CNS Assignment :-

1) **RSA Algorithm:** It is widely used encryption and decryption method in the field of cryptography. RSA is based on the mathematical properties of large prime numbers

Key Generation :

→ select two large prime numbers p,q i,e., 17, 11

→ compute the moduen, n = 17 * 11 = 187

→ compute Euclid tokent function φ(n)

$\varphi(n) = 16 * 10 = 160$

→ choose encryption exponent i,e., 160

→ choose decryption excoponect (7 * 23) % 160 = 1

∴ The public key is (e,n) and privat key (d,n)

Encryption:

→ we want to encrypt msg M, i,e., M = 88

→ apply C = M^e mod n

C = 88^7 mod 187 = 11.

Decryption:

→ we want to depcryt M = C^d mod n

M = 11^23 mod 187

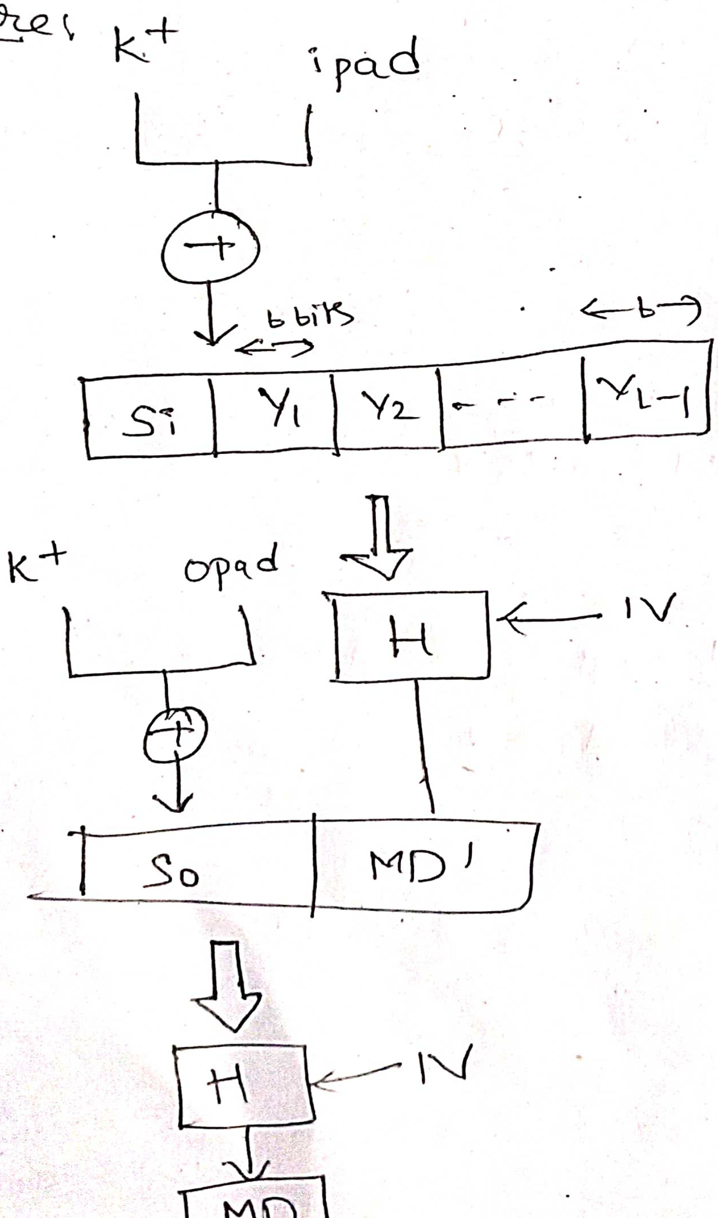
= 88.

The seccerity of RSA is dyfficulty of factoring large numbers. This property forms of RSA strength in protecting sensitive information

2) **HMAC algorithm:** stands for Hashed or. Hash based msg authentication code. It is a result of work done on developing a MAC derived from cryptographic hash functions HMAC is a great resistance towards cryptanalysis attacks as it uses the hasing concept twice

Algorithm:
It starts with taking msg M containing blocks of length 'b' bits. An i/p signature is padded to left of msg and the whole is given as i/p to hash function which gives temp msg digest.

Structure:



H→ hasing function
M→ original msg
Si → Input signature
So→ o/p signature
L= count of blocks
k= secret key
IV=

The generation of input,out signature are

$$S_i = K^+ \oplus ipad$$

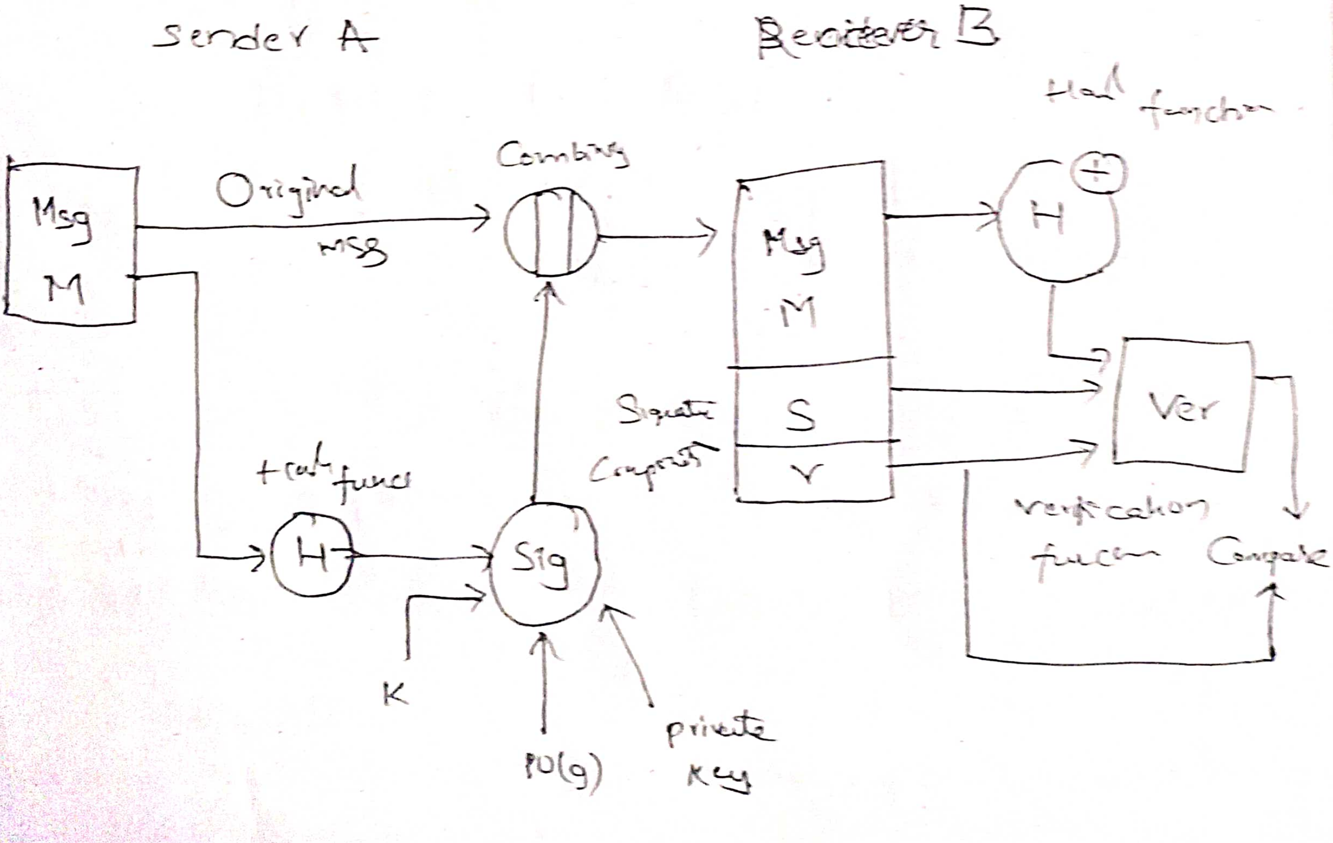
$$S_o = K^+ \oplus opad$$

$$MD' = H(S_i || M)$$

$$MD = H(S_o || MD') \quad (or)$$

$$MD = H(S_o || H(S_i || M))$$

3) **DSS Algorithm :-** It is a way of authenticating the data coming from trusted individual. It is a way of authenticating a digital data coming from trusted src. It is a federal information processing standard which defines algorithms that are used to generate digital signatures with help of SHA



Sender Side:

*) Following are I/p's-for signature function

- → Hash Code
- → random number 'K' generated for sign
- → private key of the sender... PR(a)
- → a global public key i.e... PU(g)

Reciever Side:-

there is a verification function thas inputs like

- → hash code generated by reciever.
- → signature components 's' & 'r'
- → public key of sender,
- → global public key.

4)

Host - Based Intrusion Detection System (IDS) & Intrusion Prevention System (IPS) and IDS/IPS are two types of security systems designed to detect and prevent unauthorized activities

HIDS / HIPS:-

Host based IPS/IDS on individual host machines and focuses on monitoring & analyzing activities occuring within the hosts OS and applications

Here are key Characterstics;

Detection System:-

HIDS/HIPS employ various techinques to detect intrusions, including

→ log file analysis

→ file Integrity Monitoring

→ System Call Interception

→ Behaviour Monitoring

Response Cabability!

HIPS/HIDS can have both detection-only & prevention capabilites. Detection only system generate alerts when suspious activities are detected but do not-take any automated actions. prevention systems actively block or-terminate suspicious activites based on predefined rules/policies