DATE
PAGE

CRYPTOGRAPHY & NETWORK SECURITY

★ Security Principles / Security Goals : C I A

1. Confidentiality = term used to define the prevention of disclosure of information to unauthorized individuals or systems.
   - it specifies that only sender and the recipient should be able to access the contents of a message. - protect message content.

2. Integrity (protect info accuracy)
   - means there is resistance to alteration or substitution of data, and/or that such changes are detected and provable.
   - info should not be changed, except by an authorized agent.
   - receiver of a message should be able to check whether info is changed or not. - change is detectable, provable - error control.

3. Availability (ensure info delivery)
   - availability of information resources - provides assurance that info is accessible when needed, by those who need them.
   - prevents service disruptions, denial of service etc.

★ Security Services - defines a security service as a service provided by a protocol layer of communicating open system, which ensures adequate security of the system, or of data transfers.

- service provided by protocol layer of comm. sys. that ensure security of system & data transfer

5 categories :-
1. Data confidentiality
2. Data Integrity
3. Authentication
   - ↳ Entity authentication
   - ↳ Data origin authentication
4. Non-repudiation - prevents denial of participation.
5. Access control.
   - ↳ protection against unauthorized access of resources.

C I A N A

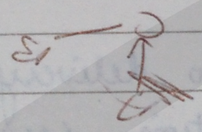
DATE
PAGE

action that compromises security of info.

* Security attack = any action that compromises the security of information owned by an organization is termed as a security attack.
- can happen either at application level or network level.

Security Attacks

Active attacks	Passive attacks
1- Masquerade	traffic analysis
2- Replay	release of message contents
3- Modification of message	
4- Repudiation	
5- Denial of service	
threat to integrity	threat to confidentiality
threat to availability	



Passive attack = attacker only reads messages, but does not alter them. - only observation, no modification.
- attacker monitors unencrypted traffic and looks for clear text passwords and sensitive info that can be used in other attacks.
- results in disclosure of info/data files to an attacker without the consent and/or knowledge of the user.

Active attack = attacker tries to bypass or break into secured systems. - include attempts to break protection barriers, introduce malicious code etc.
- results in disclosure and/or dissemination of files.
- info is altered, sequence/order of comm. disrupted.

DATE
PAGE

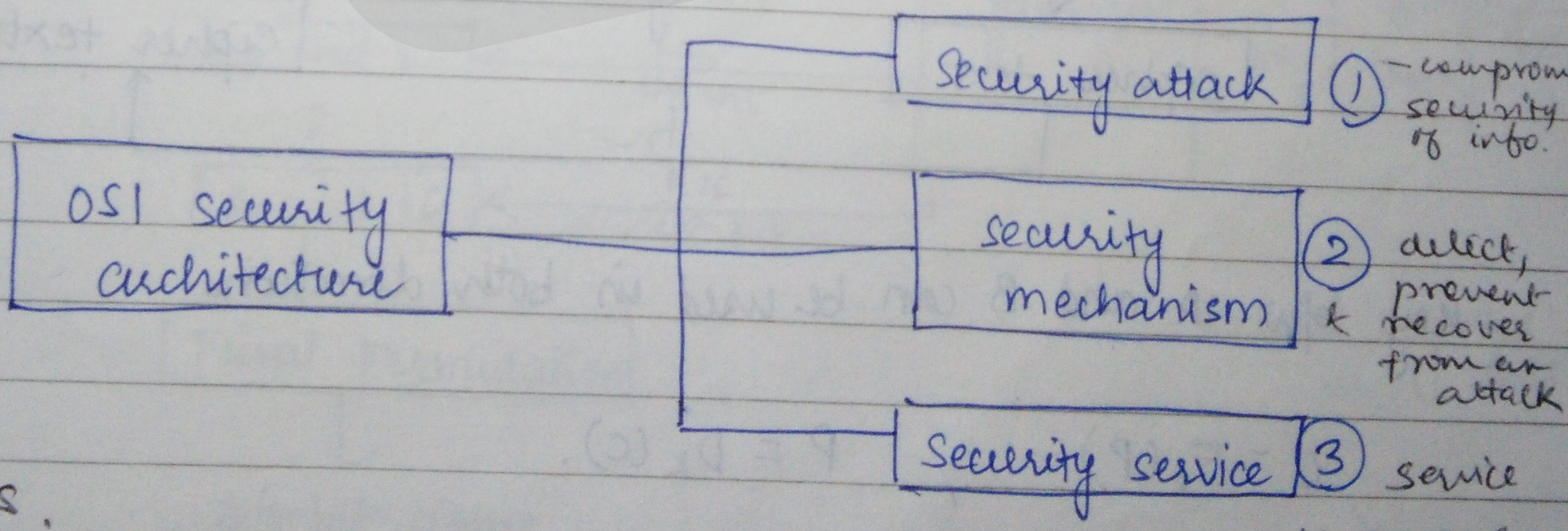
→ Cryptography - science of using mathematics to encrypt and decrypt data.
store, transmit securely.
- enables user to store sensitive info, transmit it across insecure networks (eg. Internet) such that it cannot be read by anyone except the intended recipient.
- a cryptographic algorithm works in combination with a key to encrypt the plaintext. - key used to encrypt plaintext.

→ Plain Text = original message or data which we have to send.
→ Encryption = process of transforming information (plain text) using an algorithm to make it unreadable to general public, third parties except sender and receiver. plain text x algo = cipher text.
→ Decryption = process of extracting the original info from the encrypted data, i.e. to make the information readable again.

→ Cryptanalysis = technique of decoding cipher text into plain text without the knowledge of how it was initially encrypted, i.e. cryptanalysis is the process of deciphering secret codes.
cipher → plain text

* OSI security architecture - OSI provides a useful abstract overview of security attacks, mechanisms and services.

threat = potential for violation of security which exists when there is a circumstance/event that could cause security breaches.



AIMS.

DATE
PAGE

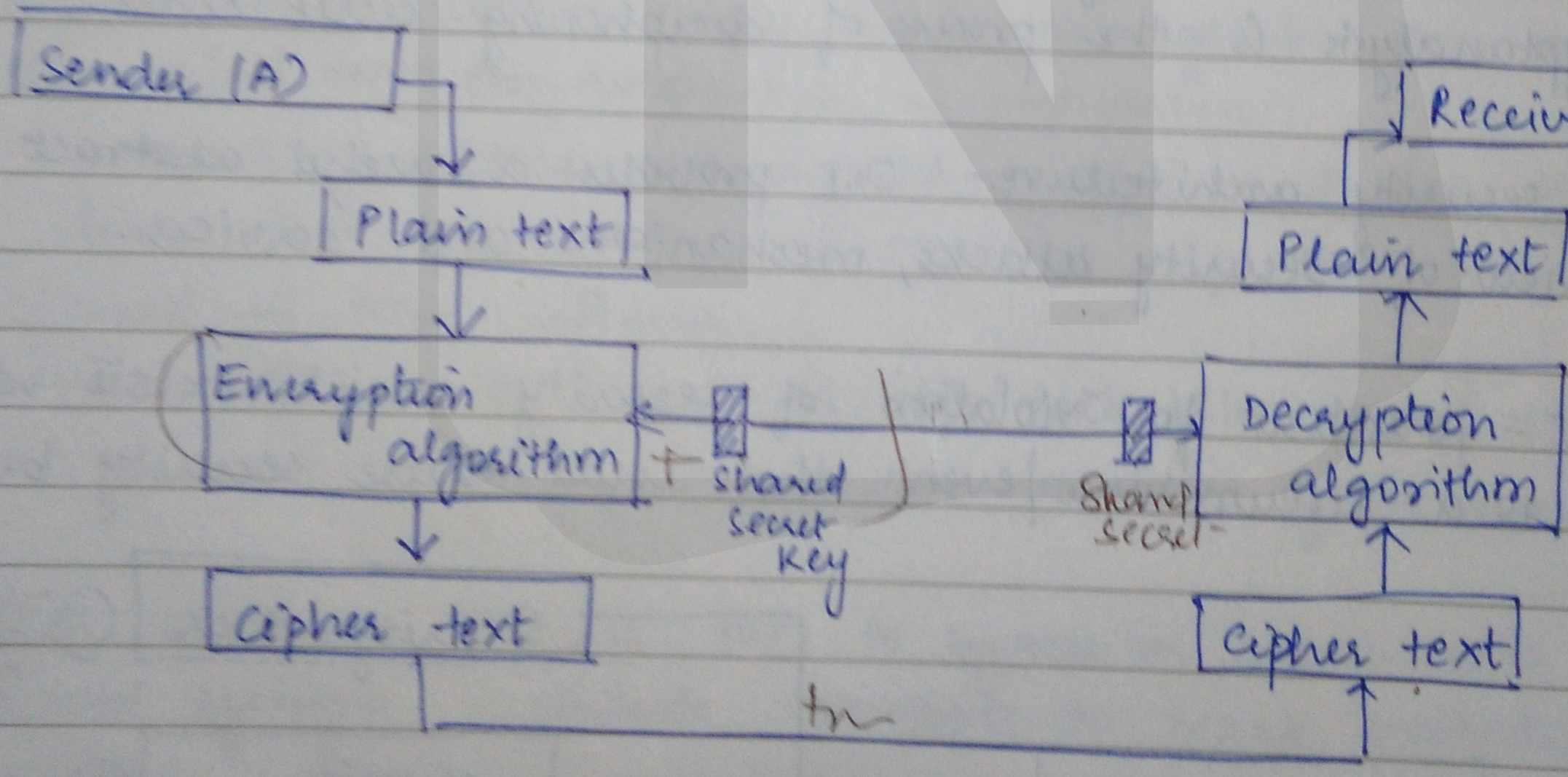
① any action that compromises the security of info owned by an organization.

③ process that is designed to detect, prevent, and/or recover from a security attack.

④ a processing or communicating services that enhances the security of the data processing systems and the info transfers of an organization. - intended to counter security attacks.

ener, decr done using same key.

Symmetric Key Cryptography - form of cryptosystem in which encryption and decryption are performed using the same key.
- to create the cipher text from plain text, sender uses an encryption algorithm and a shared secret key.
- to decrypt the message, receiver uses the same secret key.



key b/w A and B can be used in both directions.

$C = E_K(P)$, $P = D_K(C)$.

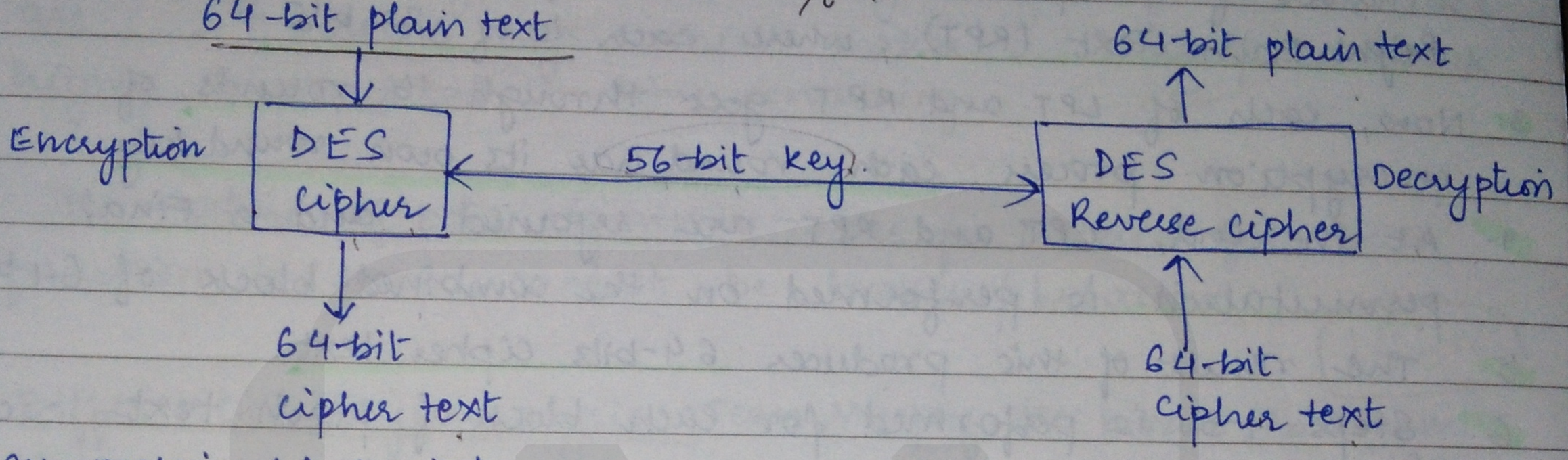
DATE

→ if there are n users, no. of keys required = $\frac{n*(n-1)}{2}$.

$n(n-1)/2$.

* Data Encryption Standard (DES) (1976)

128/64 --

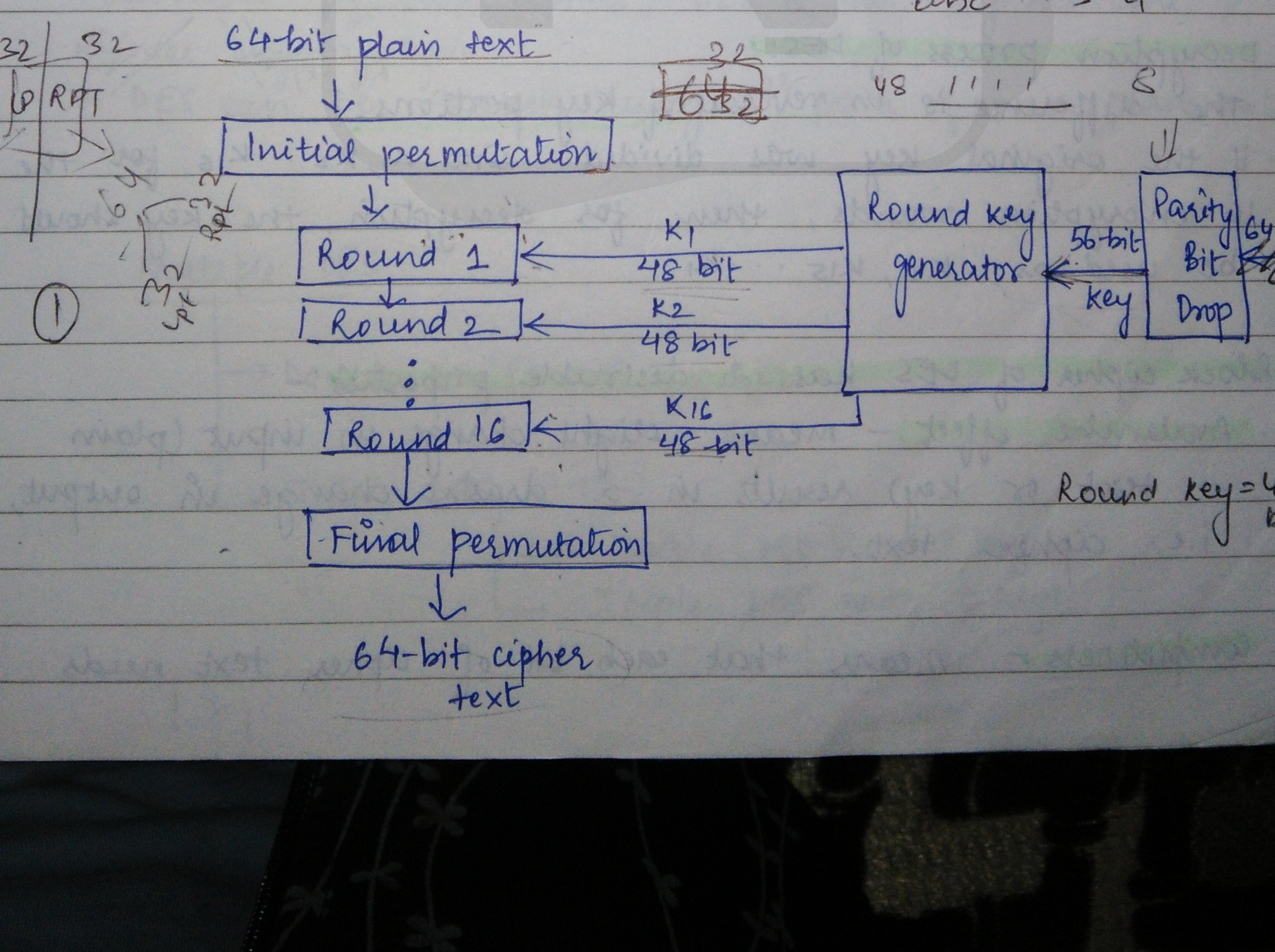


- symmetric block cipher
- developed by IBM, approved by NSA.
- uses the same binary key to encrypt and decrypt data blocks.
- operates on 64-bit data, processes it under a 56-bit key.
- DES uses a sequence of primitive operations called "round" to encrypt a data block. - 16 rounds used.

- 64-bit data, 56-bit key.
- rounds = 16.

#Encryption process of DES:-

abc → d

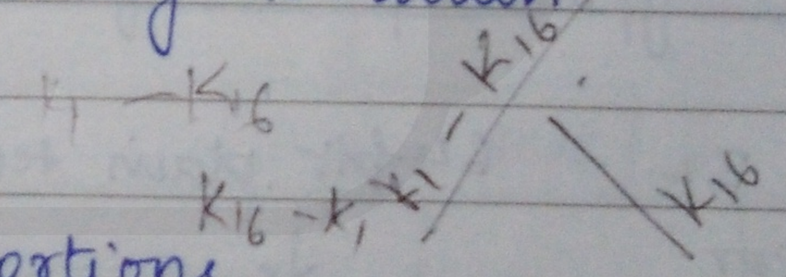


1. Messages divided into blocks of 64 bits
2. Initial permutation - LPT & RPT, 32 bits each
3. 16 rounds - each has its own key.
4. LPT & RPT combined
5. Final permutation → cipher for that block.

Steps:-

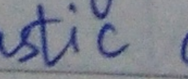
1. Plain text is broken into blocks of 64-bits. Encryption is done block-wise.
2. A block first goes through an Initial Permutation, which produces 2 halves of the permuted blocks - Left Plain Text (LPT) and Right Plain Text (RPT), where each is of 32 bits.
3. Now, each of LPT and RPT goes through 16 rounds of encryption process, each round has its own round key.
4. At the end, LPT and RPT are rejoined, and a Final permutation is performed on the combined block of 64-bits.
5. The result of this produces 64-bits cipher text.
6. Steps 1-5 is performed for each block of plain text, each of size 64-bit.
7. All cipher text are combined to form cipher text of complete message.

4 main parts of DES:-
1. Initial Permutation
2. Rounds
3. Final Permutation
4. Round Key Generation



* Decryption process of DES:-
The difference is in reversal of key portions.
- if the original key was divided into $K_1, K_2 \cdots K_{16}$ for the 16 encryption rounds, then for decryption, the key should be used as $K_{16}, K_{15} \cdots K_1$.

* Block cipher of DES has 2 desirable properties:-
1. Avalanche effect - means slight change in input (plain text or key) results in a drastic change in output, i.e. cipher text.



2. Completeness - means that each bit of cipher text needs

DATE
PAGE

to depend on many bits in the plain text.

* Strength of DES:
1. Use of 56-bit keys — 56 bit
are 2^{56} possible keys, which makes a brute-force attack highly impractical, time consuming. 2^{56}

2. The nature of DES algorithm — design criteria for DES function is secure, cannot be broken/breached.

→ Differential cryptanalysis: Eli Biham, Adi Shamir (1990)
← first published attack that is capable of breaking DES in less than 2^{55} complexities.

← this scheme can successfully cryptanalyze DES with an effort on the order of 2^{47} encryptions, requiring 2^{47} chosen plain text. — monitors how change in input affects change in output — finds patterns/non-random behavior & exploits them

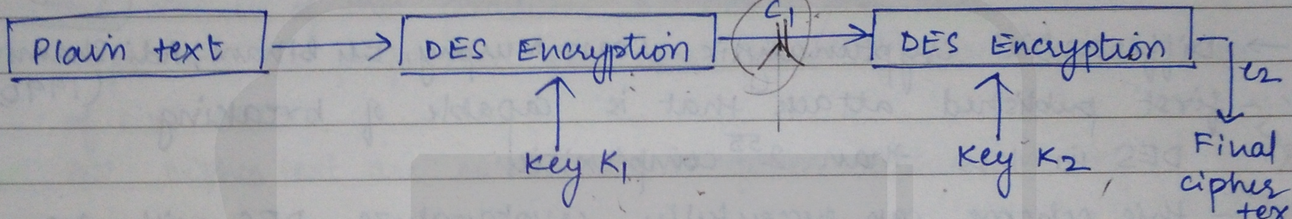
→ Linear Cryptanalysis: based on finding affine approximation to the action of a cipher. plain
- developed for block ciphers, DES is not very resistant to linear cryptanalysis.
- DES can be broken using 2^{43} pairs of known plain texts

Multiple DES
→ Double DES (2-DES) K_1 K_2
→ Triple DES (3-DES)
→ Triple DES with 3 keys
→ Triple DES with 2 keys.

DES — 6x2 — DATE PAGE

* **Double DES:-** - does twice of what DES normally does once.
  - uses 2 keys, K_1 and K_2.
  - first performs encryption on the original plain text using K_1, to get cipher text C_1.
  - Again performs DES on C_1 using key K_2 to obtain cipher text C_2.

$$P \rightarrow E(K_1, P) \rightarrow E(K_2, E(K_1, P)) = C$$



Meet-in-the-middle attack on 2-DES:-
- renders it useless
- attacker tries to break from both directions, i.e. from P to C and C to P.

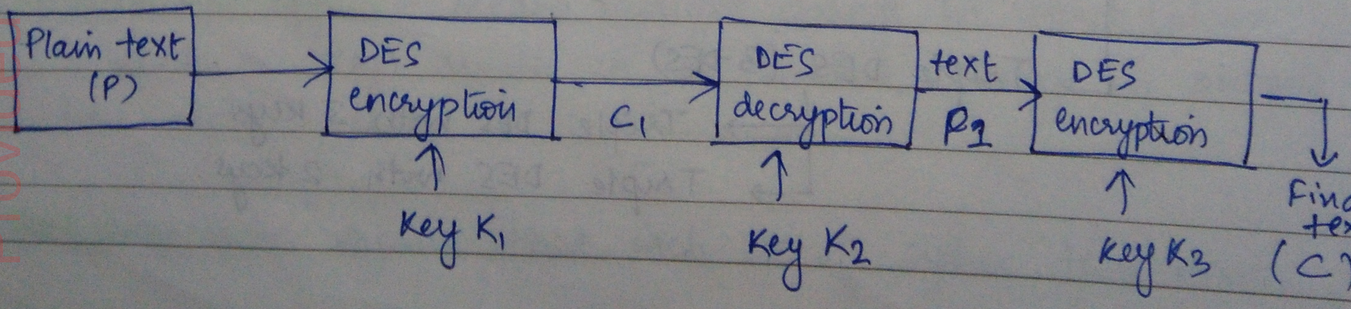
Steps: 1. Attacker encrypts P using all 2^{56} possible keys, & stores the results. The stored results will include all possible encryptions

$$P \rightarrow E(K_1, P)$$

2. Attacker decrypts C using all 2^{56} possible keys.

$$D(K_2, C) = D(K_2, E(K_2, E(K_1, P))) \rightarrow E(K_1, P)$$

* **Triple DES with 3 keys:-** uses 3 keys K_1, K_2 and K_3.



DATE
PAGE

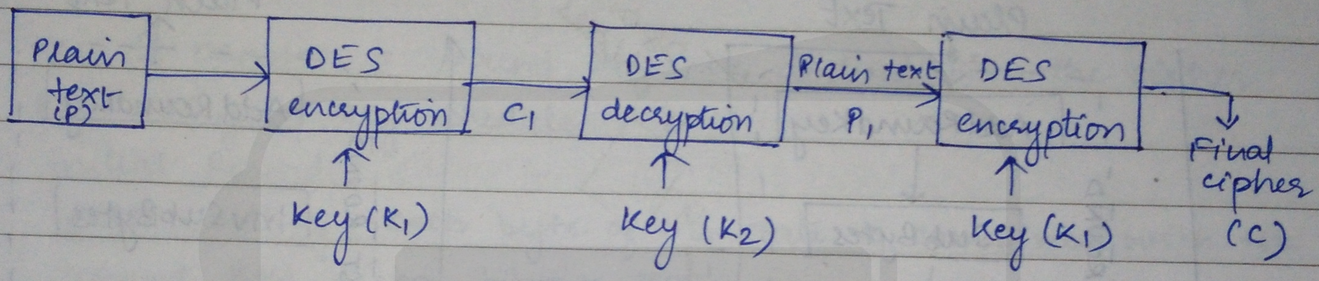
- has a 168-bit key, encrypts blocks of 64 bits.

$$C = E(K_3, D(K_2, E(K_1, P)))$$

168 bits (56×3)

(D) - 3-DES with 3 keys requires 168 (56×3) bits for the keys, which is not feasible practically. 2^{168}

★ Triple DES with 2 keys :- uses 2 keys K_1 and K_2
- requires 112 bits for keys.



$$C = E(K_1, D(K_2, E(K_1, P)))$$

★ ADVANCED ENCRYPTION STANDARD (AES) :- (2001)
- block cipher adopted as an encryption standard by the US Govt. - used in symmetric key cryptography
- substitution-permutation n/w, fast in both software and hardware
- easy to implement, requires little memory.
- fixed block size of 128 bits, Key size of 128, 192 or 256 bits.
- operates on 4×4 array of bytes, called "state".
★ satisfies the following 2 criteria of a good encryption algorithm :-

1. there must be no way to find the unencrypted clear text if the key is known, except brute force.
2. the no. of possible keys must be so large that is computationally infeasible to actually stage a successful

brute force attack in a short time.

AES cipher = specified as a no. of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text.

- each round consists of several processing steps.
- a set of reverse rounds is applied to transform ciphertext back into the original plaintext using the same encryption key.

4 different stages are used:-

1. Substitute bytes – uses an S-box to perform a byte-to-byte substitution of the block.
2. Shift Rows – a simple permutation
3. Mix Columns – A substitution that makes use of arithmetic
4. Add Round Key – a simple bitwise XOR of the current block with a portion of the key.

Steps in AES:-

1. Key Expansion = round keys are derived from the cipher key using a key schedule.
2. Initial Round =
   AddRoundKey = each byte of the state is combined with the round key using bitwise XOR.
3. Rounds =
   (i) SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table.
   (ii) ShiftRows – a transposition step where each row of the state is shifted cyclically a certain no. of steps.
   (iii) Mix Columns – a mixing operation which operates on the columns of the state, combining the 4 bytes in each column.
   (iv) AddRoundKey.
4. Final Round = (i) SubBytes (ii) ShiftRows (iii) AddRoundKey.

* Analysis of AES: AES is well-protected against all attacks that caused security breaches in DES –

1. Brute force attack:
   AES has larger key size, i.e. 128/192/256 than DES, which makes brute force attack impractical.

2^{128}

* RSA Algorithm - based on the concept of factorization.
- block cipher, each plaintext block is an integer b/w 0 and (n-1) for some n, which leads to a block size that is $\leq \log_2(n)$.
- typically, $n = 1024$.

→ Steps in RSA :-

1. Key generation : Following steps are required to create public key (e) and private key (d).
   (i) Pick 2 large nos. p and q, $p \neq q$
   (ii) Calculate $n = p \times q$
   (iii) Calculate $\phi(n) = (p-1)(q-1)$
   (iv) Choose 'e' such that HCF $(e, \phi(n)) = 1$, i.e. e is not a factor of $\phi(n)$.
   (v) Calculate d, such that $d \cdot e \bmod \phi(n) = 1$ i.e. d is the multiplicative inverse of $e \bmod \phi(n)$
   (vi) Get public key as $KU = \{e, n\}$
   (vii) Get private key as $KR = \{d, n\}$.

2. Encryption : For plaintext block $P < n$, its ciphertext is calculated using the equation :
$$C = P^e \bmod n.$$
where e = receiver's public key.

3. Decryption : For ciphertext block C, its plaintext will be calculated using equation :
$$P = C^d \bmod n$$
where d = receiver's private key

2. Statistical Attacks - combination of SubBytes, shiftRows and MixColumns transformation removes any frequency pattern in the plaintext.

3. Differential & Linear attacks - no effect on AES.

* Asymmetric key cryptography is a form of cryptosystem in which encryption and decryption are performed using different keys - one is a public key, one is a private key.
- aka public key cryptography.
- one key (encryption key) can be publicly known without compromising the secrecy, so long as the other key (the decryption key) is held secret.

1. Sender encrypts message using receiver's public key. Anyone with the public key can do this.
2. Receiver decrypts the message using his private key, which only he knows.

A+Bpublic ⟶ Bprivate

Sender

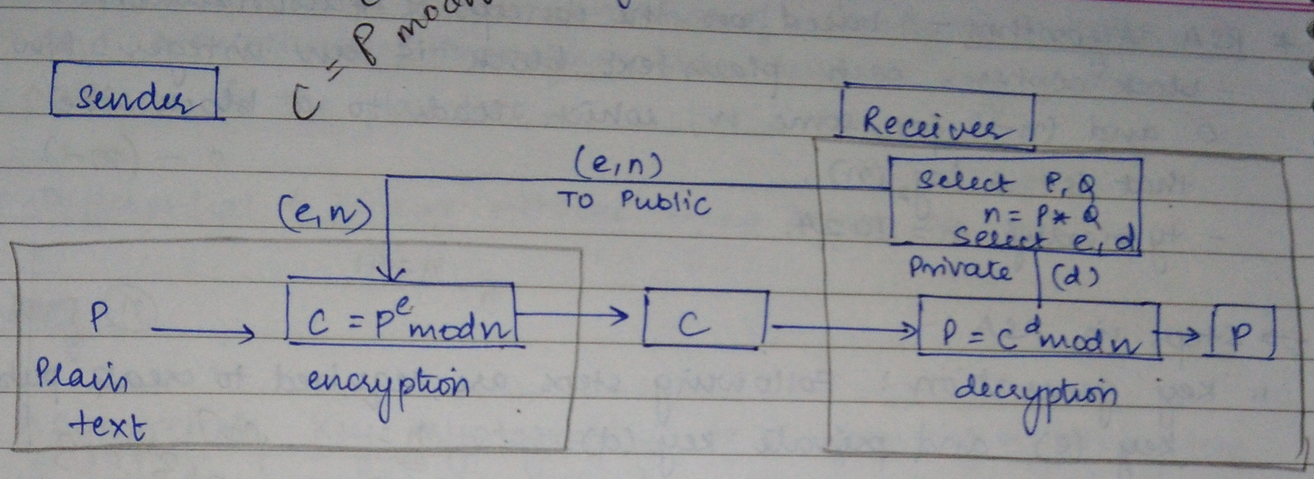
Message + Public key = Encrypted Message

Receiver

Encrypted message + private key = Decrypted Message.

$d = e^{-1} \bmod \phi(n)$.

RSA Encryption Process



* Security of RSA :-

1. Generating primes require a strong random no. generator ; any weakness in the generator reduces security.
2. Using the system requires that the private key should never be revealed.

* ELLIPTIC CURVE CRYPTOGRAPHY :

Elliptic curves are cubic curves of the form $y^3 = x^3 + ax + b$.

- public key cryptographic system involve arithmetic operations on Elliptic curve over finite fields which is determined by elliptic curve domain parameters.

- ECC domain parameters are :

$$D = (q, FR, a, b, G, n, h)$$

- q = prime power, i.e. $q = 2^m$, or $q = p$ where p is prime
- FR = field representation of method used
- a, b = field elements
- G = base point
- n = order of point G
- h = cofactor

→ length of Key in ECC = bit length of n.

DATE
PAGE

→ Message authentication = mechanism / service used to verify the integrity of a message. - assures that the data received is exactly as sent by the sender, ~~and~~
- also verifies identity of sender.

Message authentication = integrity + data origin

- common techniques are: 1. message authentication code (MAC
2. secure hash function

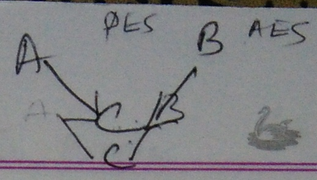
Types of authentication:-

1. Peer-to-peer authentication - applicable to a connection oriented environment like TCP.
   - provides ~~security~~ security against masquerade or unauthorized replay.
2. Data Origin authentication - applicable to a connectionless environment like UDP.
   - provides confidence to the recipient that message received has been sent by the alleged sender.

* Requirement for message authentication arises due to the following reasons:-

1. Disclosure - release of message contents to any person or person not having right credentials / authority.
2. Traffic Analysis - discovery of pattern of traffic b/w parti
3. Masquerade
4. Content modification
5. Sequence "
6. Timing "
7. Source repudiation
8. Destination repudiation

A-6



DATE
PAGE

* Authentication functions — functions used for authentication purposes are of 3 types :-

1. Message Encryption - cipher text of entire message works as an authenticator to check the message authentication.
2. Message Authentication code (MAC) - a function and secret key that produces fixed length hash code works as an authenticator to check message authentication.
3. Hash Function - A function that produces a fixed length hash code of variable length message works as an authenticator.

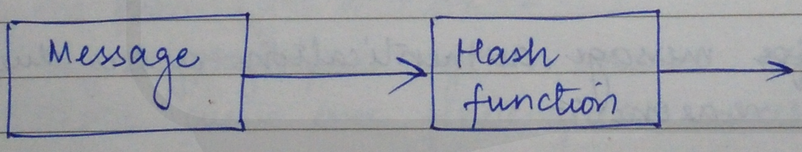
16 - 5

* Hash Function = maps a message of any length to a fixed-length hash value, which serves as an authenticator.

$$h = H(M)$$

h = hash value
H = hash function
M = message.

- h provides error detection capability, helps maintain integrity of data.



Properties :-

1. One Way property = A hash function is a one way function. It is easy to generate h from M, but impossible to obtain M from h. $M \rightarrow h$, $h \not\rightarrow M$

2. Weak Collision Resistance = given an input M_1 it should be hard to find another input M_2 where $M_1 \neq M_2$, such that $H(M_1) = H(M_2)$.

3. Strong Collision Resistance = it should be extremely hard to

$(M_1, h_1) \longrightarrow h_2, M$

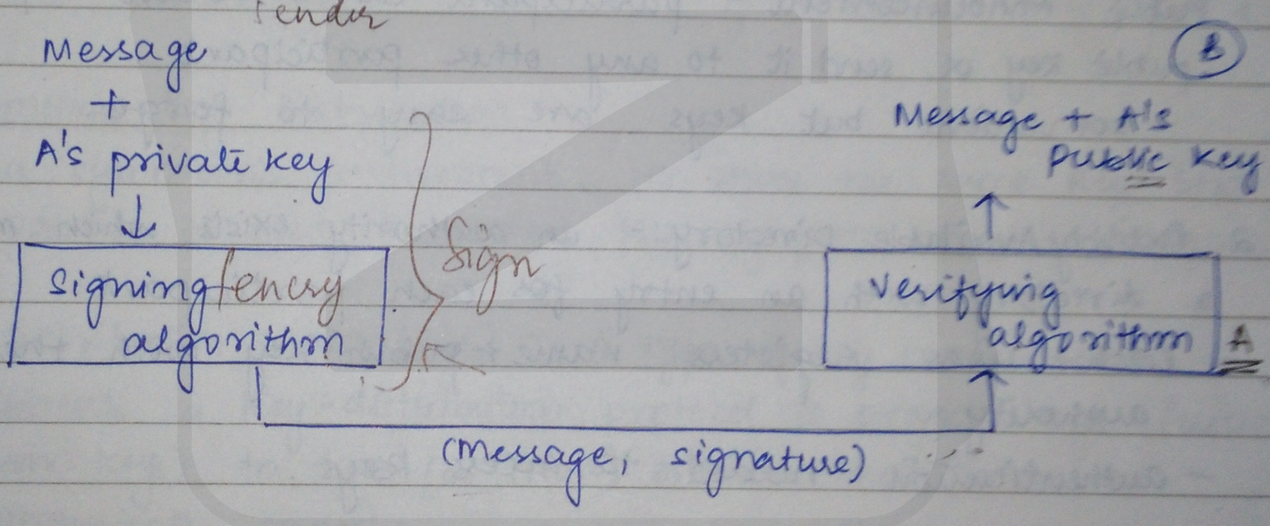
determine a message pair (M_1, M_2) having same hash value h_1.

→ Digital Signature = an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.

- signature is formed by taking the hash of a message and encrypting the message with the creator's private key.
  hash + private key
- signature guarantees the source and integrity of the message.
  confi

→ Properties of DS:-

1. must verify the author and date and time of signature.
2. must authenticate the contents.
3. must be verifiable by third parties, to resolve disputes.



→ Benefits of DS:-

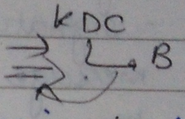
1. Authentication: provides message authentication as well as verification of sender's identity.
2. Integrity: provides assurance that the message is altered, because attacker cannot have same signatures as sender.

DATE
PAGE

3. Non-repudiation : helps avoid scenarios where a sender denies sending a message - trusted 3rd party verifies sender's signature + keeps and maintains a copy of the original message.

4. Confidentiality: prevents leakage of info.

Public



Key Management & Distribution :- the key must remain secret.
- known only to communicating parties.
- exchange of keys should be done with great care to prevent theft / forgery of key.

→ Ways of Key distribution :- (Pg. 200-201)

1. Public Announcement - participant can broadcast his/her public key or send it to any other participant.
   - convenient but keys are easy to forge.

2. Publicly Available Directory :- an authority exists which maintains a directory with an entry for each participant.
   - each user registers name + public key with the authority.
   - authentication needed to access keys.

3. Public key authorities :- (authority)
   - tighter control over security.
   - timestamp + authority's sign required
   - prevents interception & modification.
   - If A wants B's public key, it sends a request to a centre - centre supplies necessary info.

KDC

DATE
PAGE

4. Public Key Certificates :- a public key certificate is an electronic document which uses a digital signature to bind a public key with an identity.
- used to verify that a public key belongs to an individual.

Version
Certificate S.No.
Issuer's signature
Issuer
Validity
Subject
Public key info
Issuer unique identifier
Subject unique identifier
Extensions

CA
=

fields in an X.509 certificate

Symmetric Key Distribution

In a symmetric environment, we share the same key b/w 2 parties + need to protect the key from access to others.

→ Key Distribution Center (KDC) - A type of key center that implements a key-distribution protocol to provide keys (usually, session keys) to two (or more) entities that wish to communicate securely.

Steps :-

1. User A sends a request to KDC asking for session key b/w itself and B.
2. KDC informs B about A's request.
3. If B agrees, session key is created b/w 2 users.