Page No.
Date:

Cryptography: The art as well as science of secret writing of information/messages and makes it non-readable.

Types of Cryptography → Symmetric Cryptography (same Key)
→ Asymmetric Cryptography (two Keys)

* Stream Cipher
→ Algorithm applied to each binary digit in data stream

* Block Ciphers.
→ Algorithm applied to block of data.

* Substitution Cipher Tech.
→ Caesar Cipher
→ Monoalphabetic Cipher
→ Polyalphabetic Ciphers
→ Playfair Cipher
→ One Time Pad
→ Hill Ciphers.

* Block Cipher modes
→ Electronic Codebook (ECB)
→ Cipher Block Chaining (CBC mode)
→ Output Feedback (OFB)
→ Counter (CTR).

* Data Encryption Standard (DES)
64 bit plaintxt input → encrypts 64 bit size block

* Double DES → 2 Keys * Triple DES → 3 Keys.

* AES (Advance Encryption Standard)
Input Key is required and data size 128, 192, 256 bits. Steps (1) SubBytes (2) ShiftRows (3) MixColumns (4) AddRoundKey

* Public Key Cryptography:—
RSA Algorithm.
Its a block Cipher which converts plaintext into cipher text at sender and vice versa at receiver side.

Page No.
Date:

Possible Attacks on RSA:

→ Brute force attack (Hacker tries all posible private keys)
→ Mathematical attack (Hacker tries to factorize product of 2 primes)
→ Timing attack (Depends on running time)
→ Chosen ciphertext attack (Hacker tries attack on all private

MAC → Message Authentication Code.

CMAC → Cipher Based →

* Deffic Hellman Key Exchange.
Also known as key exchange algorithm or key agreement algo. Its used to generate same private cryptographic key at sender as well as receiver end so that there is no need to transfer this key from sender to receiver.

* Hashing is a process of converting a given key into another value. (M → data)
$h = H(M)$.

* Digital Signature
→ Message Authentication application.
→ Similar to MAC.

* Secure Hash Algorithm (SHA)
→ SHA-1 takes input msg. of a maximum length less than 2^{64} bits and reproduce an output of 160 bit message digest.
→ Stronger against Brute-force attack.

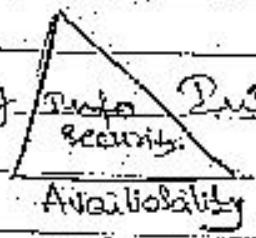
* MD#5 ~~is~~ uses 128 bit message digest.
Takes 4 rounds.

* Application of Cryptographic Hash func.
1) Data Authentication
2) Digital Signature
3) Password Storage
4) Key Generation
5) Intrusion Detection & Virus Detection Tech.

* Kerberos
Authentication protocol. Uses the concept of the ticket as token to prove the identity of the user.

KDC → Key Distribution Centre.

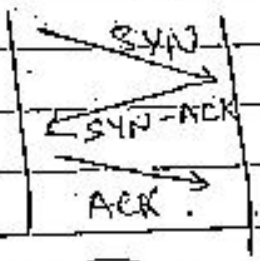
Page No.
Date:



CIA

ARP Spoofing → Address resolution Protocol.
→ Malicious prog over local area network.
→ Attacker's MAC address connected to authentic IP address.
→ So attacker gets info from IP add.
→ Multiple IP with single target MAC add.

IP Spoofing → The attacker sends SYN packet with fake IP to victim to establish connection.



DNS Spoofing → Domain Name Server
→ Used to redirect online traffic to a fraudulent website that resembles its intended destination.

DOS Attack → Denial of service
→ overflow of email, spam ... to victim.
→ Unables victim to use internet.

Types of DOS
→ Flood attack
→ Ping of Death
→ SYN attack

Page No.
Date:

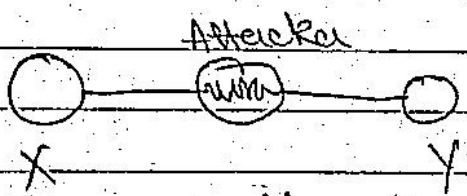
IDS → Intrusion Detection.
→ Anti-virus software.
→ Detects diff. attacks.

Firewall → Barrier place between inside and outside network to protect organization from inside & outside hackers.

Virus & Worms
→ Malacious software.
→ needs user interaction and the multiplies.
does not ——— .

Trojan horse → A Computer program.
→ Along with useful some malicious code.
→ useful info stole from attacker etc..

Man in the middle Attack.



person X, person Y not aware of attacker & altering the msgs.