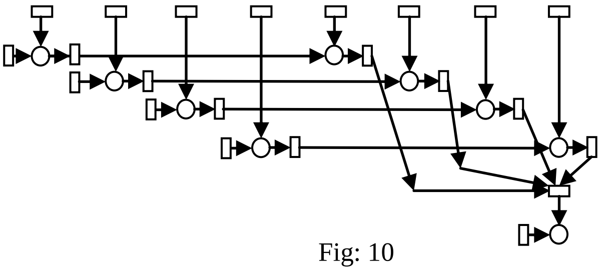

Fig: 10

- If the bits X, Y, Z are independent and unbiased then each bit of F(X, Y, Z), G(X, Y, Z), H(X, Y, Z), and I(X, Y, Z) are independent and unbiased.

B. Advantages: It is simple to implement.

C. Disadvantages:

i. It is not suitable for SSL certificates.
ii. It is not suitable for digital signatures.

D. Applications:

- It is used to check data integrity.
- It is used in the field of electronic discovery
- It is used to store passwords.

VIII. CAST 128

Cast -128 is based on the initial name of the inventors. Cast 128 was created in 1996 by Carlisle Adams and Stafford Traverse. It is also known as a cast 5 and is used as the default version in some versions of PGP[7].

Definition: CAST – 128 is a 12 or 16 round feistel network with a 64 bit block size. The key size ranges between 40 to 128 bits.

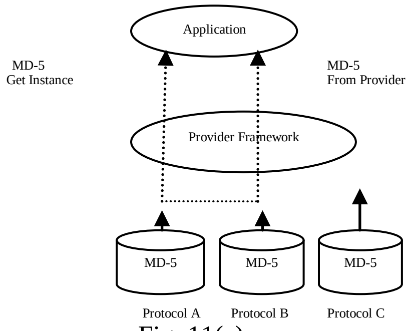

Fig: 11(a)

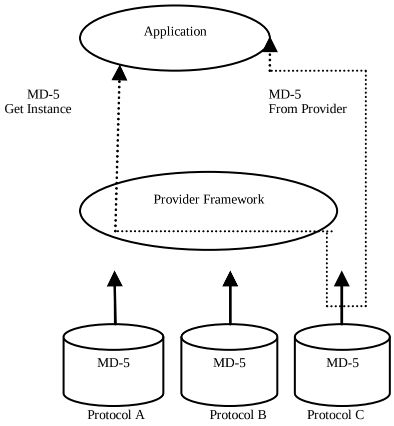

Fig: 11(b)

A. Components of CAST

Following are the components [8]:

- 8 x 32 bit S-Boxes
- Key Dependent Rotations
- Modular Addition
- Modular Subtraction
- XOROperation

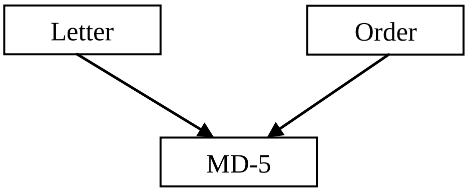

Fig: 12

Cast 128 consists of three alternating types of round functions. These round functionas are similar in structure and differs only in the choice of operation. i. e., Addition, Subtraction and XOR.

B. Cipher algorithm

Cast -128, a symmetric block cipher is used for securing encapsulating security payload (ESP). Here the block size is of 64 bits and the mode used IS CBC.

Key Size

Cast-128 is designed in such a manner that it can alloy key sizes from 40 bits to 128 bits.

The key size is incremented on-8 bits basis i.e.,40,48,56,64…..,128bits.

C. Case 128 Encrypted Algorithm

The encryption algorithm of cast -128 is explained with the help of four steps:

Input

The input of class-128 is:

a) Plaintext denoted by m, m2, m3….. m64.

b) Key denoted by k1,k2,….,k127,k128

Output

the output of cast of 128 is;

a) Cipher text denoted by c1,c2,…..,c64.

Step1: schedule: compute 16 pairs of sub keys (kmi,kri)

Where

a)kmi is used as masking key .

b) kri is used as rotation key.

Step 2 :Split the plaintext in to left and right 32 bit halves.

L_O=m1, m2........ m31, m32

R_O= m33, m34…....... m63, m64

(L_O, RO)= (m1, m2….....m64)

Step3 : compute Li and Ri (16 rounds of i from 1 to 16) as

Li = Ri-1

Ri = Li -1 ^ f (Ri-1,Km_j, Kr_j)

Step 4: Exchange the final blocks L16, R16 and concatenate to form the ciphertext.

(c1,…..,c64) ⇦ (R16,L16)

d. Payload

cast-128[9] requires an explicit Initialization vector (vi). The size of Initialization vector is of 8 octets. IV is randomnly generated for each packet and is used for encrypting the plaintext.

During the decryption process the first 8 octets of payload are used for Initialization vector to decrypt the remaining payload octets.

Subsititution Boxes:

Cast-128 makes use of eight subsititution boxes:

a)s1,s2,s3,s4 are rounds functions s-boxes.

b)s5,s6,s7,s8 are keys schedule S-boxes.

Performance

Cast-128 runs 3 time faster than the highly Optimized DES implementation. Cast-128 runs 5-6 times faster than the DES implementation Found in typhical applications.

Advantages:

a)cast-128 offers good resistance to linear cryptanalysis, differential cryptanalysis and related key cryptanalysis.

Uses:

a)these are worldwide on royality basis for commercial and non commercial purpose.

IX. E CAST- 256

Defination

Cast-256 is a block cipher whiceh was derived from cast-128[10].

It uses same elements as cast-128 and included S-boxes. Cast -128 is also known as 12 quad rounds.

The acceptable key sizes in cast-256 are 128,256,160,224or192 bits and are composed of 48 rounds.

X. IDEA(INTERNATIONAL DATA ENCRYPTION ALGORITHM)

A. Definition

Idea is a symmetric kind of block cipher using 52 sub keys. The plaintext is split into four separate 16 bit long quarters. Each sub key is of 16 bit.

B. How the bits are used?

In IDEA, two bits are used during each round and four bits are used before each round. After the completion four bits are again used. Thus idea consists of eight rounds. The designers of IDEA[11] are Xuejia Lai and James Massey.

C. Function

The two 16 bits values are brought together to produce a16 bit outcome.

D. Operators

a) Bitwise exclusive OR

b) Addition modulo to 2^{16}

c) Multiplication modulo to $2^{16}+1$

E. Subkey generation

Subkey generation of IDEA[12] can be explained in the following steps:

a) The 128 bit of IDEA is taken as the first eight subkeys: k(1) ……………k(8).

b) After the 25 bit circular left shift is done, next subkeys are obtained.

c) The whole process repeated space until all the subkeys are obtained.

F. Security

From various methods, it was included that it is immune under certain assumptions.

XI. REFERENCES

[1] William Stallings, “Cryptography and Network Security, principles and practices”, 4th Edition, March, 2007

[2] Keliher, Liam et al "Modeling Linear Characteristics of Substitution-Permutation Networks". In Hays, Howard & Carlisle, Adam. Selected areas in cryptography: 6th annual international workshop, SAC', 2000.

[3] Morris Dworkin , "Recommendation for Block Cipher Modes of Operation – Methods and Techniques", Special Publication 800-38A NIST, December 2001

[4] Van Tilborg, Henk C. A.; Jajodia, Sushil, eds. “Encyclopedia of Cryptography and Security” 2011 .

[5] William Stallings NIST Special Publication 800-57 Recommendation for Key Management — Part 1: General (Revised), March, 2007.

[6] ISO/IEC “Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher” 10118-2:2010

[7] ISO/IEC “Information technology — Security techniques — Modes of operation for an n-bit block cipher”, 10116:2006 .

[8] Cusick, Thomas W. & Stanica, Pantelimon “Cryptographic Boolean functions and applications”, 2009 .

[9] Matsui, M. and Yamagishi, A. "A new method for known plaintext attack of FEAL cipher". Advances in Cryptology - EUROCRYPT 1992.

[10] ISO/IEC 9797-1: “Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher”, ISO/IEC, 2011.

[11] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback, “Report on the Development of the Advanced Encryption Standard (AES)”, National Institute of Standards and Technology (NIST), October 2000.

[12] Junod, Pascal & Canteaut, Anne “Advanced Linear Cryptanalysis of Block and Stream Ciphers” , 2011.