Module -V

Cryptography & N/w security

* Info Security: (p)s & methodologies that are designed & implemented to protect print, electronic / any othr form of confidential, private & sensitive data from unauthorized access.

* cybr security: It is a subset of info .S, is a practice of protecting systms, n/w & prgms frm digital attacks.

* N/w security: It is a subset of cyber .S, aims to protect the undrlying n/w-ing infrastr~ & n/w resources frm unauthorized access.

I Goals of N/w security:

* N/w .S entails protecting the usability, reliability, integrity & safety of n/w & data.

* primary goal of n/w .S are —

Confidentiality — () is to protect precious business data frm unauthrized persons.

Integrity — means maintaining & assuring the accuracy & consistncy of data.

Availability — () is to make sure that

the data, n/w resources are continously availalele to the legitimate users.
These 3 pillers of n/w.s are represnted as CIA triangle

II security Attacks :

* It is the attempt to expose, alter, destroy, steal unauthorized access to use of an asset.

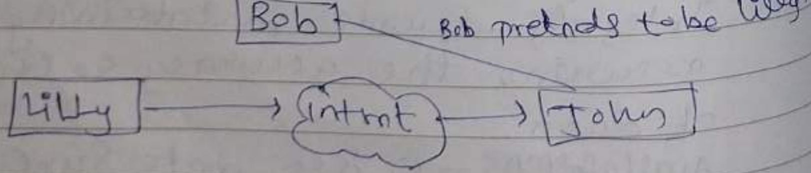
* 2 types

a) Active attacks :

It tries to change system resources with their ()-ality.
It entail some form of data stream manipulation. It takes follow forms -

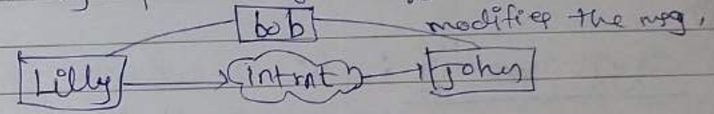
i) Masquerade :

Refers to whn an attackr impersonates an ~~ua~~authorized user/systm to gain unauthorized access to resource.



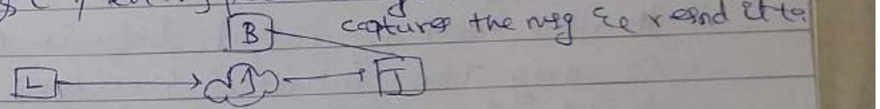
2) modifica^n ~~of~~ msgs :

Refers to unauthorized altera^n made to data as it is transmitted b/w systms/users.
This can involve changing the contnts of msgs, inserting melicious code/links, dlting parts of msgs, etc.



3) Replay :

* Here, an attackr intrcepts ie records legitimate data transm like authntica^n reqst / encrypted msgs.

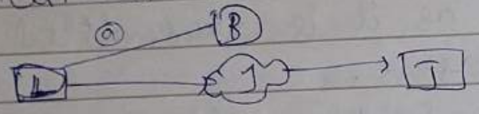


b) passive attacks :

Refers to unauthorized attempt to access/retrive info from a systm/n/w without altring the data being transmitted.

i) releasing msg content :

refers to unauthorized disclosure of the info contained within a msg to parties who are not intended recipients.



(b) bob reads the contents of msg which Lilly snds to John.

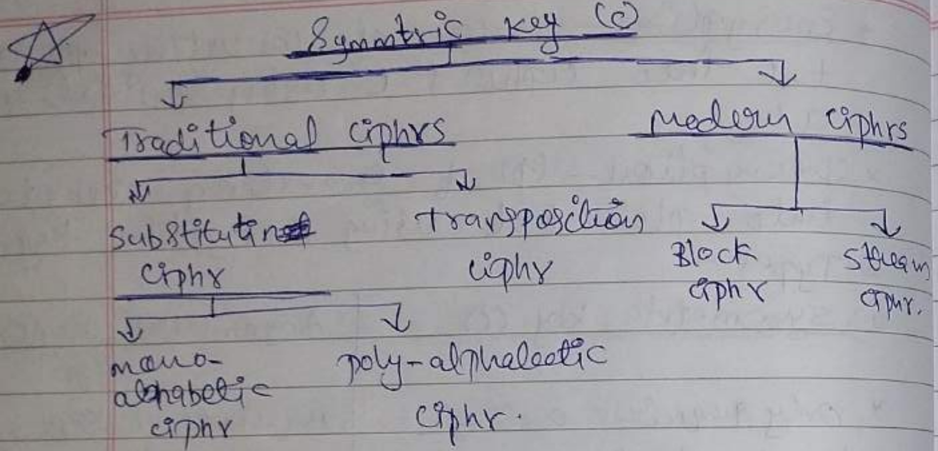
2) Traffic analysis

⇒ cryptography : (c)

* Technique of securing info & commuⁿ through use of codes so that only those person for whom the info is intended can undrstand it.
* It uses codes to protect data & commuⁿ so only the intended receivrs can decode & undrstand thm.
* It aims to keep data & msgs private & inaccessible to possible threats.
* ~~uses → random no generation~~
  ~~↳ paymnt appliⁿ & card transaction~~
* Plain txt – refers to original, readable data bfre any encryption is applied.
* Cipher txt – is the encrypted form of plain txt, making it unreadable without the decryption key.

* Encryption – process of convrting plain txt into cipher txt. using an (al) & a key.
* Decryption – (p) of convrting ciphr txt into plain txt using decryption key.
* Types –

a) symmetric key (c)	Asymmetric key (c)
* Only requires a single key for both encrypⁿ & decrypⁿ.	requires 2 keys, a public & private key, 1 to encrypt & othr 1 to decrypt.
* Size of ciphr txt is the same / smallr than the original plain txt.	— — — same / largr than — — —
* Encryption (p) is vry fast	— — — slow.
* used whn a large amount of data is required to transfer	— — small amount of data — — —
* Hence, resources utilization is low	— ~ — high
* Security is less as only 1 key is used for both E & D purpose	— more secure as 2 keys ~
* eg → AES, DES	eg → DSA & RSA.



I Traditional . c	Modern . c
* Encryption method is based on substitu^n & transposition	utilize complx mathematical (a)
* Smallr key size	largr key size
* Generally less secure	high secure
* may hue slowr performnce dueto simpler (al)	often optimized for speed & efficiency
* less used in modrn system	widely used

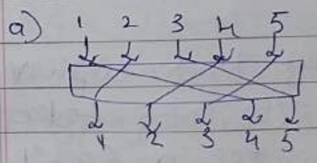
II Substitution . c	Transposition . c
* changes its identity bt retain its position	changes its position bt retains its identity
* Simple (p)	complx than S. c
* Easy to crack the code	difficult to crack the code
* unauthorized users can easily access the data	difficult ~
* time complexity of E & D is less	high
* eg → caesar ciphr	eg → columnar transp^n . c

III components of modern block cipher:

1) Transposition units : permutation^n.

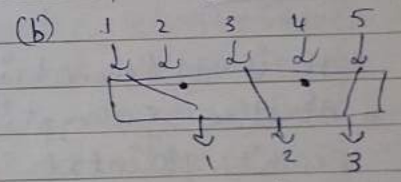
Modern . b . c uses 3 types of P-boxes -

a)



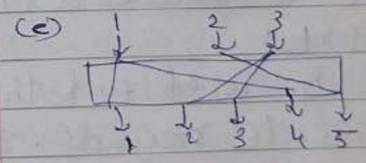
Straight P-boxes

(b)



compression P-boxes

(c)



Expansion P-boxes.

2) Substitu^n units

Implemented through S-boxes . S-box replace blocks of i/p bits with anothr block of o/p bits based on a predefined Substitut^n table.

3) Shifting unit :
refers to the op^r. like bit rotations or circular shifts applied to data during encryption & D process.

4) Swap units :
It is sple case of O shift op^r where the non shifted bits $k = n/2$.

5) Split & combine units.

IV DES (data encryption Standard) :

- * It is a symmtric key block cipher
- • At the Encryption site, DES takes a 64-bit plaintxt & creates a 64 bit ciphrtxt, at decryption site, DES takes a 64-bit ciphrtxt & create a 64 bit block of plain txt.
- * 56-bit ciphr key is used to both E&D.
- * Rounds : DES uses 16 rounds. Each round of DES is an invertible transforma^n.
- * DES () : The heart of DES is DES func.

It applies a 48-bit key to the right most 32 bits to produce 32-bit o/p.

V modern stream ciphrs :

Are symmtric key ciphrs that encrypt plaintxt data by generating a pseudorandom stream of bits, which is combined with the plaintxt using bitwise XOR op^r.

eg → RC4, Rabbit, Salsa20.

✱ Asymmetric key ciphrs :

I RSA Cryptosystem : (Rivest-Shamir-Adleman)

- * It is a widely used asymmtric cryptographic (al) for secure data transm-
- * uses a pair of keys - ① public key can be shared openly while ② private key is kept secrt.
- * To encrypt a msg using RSA, the sndr uses the recipient's public key to prform modular exponentia^n. the rslt is ciphrtxt.
- • To decrypt the ciphrtxt, the recipient uses their private key to perform

anthr modular exponentiaⁿ resulting plaintxt msg.

- widely used appli including secure commuⁿ, digital signature, etc.

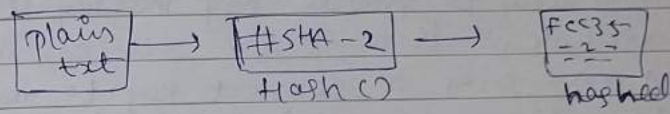
=> **other aspects of security:**

I **msg Integrity:**

- It describes the concepts of ensuring that data has not been modified in transit.
- This is typically accomplished with the use of a hashing (al).
- To preserve the integrity of a msg, the msg is passed through an (al) → cryptographic hash ().

The () creates a compressed image of the msg → digest.

II **Hash ()** : A cryptographic hash () takes a msg of arbitrary length & creates a msg digest of fixed length. Creating such a () is best accomblished using iteration. Several hash (al)s are designed by Ron Rivest, these are referred to as MD 2, MD4 & MD5, (MD → msg Digest).



III **Msg Authentication:**

- MAC (msg·A·code) is a symmtric key cryptographic technique to provide msg authenticaⁿ.
- for establishing MAC (p), the sndr & receivr share a symmtric key 'k'.
- Similar to hash, MAC () also compresses an arbitrary long i/p into a fixed length o/p.
- Major diffrnce b/w MAC & hash is that MAC uses ~~#~~secrt key during the compression.

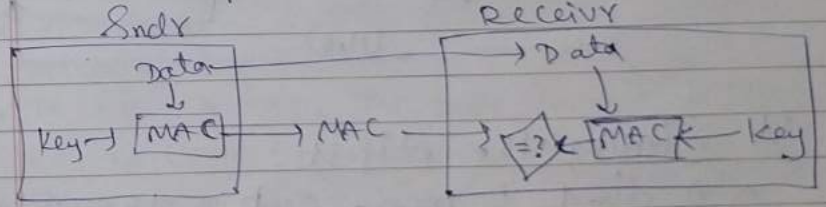
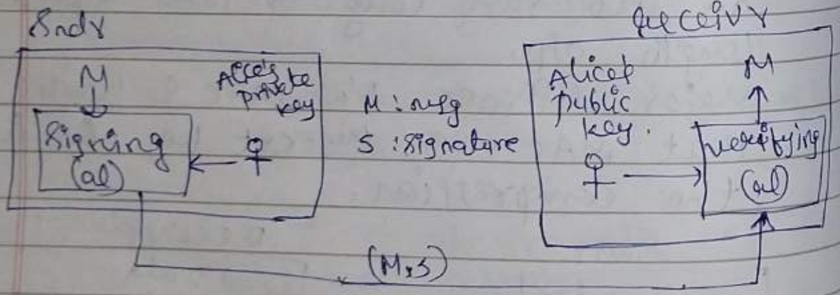


fig: MAC diagram

=> Digital Signature :

- Anthr way to provide msg integrity & msg authnteaⁿ is a D.S.
  A MAC uses a secrect key to protect the digest, a digital signature uses a pair of private -public keys.
- when a sndr snds a msg to a receivr, the receivr needs to checks the authnticity of the sndr, the receivr needs to be sure that the msg comes from the original sndr & not frm somebody else.
  The receivr can ask the sndr to sign the msg electronically,



I Signing the digest :

- A digest is made out of the msg at the sndr's site. The digest then goes through the signing (p) using the sndr's private key.
  The sndr then snds the msg & the signature to the recevr.

II Digital Signature service :

- It can directly provide services for msg authnticaⁿ & msg integrity.
- It does not provide service for msg confidentiality.
- Involves creating, varifying & managing digital signatures to ensure the authnticity & integrity of electronic msgs.

III RSA digital signature scheme :

- widely used cryptographic (al) for secure commu- & digital signature.
- here, each entity generates a public-private key pair.
- To sign a msg, the sndr uses their private key to encrypt a cryptographic hash of the msg. This creates the digital signature.