UNIT 5 CRYPTOGRAPHIC ALGORITM

Mathematical Preliminaries

The combination of set of integers and the operations that are defined on the element of a set is called an algebraic structure.

1) Groups (G)

A group (G) is a set of elements with binary operation '.' that satisfies 4 properties –

i) Closure : If both a & b belong to same group G, then $a \cdot b$ is also element of G.
For $a, b \in G$, $a \cdot b \in G$.

ii) Associativity : If a, b and c belong to same group G, then
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

iii) Identity : For all G, there always exists an identity element e within the same group such that $a \cdot e = e = e \cdot a$

iv) Inverse : For each a in G, there always exists an inverse element 'a'' within the same group such that $a \cdot a' = a' \cdot a = e$

IF the operation is also commutative ($a * b = b * a$), the group is called an Abelian Group.

2) Rings

A ring is a set R, with 2 operations : addition (+) and multiplication (·) such that :

i) (R, +) is an Abelian Group.

ii) Multiplication is associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

iii) Distributive laws : $a \cdot (b+c) = a \cdot b + a \cdot c$
$(a+b) \cdot c = a \cdot c + b \cdot c$

3) Fields

A field is a F with 2 operations : addition (+) and multiplication (·), such that:

i) (F, +) is an Abelian Group

ii) $F - \{0\}$ is an abelian group under (·) multiplication

ie A field is a ring in which every non zero element has a multiplicative inverse, and multiplication is commutative.

Every field is a ring, but not every ring is a field.

4) Prime Numbers

It is a natural number greater than 1 that has no positive divisors other than 1 and itself. ie prime no. p can be divided evenly by 1 and p itself.

eg. 2, 3, 5, 7, 11 ...

Symmetric key algorithms

DES - Data Encryption Standard.

Operation of DES involves taking 64 bit block of P as input and transforming it into corresponding 64 bit of C (ciphertext) block.

Plain text input → 64 bits
Key input → 64 bits (8 bits are for parity)
IP (Initial Permutation) → 64 bits
Subkey for each round → 48 bits
E-box → 32 bits ⇒ 48 bits
S-box input → 48 bits (8 blocks of 6 bits each)
S-box output → 32 bits
P-box → 32 bits
FP → 64 bits.

Step1 Initial Permutation (First Shuffle)
The 64 bit P is rearranged according to a fixed pattern. No bits are lost, just their positions change.

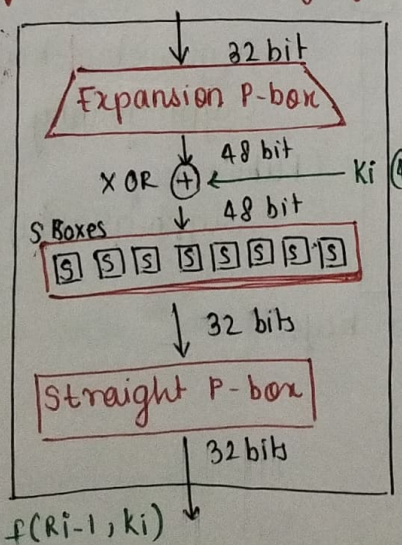
Step 2 After IP, divide it into two 32-bit halves:
Left half (L0) - 32 bits
Right half (R0) - 32 bits

Step3 DES applies 16 rounds of processing.
In each round: the left part of next round becomes right part of previous round. $L_i = R_{i-1}$
: the new right part is XOR of the left part & the f-function applied on the right part & a round specific key. $R_i = (L_{i-1}) \oplus f(R_{i-1}, K_i)$

Step4 After 16th round, the two halves are swapped.

Step5 Final Permutation (IP^{-1})
Another rearrangement of bits. Results in 64 bits ciphertext.

♥ DES Function (f-function)



The f-function has 4 steps

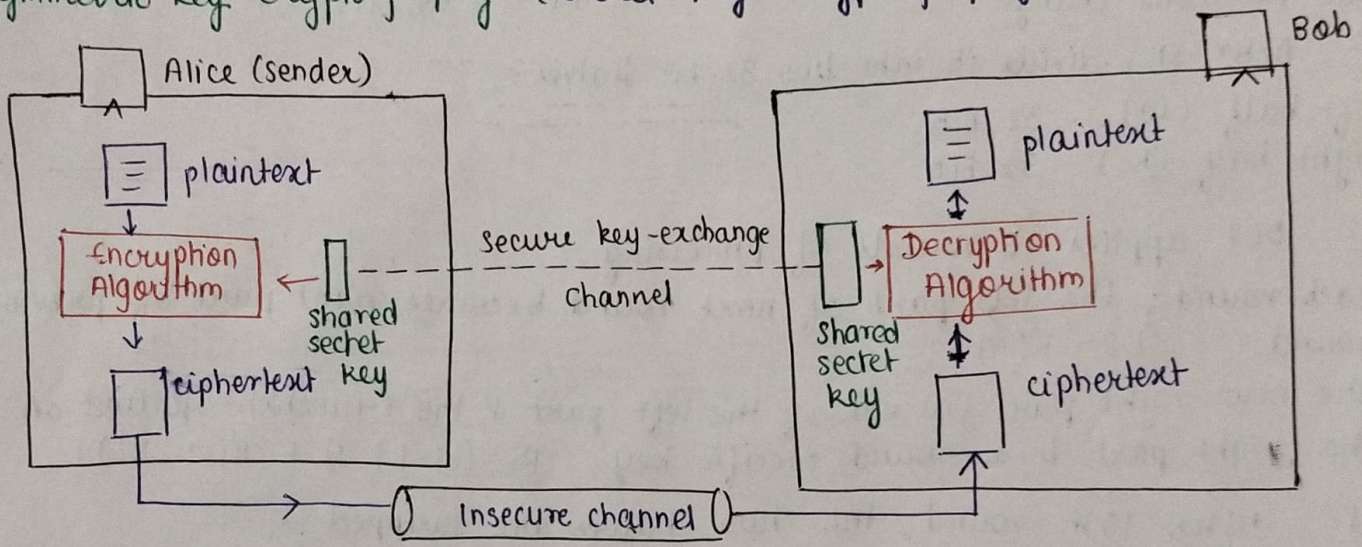
1) Expansion - Expands 32 bits to 48 bits by repeating some bits based on fixed table.
2) XOR with Round key - The 48 bit expanded block is mixed with 48 bit round key using XOR.
3) Substitution (S-Boxes) - 8 S-boxes, each takes 6 bits and outputs 4 bits. (6x4 = 32) This reduce 48 bits back to 32 bits.
4) Permutation (P-Box) - Rearranges the 32 bit for more mixing.

Cryptography ? It is the practice and study of techniques for secure communication in the presence of malicious behaviour. It involves converting plaintext into ciphertext to prevent unauthorized access.

Encryption It is the process of converting plain text into cipher text using an algorithm and a key, so that only authorized users can read it. It hides the original information and protects it from being understood by anyone who doesn't have the key.

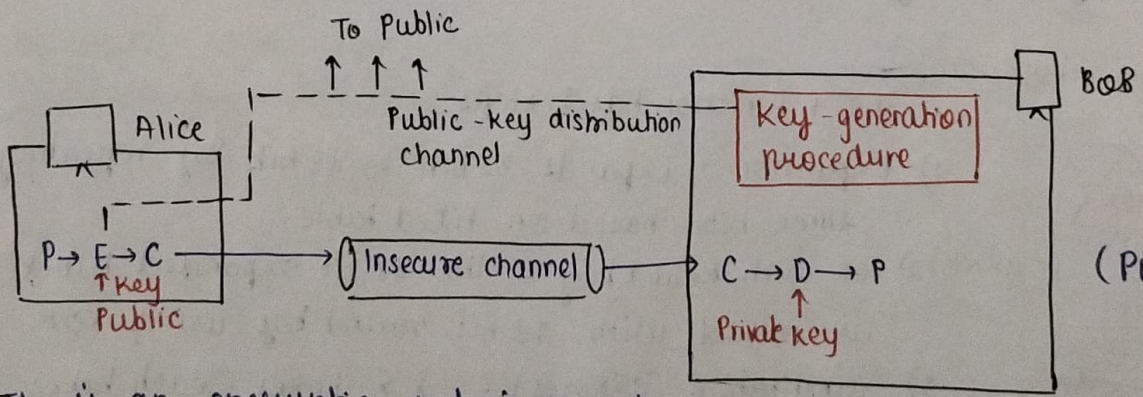
Decryption It is the process of converting cipher text back into plain text using a key, so the original message becomes readable again.

Symmetric key cryptography (secret key cryptography)



It is an encryption technique where the same key is used for both encryption and decryption of data.

Eg. AES, DES, RC4



Asymmetric-key cryptography (Public key cryptography)

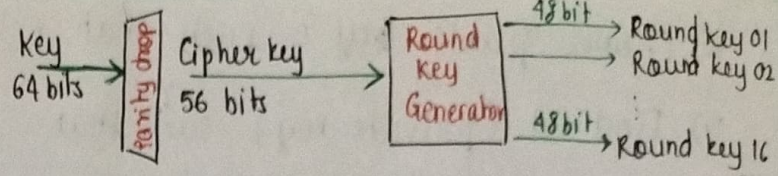
It is an encryption technique, that uses 2 different keys:

a public key for encryption &

a private key for decryption

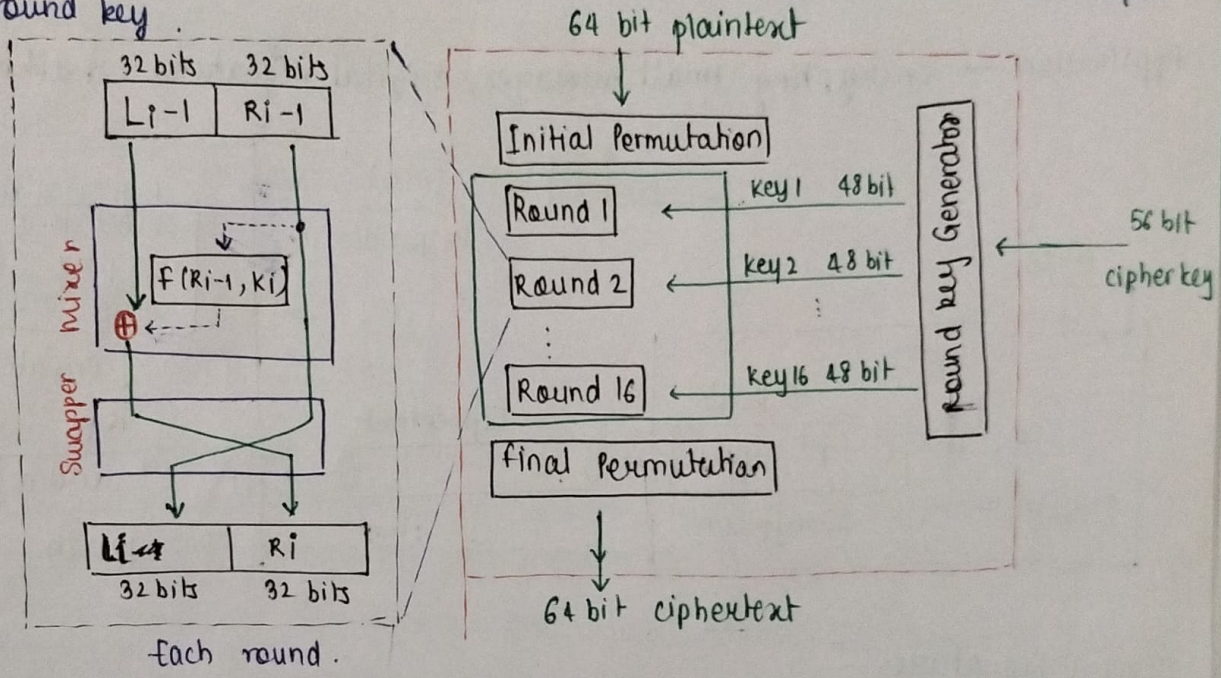
Eg. RSA, Diffie-Hellman, ECC

Key Generation (for 16 Rounds)



Start with 64 bit cipher key.
Drop 8 parity bits → get 56 bits.
These 56 bits are processed to create sixteen 48 bit round keys
: Apply Permutation.
: Split it into two 28 bit halves.
: Shift left by 1 or 2 (depending on the round).
: Combine halves → compress 48 bit using table
Result is 16 different round keys (K1 to K16). Each round uses its own unique 48 bit round key.

compression



Advanced Encryption Standard (AES)
It is a symmetric key block cipher. It is successor of DES. It is faster, more secure, and works on large key sizes.

> Public key Encryption and Hash function.

RSA - (Rivest, Shamir and Adleman) Cryptosystem.
It is a public key (asymmetric) cryptosystem.
It uses two keys : Public key (e, n) for encryption.
Private key (d) for decryption.

Working of RSA:
1) key Generation : i) Choose two large prime numbers p & q of equal lengths.
ii) calculate $N = p \times q$ and $\phi = (p-1) \times (q-1)$

iii) Choose public key 'e' such that e & ϕ are coprime (ie have 1 as common factor)

iv) Find 'd' (private key) such that

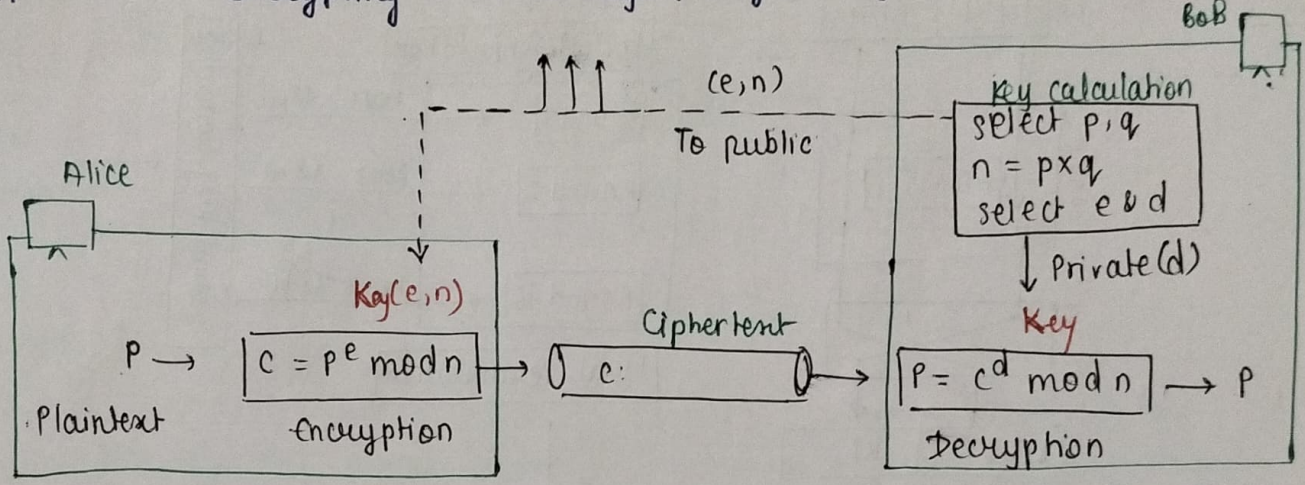
$$(e \times d) \bmod \phi = 1 \qquad d = e^{-1} \bmod \phi$$

v) Public key = (e, n) & Private key = (d, n)

2) Encryption : $C = P^e \bmod n$

3) Decryption : $P = C^d \bmod n$

Application → encrypting small messages, Digital Signatures, Authentication



Digital Signatures

Another way to provide message integrity and message authentication

Digital signature uses a pair of private - public keys.

When sender wants to send message to Receiver :

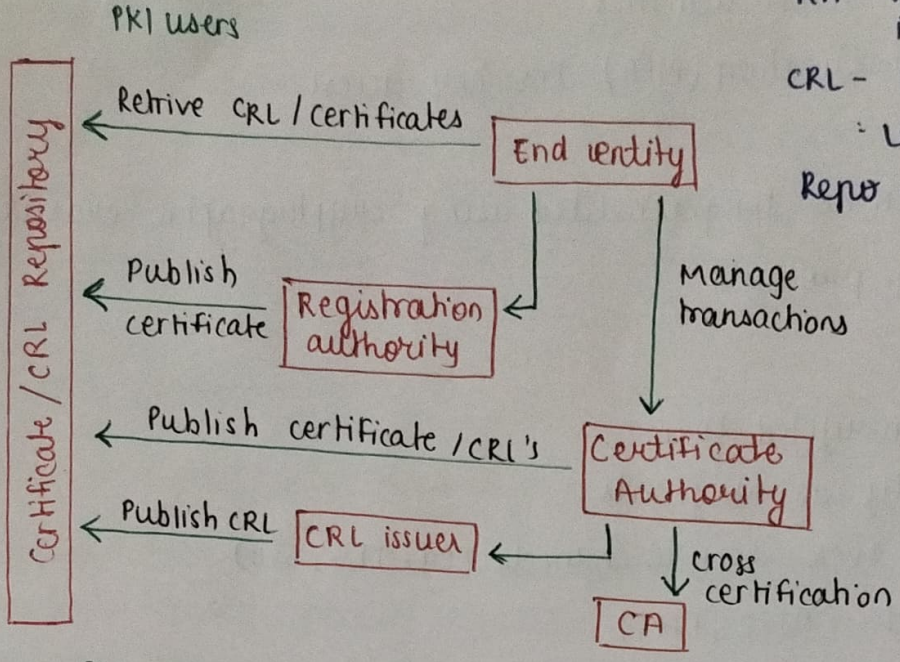
- Sender signs the message using her private key.
- Receiver verifies the signature using sender's public key.

Services provided by Digital Signatures :

1) Message Authentication - sign proves who send it.
2) Message Integrity - any change breaks the signature.
3) Non-repudiation - possible when Trusted Third Party is involved. The trust center saves the message, the identities, the signature & a timestamp. If Alice denies later, the trusted center has proof.
4) Confidentiality is not provided. (needs encryption separately)

Diagram:

CA - Issues & signs digital certificate
RA - Verifies identity before certificate issuance.
CRL - Certificate Revocation List : Lists Revocked certificates
Repo - storage area



PKI management entities

Private key Management

- One of the most critical points of security failure in private key encryption is the management and protection of cryptographic keys.
- Private keys must be protected ; compromise leads to exposure of all encrypted data. Keys needs to be stored and sometimes transmitted securely.

Best Practices -

1) Secure storage :
- Use Hardware Security Modules (HSMs), smart cards or encrypted file systems.
- Ensure physical and logical security
- Restrict access to authorized personnel only.
- Implement separation of duties

2) Key Rotation :
- Rotate keys regularly to reduce risk exposure.
- Automate rotation where possible.
- Re-encrypt data with new keys after rotation.

3) Access Control :
- Limited access strictly to authorized users.

- Use Role Based Access Control (RBAC).
- Monitor and log all key access activities.
- Employ Multi-factor Authentication (MFA) for key access.

4) Key Destruction:
- Securely destroy keys when no longer needed using cryptographic erasure.
- Audit and log destruction process.

5) Backup and Recovery:
- Backup keys securely in encrypted form.
- protect backup as rigorously as originals.
- Transmit ~~chann~~ keys only over secure channels (eg. TLS, SSH)
- Follow compilance standards (NIST, FIPS)

Effective private key management involves secure storage, regular rotation, strict access control, and secure destruction of keys. These practices protect sensitive data from unauthorized access and maintain the integrity of cryptographic systems.

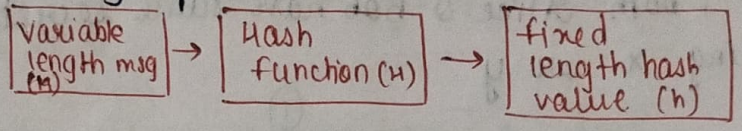
Hash function

A cryptographic hash function takes any size of message and shrinks it into a fixed size digest.

It uses a smaller building block called a compression function to handle small fixed sized inputs

Compression function = Takes bigger chunks & compress it into smaller fixed size pieces.

Eg · MD2, MD4, MD5



> Digital certificates and Public key infrastructure.

Digital certificate - It is an electronic document issued by a trusted third party (called a Certificate Authority) that proves the ownership of a public key by binding it to the identity of an individual, organization, or website. It ensures secure communication by enabling authentication & encryption.

Key generation → Registration → Verification → Certificate creation

Types: Email, Server Side SSL, Client Side SSL, Code signing

Diffie - Hellman key Exchange -

The main aim is to allow 2 parties to securely create a shared symmetric key (same key) over an insecure channel - without using a key Distribution center (KDC) and without exchanging private keys

Algorithm:

i) select 2 public integers p and g (where p is prime and g is base of p ie primitive root modulo p)

ii) Alice chooses a secret random number x (kept private)
Bob chooses a secret random number y (kept private).

iii) Alice calculates $R_A = g^x \bmod p$ and sends R_A to Bob

Bob calculates $R_B = g^y \bmod p$ and sends R_B to Alice.

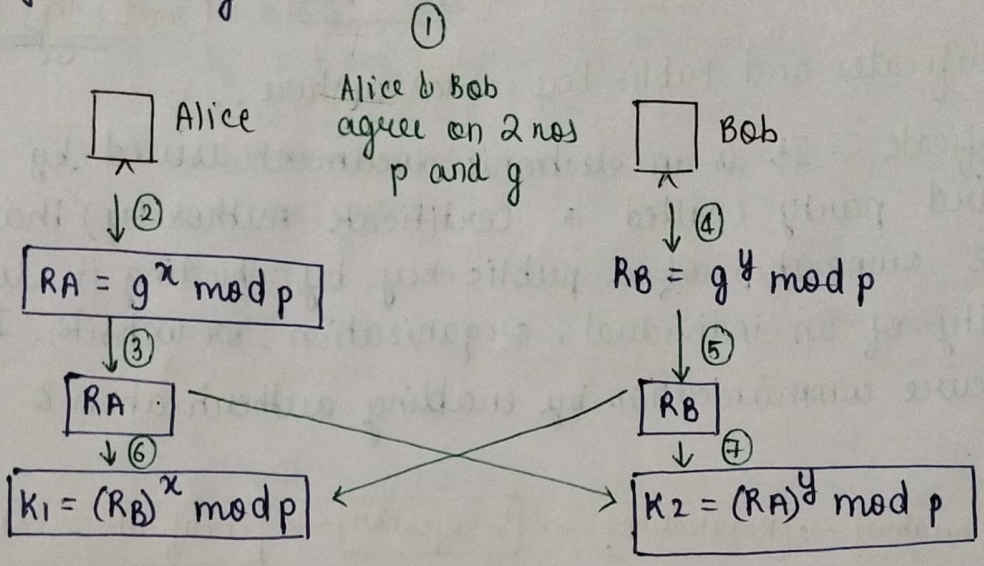
iv) Now, Alice uses R_B to calculate shared key

$$K = R_B^{\,x} \bmod p$$

Bob uses R_A to calculate shared key

$$K = R_A^{\,y} \bmod p$$

v) Now, both Alice & Bob have same secret key 'K' without ever sharing x or y



As it turns out $K_1 = K_2 = K$.

K is shared symmetric key bet^n Alice & Bob.

Disadvantages

Vulnerable to Man in the Middle ~~Attacks~~
No Authentication
Computationally expensive - Requires very large nos, which can be slow.
Exposed key exchange.

Public key Infrastructure X.509
It is a framework for using digital certificates in a secure way.
It uses X.509 certificates, which are files that confirm someone's identity and contain public key.