NETWORK SECURITY

UNIT 4

WIRELESS NETWORK SECURITY

- IEEE 802.11 – WLAN (Wi-Fi) & IEEE 802.11i – WPA & IEEE 802.1X – Port-based Network Access control.

Defn: The Wireless Application Protocol (WAP) is a standard to provide mobile users of wireless phones & other wireless terminals access to telephony & information services including the internet & the web. [WAP Security → WTLS]

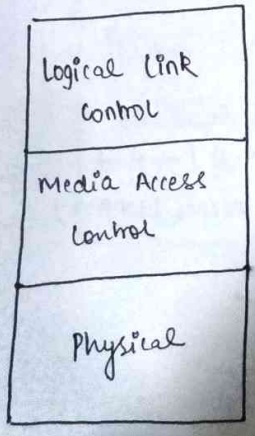
IEEE 802 – a committee that has developed standards for a wide range of LANs.

Terminology Table

1) Access Points	a network device that allows other Wi-Fi devices to connect to a wired/wireless network.
2) Basic Service Set (BSS)	group of wireless devices that can communicate with each other within a specific coverage area.
3) Coordination Func.	mechanisms for managing access to shared medium.
4) Distribution System (DS)	a system to BSS(s) + LAN(s) = ESS
5) Extended Service Set (ESS)	a wireless network created by multiple access points which appears to users as a single seamless n/w.
6) MAC PDU (MPDU)	unit of data exchanged blw 2 MAC peer entities using the services of the physical layer.
7) MAC SDU (MSDU)	information that is delivered as a unit blw MAC users.
8) Station (s)	any device that contains IEEE802.11 conformant MAC & physical layer.

- Wi-Fi Alliance – 1999; Wireless Ethernet Compatibility Alliance (WECA) interoperability for 802.11b products & Wi-Fi certification (Wi-Fi5, WPA, WPA2)

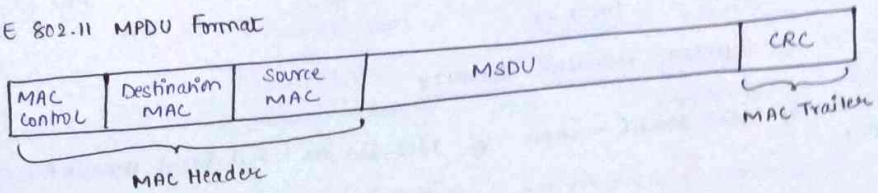
IEEE 802.11 Protocol Architecture:



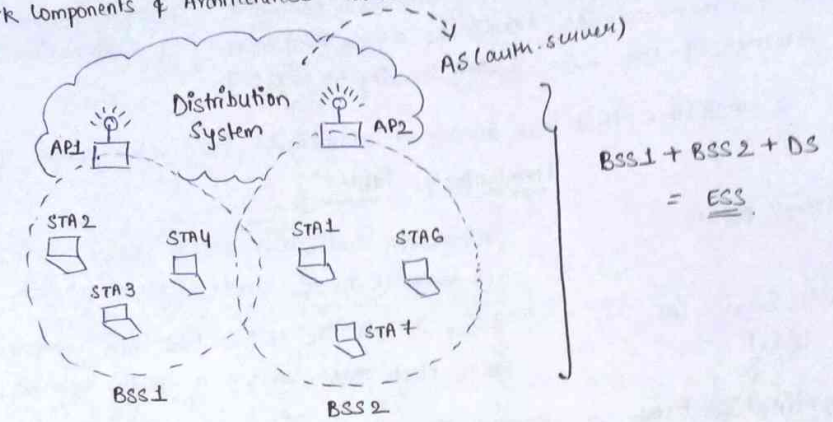
	General	Specific
Logical Link Control	Flow control Error control	
Media Access Control	Framing, Addressing Error detection Medium Access	Reliable data delivery wireless AC protocols
Physical	Encoding/Decoding Bit Transm./Rec. Transmission medium	Freq. band defn wireless signal encoding

IEEE 802.11i Services

IEEE 802.11 MPDU Format



IEEE 802.11 Network Components & Architectural Model



IEEE 802.11 Services

Service	Provider	Used to Support
1) Association	DS	MSDU delivery
2) Authentication	Station	LAN access & security
3) Deauthentication	Station	LAN access & security
4) Disassociation	DS	MSDU delivery
5) Distribution	DS	MSDU delivery
6) Integration	DS	MSDU delivery
7) Privacy	Station	LAN access & security
8) MSDU delivery	Station	MSDU delivery
9) Reassociation	DS	MSDU delivery

IEEE 802.11i WLAN Security :

Wired Equivalent Privacy (WEP) → Wi-Fi Protected Access (WPA) → (current) Wi-Fi Protected Access (WPA-2)

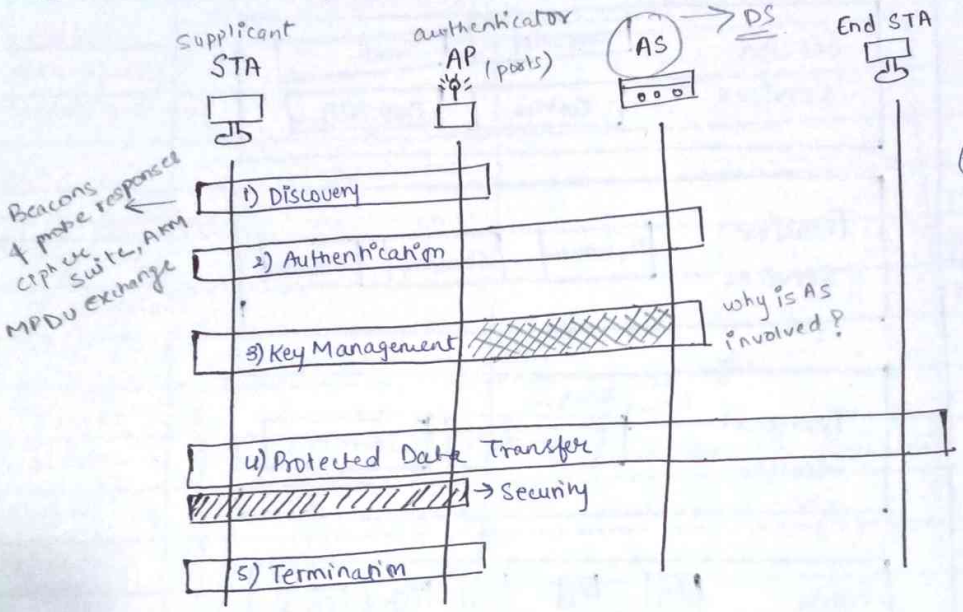
Wi-Fi 5.0

Robust Security Network (RSN)

IEEE 802.11i Services

Service	Provider	Used to Support
1) Authentication	AS	WLAN Access Control & security
2) Access Control	AP	WLAN Access Control & security
3) Privacy & Integrity	AP	WLAN Access Control & security

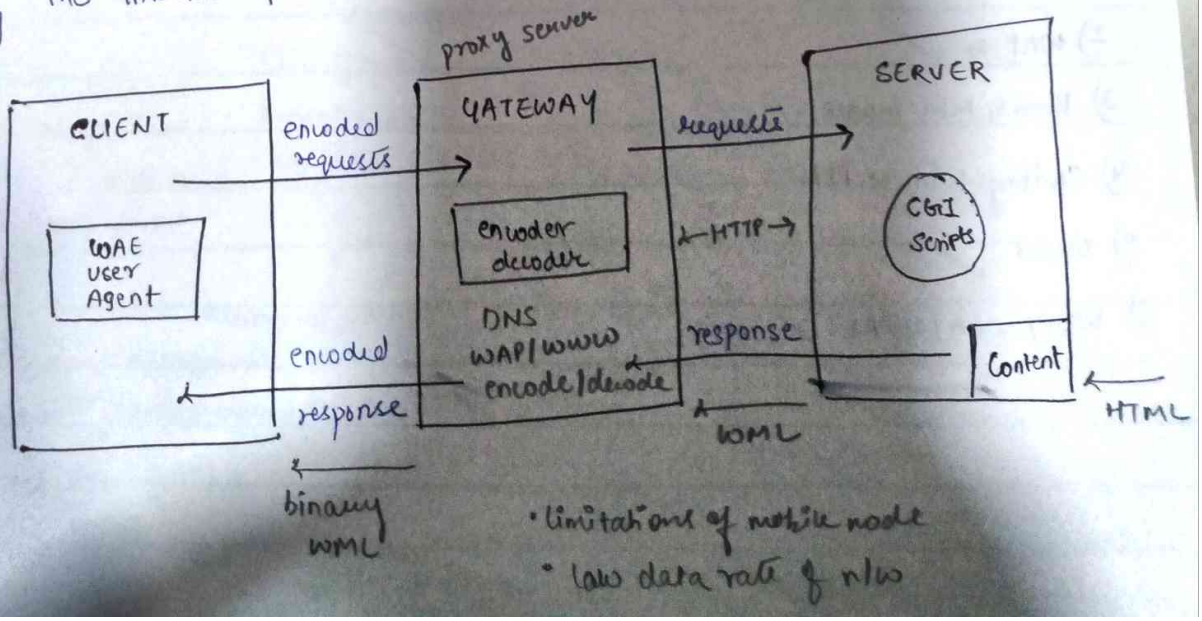
IEEE 802.11i Phases of Operation: what exactly is RSN? Is it like WEP/WPA?



(*) End-to-End security is a myth.

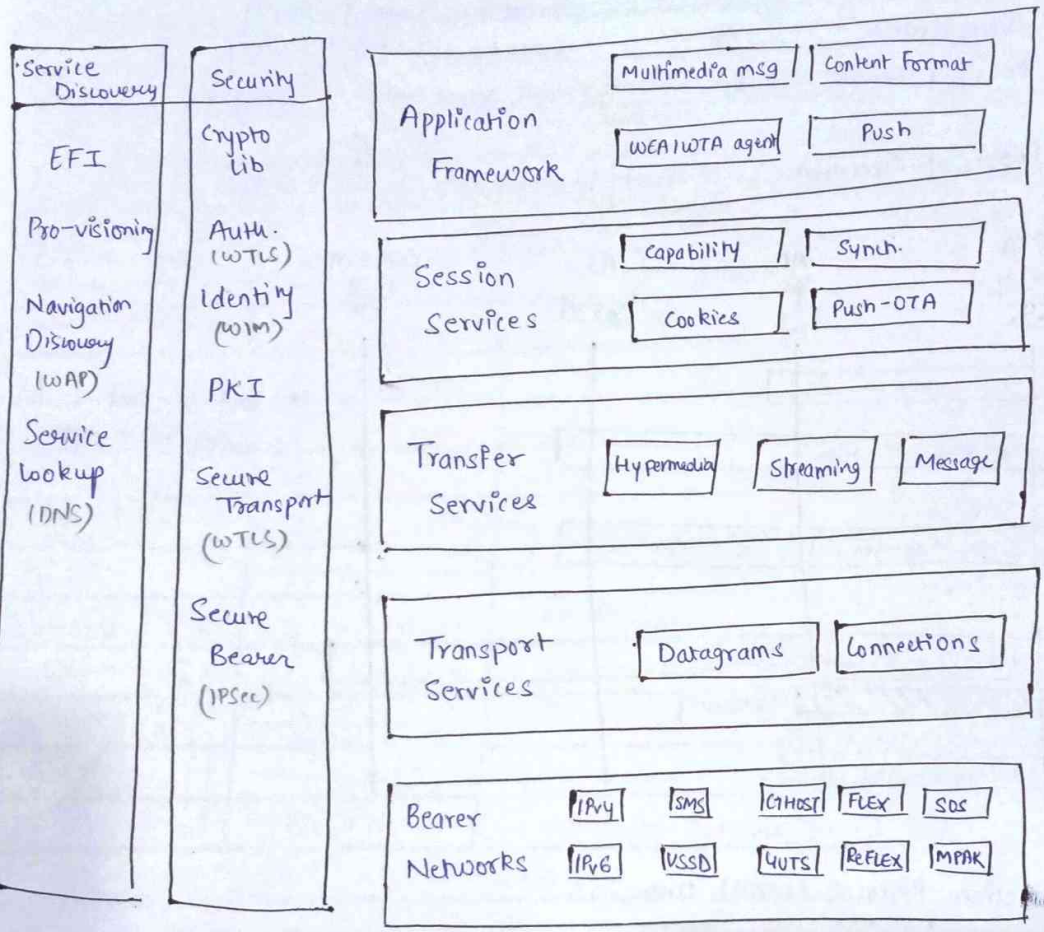
Wireless Application Protocol (WAP) Overview:

Defn: The WAP is a universal, open standard developed by the WAP forum to provide mobile users of wireless phones access to telephony & information services including the internet & the web.



- limitations of mobile node
- low data rate of n/w

WAP Architecture.



—— x —— Syllabus —— x ——

1) 802.11 Protocols ✓
2) WAP & ✓
3) Prom & Mon modes
4) Sniffing Wireless Pkts
5) WLAN ✓
6) WEP/WPA/WPA2 ✓

WML:
- text/image
- deck/card
- navigation

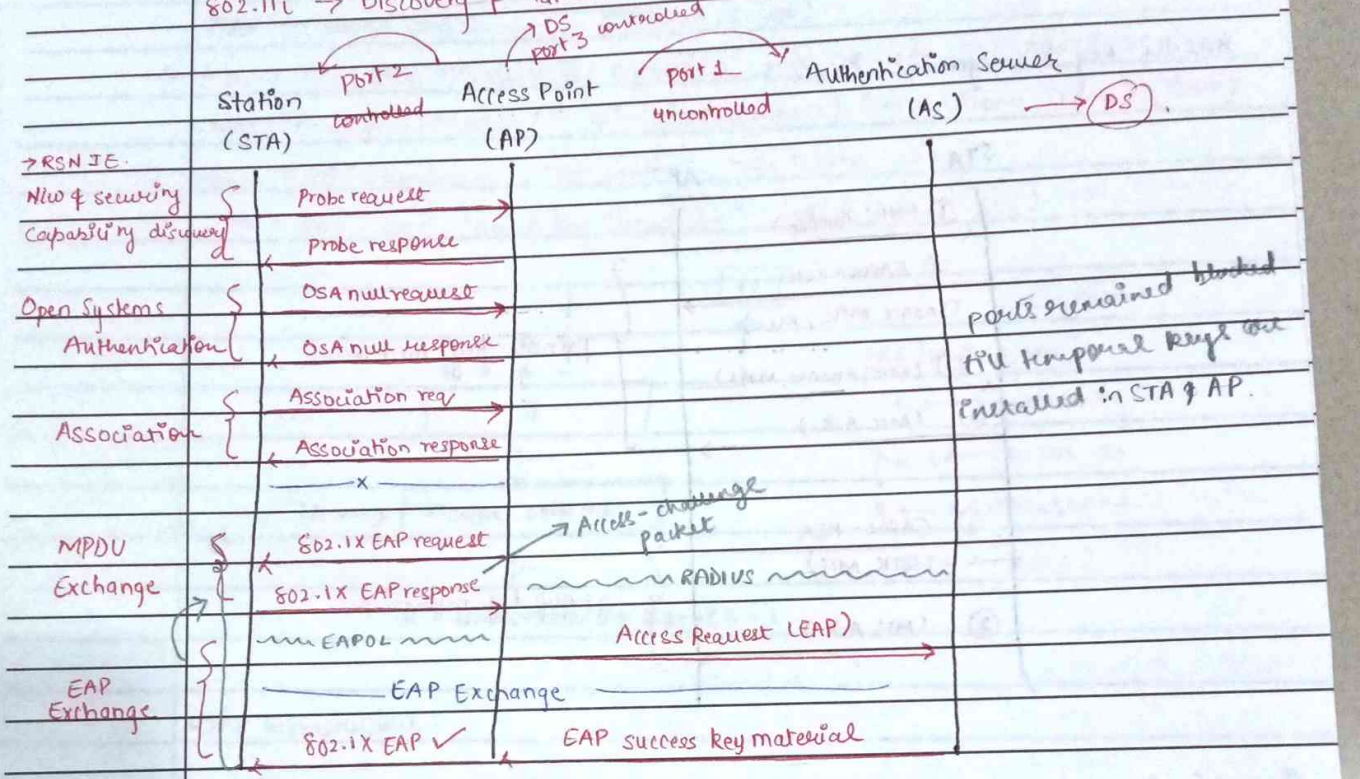
a card is one or more units of interaction
a deck is similar to an HTML page

WAE components
- WAE user agent
- WTA
- Std content encoding
- Push
- Multimedia messaging

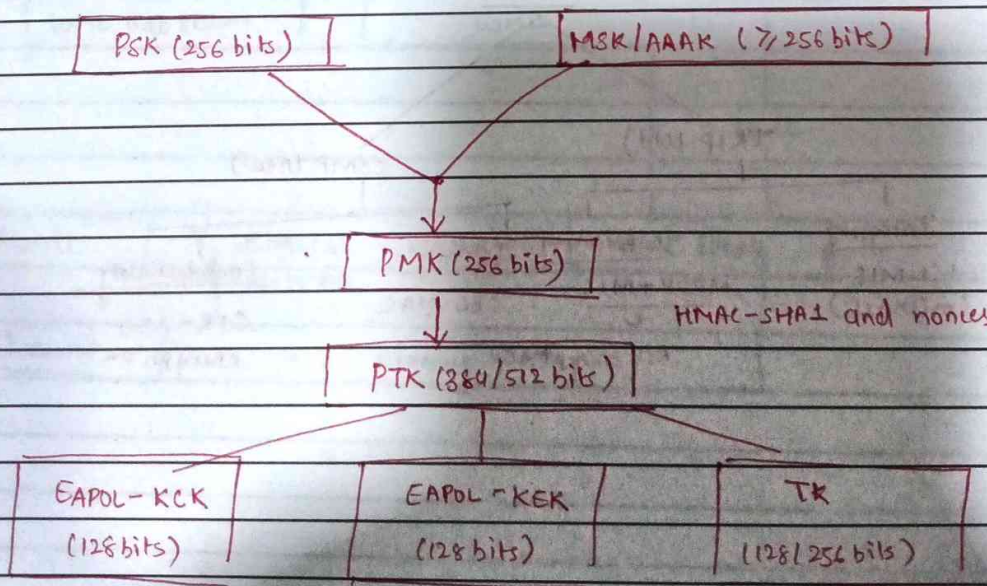
WSP - connection-less & oriented
WTP - req/resp

Topic ..... Date .....

802.11i → Discovery & Authentication Phases :

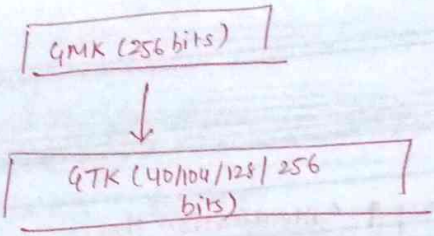


802.11i → Key Management Phase → Key Hierarchy



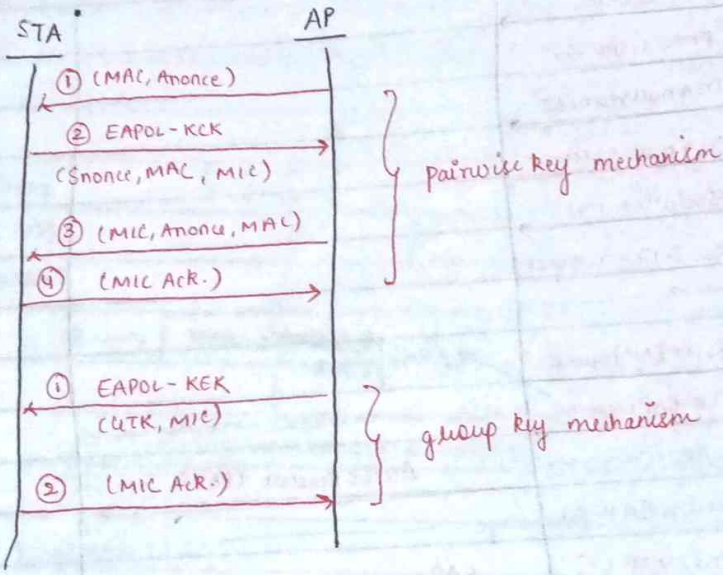
Pairwise Key Hierarchy.

Teacher's Sign. .....

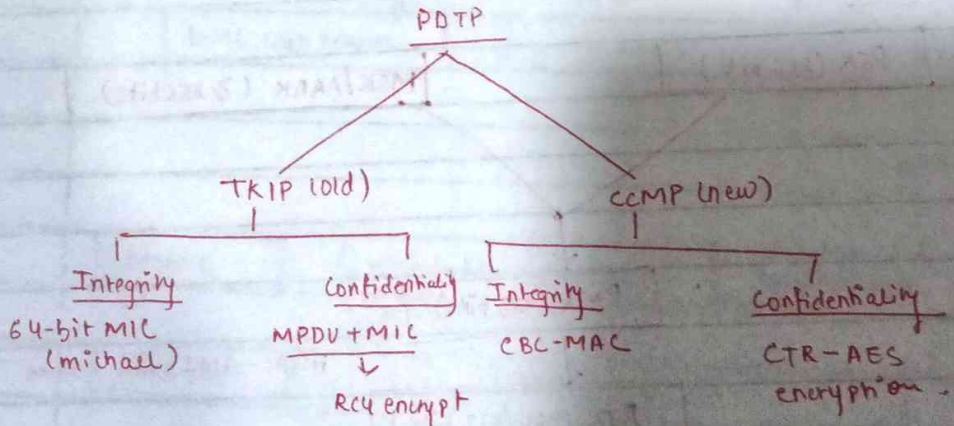


Group Key Hierarchy

802.11i Key Management Phase :



802.11i Protected Data Transfer Phase :



Topic ..... Date .....

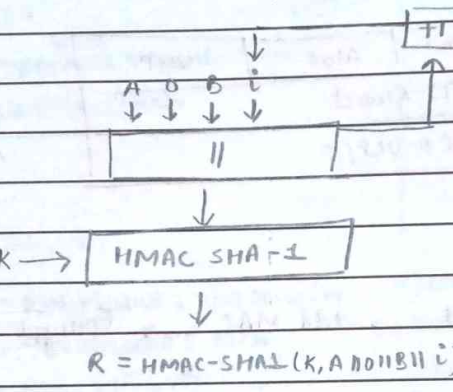
802.11i Pseudorandom function:

PRF → HMAC SHA-1 PRF(K, A, B, len)

→ PTK = PRF(PMK, "Pairwise key expansion", min(AP-Addr, STA-Addr) ||
max(AP-addr, STA-addr) || min(ANonce, SNonce) || max(ANonce, SNonce), 384)

→ Nonce = PRF(Random no., "Init Counter", MAC || Time, 256)

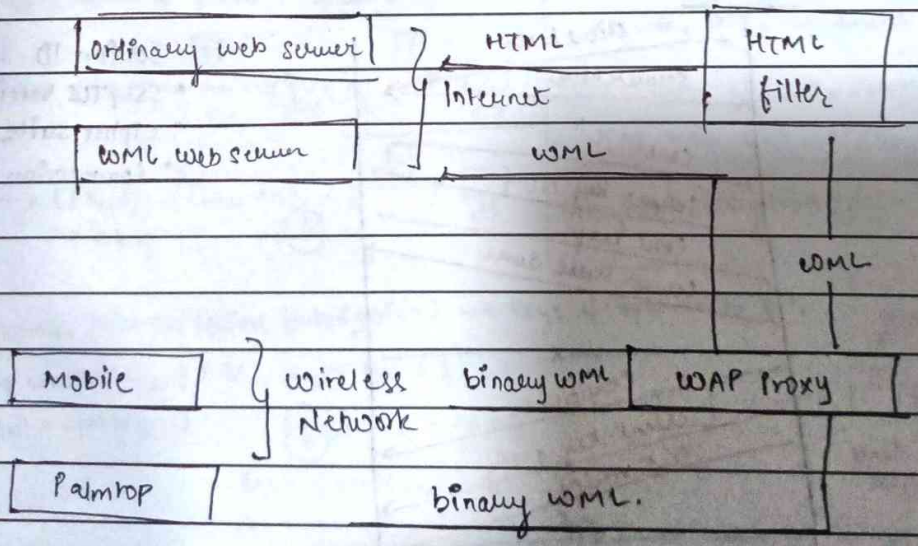
→ GTK = PRF(GMK, "Group Key Expansion", MAC || Gnonce, 256)



R = HMAC-SHA1(K, A || 0 || B || i)

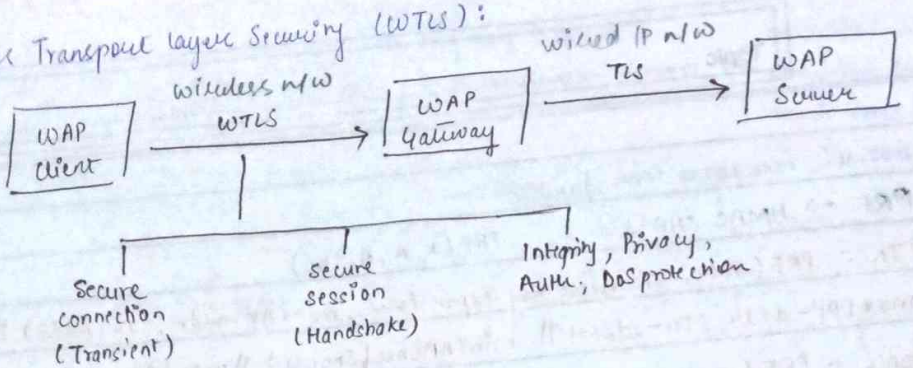
PRF(K, A, B, len)
R ← null string
for i ← 0 to len do
R ← R || HMAC SHA-1
Return(R, len)

WAP Infrastructure:

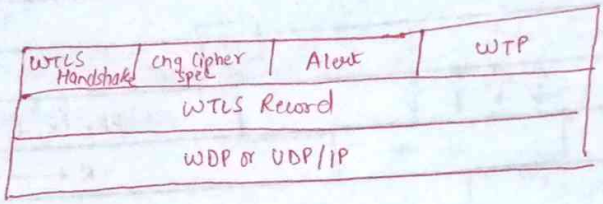


Teacher's Sign. .....

Wireless Transport layer Security (WTLS):



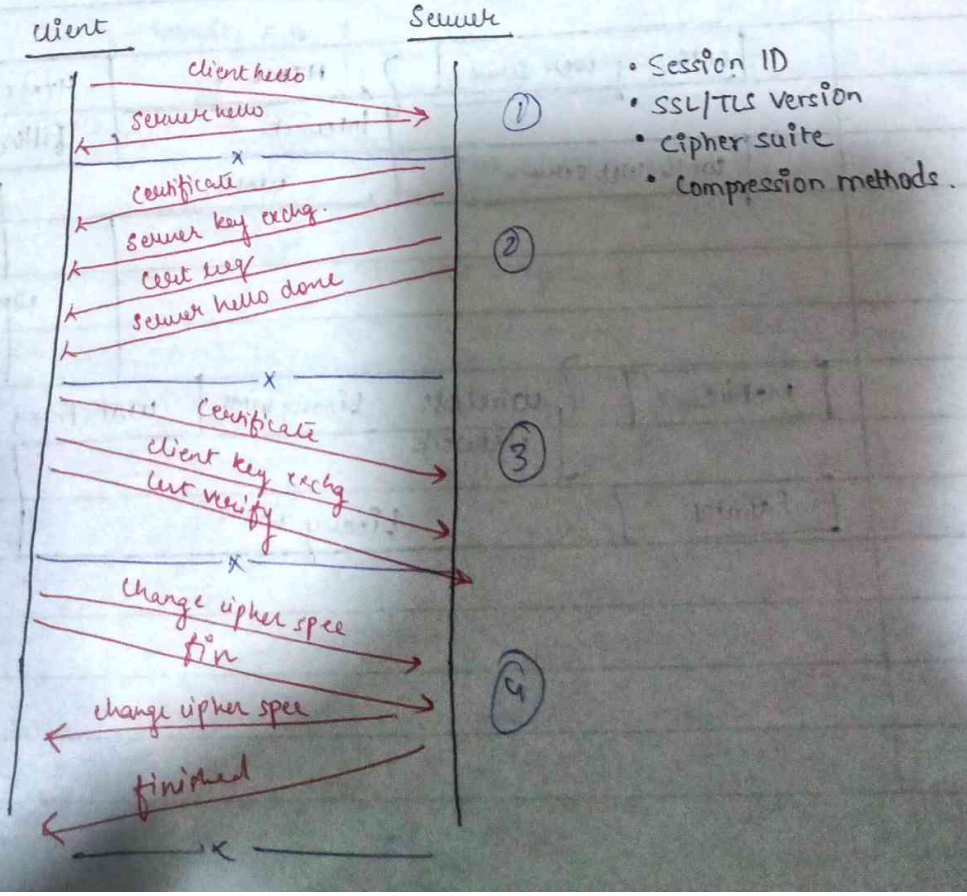
WTLS Protocol Architecture:



WTLS Record Protocol:

User data → compressed → add MAC → Encrypt → WTLS header

WTLS Handshake Protocol: SSL Handshake Protocol.

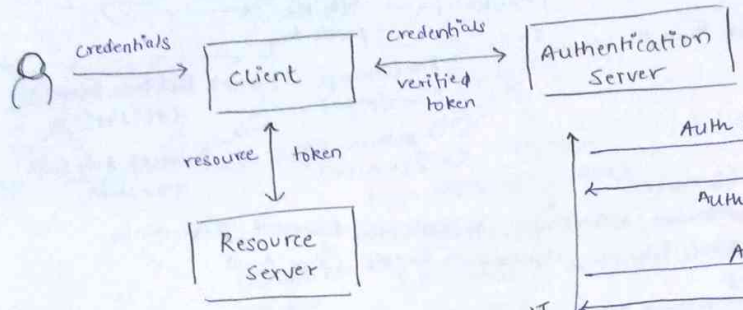


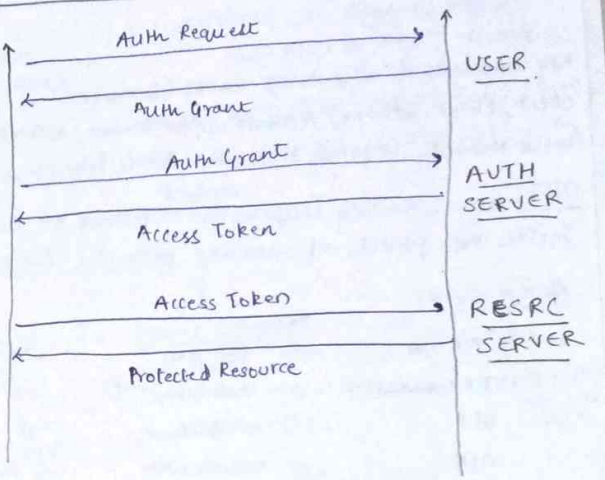
- Session ID
- SSL/TLS version
- Cipher suite
- Compression methods.

Authentication

"users are who they say they are"

↳ to ensure this → Authentication Servers
- centralized authentication
- streamline tasks.
- Forensic Value AS (investigation)



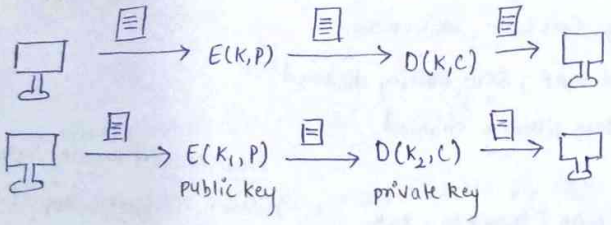


Examples w.r.t GOOGLE:
1) Authentication Server - OAuth 2.0 & OpenID connect (Gsuite)
2) Resource Server - Google Drive, Gmail
3) Client - Company

Types of Authentication Servers:
1) Firebox Authentication - WatchGuard; n/w security
2) AuthPoint Authentication - WatchGuard; MFA
3) RADIUS Authentication - AAA; WiFi; VPN
4) VASCO Authentication - 2FA; digital security
5) SecureID Authentication - RSA; MFA; Tokens
6) LDAP Authentication - single sign on (SSO)
7) Active Dir Authentication - Kerberos; NTLM

* Lightweight Directory Access Protocol
* Remote Auth. Dial-in User Service

- Encryption - Confidentiality ; Hashing - Integrity, Auth.



Stream - bit, confusion/substitution, faster, no redundancy, less code, OTP, hardware

Block - blocks, C|S|D|T, slower, redundancy, more code, DES, software.

- Assymetric Encryption (DS) - Non repudiation, Authentication

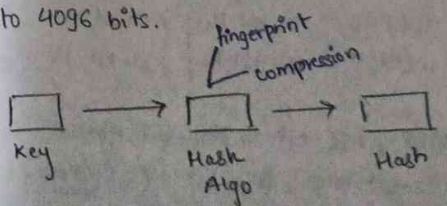
RSA - Rivest, Shamir, Adleman (prime factorization) → keys of upto 4096 bits.

p, q s.t p & q are prime; p ≠ q Public key = {e, n}

n = p x q $\phi(n) = (p-1)(q-1)$ Private key = {d, n}

e? gcd($\phi(n)$, e) = 1 Enc: $c = m^e \bmod n$

d? $de \bmod \phi(n) = 1$ Dec: $M = c^d \bmod n$

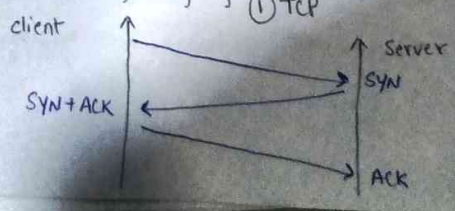


MD5: md5sum; 128-bit o/p; 512-bit block processing

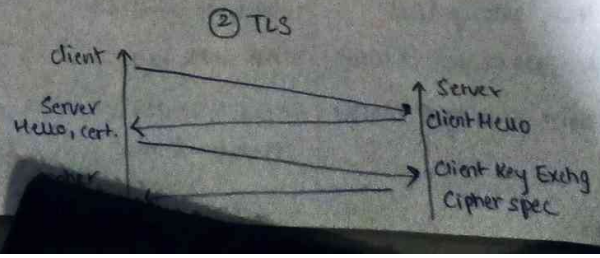
SHA: 1 (160-bit o/p), 2 (224, 384, 256, 512 bit o/p)

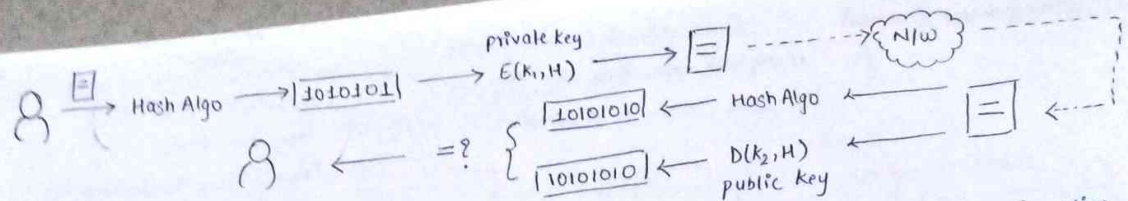
TLS - Encryption, Authentication, Integrity

① TCP



② TLS





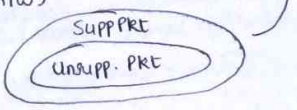
Cipher Suites – sets of instructions on how to secure network communication.

→ Key Exchange (Sym / Asym) → Bulk Data Encryption (AES / 3DES)

→ Authentication (RSA / DH) → Message Auth. Code (SHA / MD5)

Key components of N/w Access Control (10 Marks):
Client, Client Software, Authentication Server, Authenticator, Authentication Framework, Quarantine, Guest Network, Corporate Network, Public Internet, Management Console, Client Agent

Defn: Generic Routing Encapsulation – protocol for encapsulating data packets that use one routing protocol inside the packets of another protocol. (direct P2P connection over a n/w)



NMAP SCANS:

-sS : TCP SYN	-Pn : Port Scan	-sX : XMAS
-sT : TCP CONNECT(-p)	-sn : Host Disc. (-sP)	-nS : Null Scan
-sU : UDP	-PR : ARP Disc.	-sF : TCP FIN
-sA : ACK	-n : DNS resolution	-O --osscan-guess --osscan-limit : OS Fingerprinting

Advantages: Sec conn, privacy, integrity, fast perf, SEO

TLS Process – Client Hello, Server Hello, Server's D.S, Verified D.S, Premaster secret, Session key Exchg, Client is ready.

IEEE 802.11 – WiFi; Speed (54 Mbps – 104 bps); Frequency (2.4 GHz, 5 GHz) } WEP – wired equivalent privacy.
↳ 1997; 802.11a/b – 1999; 802.11g – 2003

WAP Security Issues – unprotected, rogue WAP, sniffing, Evil Twin, WEP Cracking

Monitor Mode – RFMON; capture pkts w/o associated WAP; SSID filtering disabled

Promiscuous Mode – capture pkts after associating; SSID filtering enabled

WEP – RC4 stream cipher, CRC-32 checksum, Open Sys Auth / Shared key Auth.
WEP40 – 40 bit key; 24 bit IV; 64 bit RC4 key
WEP104 – 104 bit key; 24 bit IV; 128 bit RC4 key

WPA – 2003; 256-bit & 384-bit HMAC
192-bit enc; 48-bit IV (WPA3)

Flow Record Processing System:
1) Sensor 3) Aggregator
2) Collector 4) Analyzer

Flow Analysis Techniques:
1) Filtering 3) Dirty values
2) Baselining 4) Activity Pattern Matching

Router	WAP
Hub, sets up LAN	wired → wireless
Wireless Router → WAP	WAP → X Router
LAN + security + transfer	access to router's established n/w

Types of Evidence:
1) Volatile – CAM table, I/O Memory, DHCP leases, history
2) Persistent – OS Image, boot loader, startup config files.

Requirements of Symmetric enc < strong enc algo
key exchange must be secure.

comp secure
cost > value time > lifetime

Type of Operations → Subst. Transp.

No. of keys → Symm. Asymm.

Plaintext Processing → Block (DES, 3DES, AES) Stream (RC4)

Assumption: enc algo is known but key is kept secret

On avg half of all possible keys must be tried to achieve success with brutforce.

Cryptanalysis (attempting to discover plaintext or key).

pseudorandom no. gen.

Ciphertext only
enc algo
Ciphertext (x_1, x_2)

Known Plaintext
enc algo
ciphertext
plain-cipher

Chosen Plaintext
enc algo
ciphertext
chosen plain-cipher

Chosen Ciphertext
enc algo
ciphertext
chosen cipher-plain

Chosen Text
enc algo
cipher
chosen { plain-cipher / cipher-plain

→ unconditional security
→ computational security

Brute Force Table (1/2)

(block size) Key Size (bits)	(Key Space) No. of Alt. keys	Time @ 1μs/dec	Time @ 10^6 dec/μs.
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 min	2.15 ms
(DES) 56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 yrs	10.01 hrs → (X)
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} yrs	5.4×10^{18} yrs.
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} yrs	5.9×10^{30} yrs.
26 char/perm.	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} yrs	6.4×10^{6} yrs.

Fiestel Structure – 1973, Horst Fiestel of IBM, Symm Block Cipher
Block size (128), Key size (128), Rounds (16), subkey Gen algo, Round Funct'on.
Fast soft enc/dec, ease of analysis.

Data Enc Std (DES) – 1977, FIPS 46 – NIST
plaintext – 64 bits, key – 56 bits, rounds – 16
proved insecure in July 1998 by EFF

3DES – 1985, ANSI X9.17

168 bits = K_1, K_2, K_3

112 bits = K_1, K_2, K_1

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

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

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

AES – Joan Daeman & Vincent Rijment, 2001 – NIST (FIPS PUB 197)
plaintext / block – 128 bits key – 128, 192, 256 rounds – 10
(44 words – 4 words subkey)
Sub bytes (S-box), Shift Rows, Mix Colms, Add Round Key (Key)

RC4 – 1987, Ron Rivest ; SSL/TLS, WEP, WPA 2
State vector – 256 bytes key – 1–256 bytes
(8–2048 bits)

Message Authentication Code (MAC) – Secret key to generate a small block of data (MAC) that is appended to the message. $MAC_M = F(K_{AB}, M)$

One-way Hash Function – accepts a variable size msg & produces a fix size digest H(M)

- variable len input
- fixed len output
- easy to compute
- given h, find x, $H(x) = h$ — pre-img resist. — 2^n
- $y \neq x$, $H(x) = H(y)$ — sec-PR, weak collision resistant — 2^n
- (x, y), $H(x) = H(y)$ — strong collision resistant — $2^{n/2}$

Bday Attack

SHA-NIST → SHA-2

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
No of steps	80	64	64	80	80
Security	80	112	128	192	256

Public Key Crypto – Bob enc msg using Alice's pub key, Alice dec. msg using her pvt key

RSA – 1977, Ron Rivest Adi Shamir Len Adleman (block cipher)

$c = M^e \bmod n$ $M = c^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

$p, q \rightarrow n = (p)(q) \rightarrow \phi(n) = (p-1)(q-1) \rightarrow e \rightarrow d \bmod \phi(n) = 1$

Diffie Hellman – $K = (Y_B)^{X_A} \bmod q$; $K = (Y_A)^{X_B} \bmod q$

Topic ..... Date.....

Classical Substitution Ciphers:

→ replacement/substitution of bits & bit patterns.

1] Ceaser Cipher – Julius Ceaser, military affairs, n=3 (default)

a b c d.e .... x y z

D E F G. H .... A B C

0 1 2 3 4 .... 23 24 25

$C = E_K(p) = (p+K) \bmod 26$

$p = D_K(C) = (C-K) \bmod 26$

Key space = 26.

Example: C = "GCUA VQ DTGCM" → try all 26 combos.

2] Monoalphabetic Cipher – shuffle the letters arbitrarily.

Key space = 26! = 4x1026 = 4104 keys. Key len = 26.

Example: p = ifiweretoa → [Z, J, K, Q, X]

c = wirfyfuh problem: language characteristics [E, T, R, I, N, O, A, S]

3] Playfair Cipher – Charles Wheatstone, Baron Playfair, 1854, encrypt multiple letters

Key = 5x5 matrix of keyword ("MONARCHY") Key Space = 26x26 = 676.

Key =

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

plaintext enc. 2 letters at a time:

1) repeated letters: "balloon" → "ba lx lo on"

2) same row: "ar" → "RM"

3) same column: "mu" → "cm"

4) else: "hs" → "BP", "ea" → "im"

4] Polyalphabetic Ciphers – Vigenere cipher, multiple cipher alphabets, letter frequencies are obscured, key len = multiple letters, Key = keyword.

Example: keyword = hello p = Iamsolost

p = I AM SO LOST

K = H EL LO HELL

C = Q EY E ....

Aids – Saint Cyr Slide, Vigenere Tableau.

Kasiski Method – Babbage/Kasiski, repetitions in ciphertext give clues to period.

Teacher's Sign. .....

4] Autokey Cipher - Key = p length, Vignere, frequency characteristics.

Example: key = deceptive.

p = we are discovered save yourself
k = deceptivewearediscoveredsav
c = ZICVTW.....

5] One-Time Pad - if a truly random key as long as msg is used, cipher is secure; C bears no statistical relation to P; use key only once; safe distribution of key.

Classical Transposition Ciphers.

Rearranging the letter order (freq dist is same as plaintext)

1] Rail-Fence Cipher

Example: p = meet me after the toga party.

M E T M E A F T E R T H E T O G A P A R T Y
E T E F E T E O A A T.

C = MEMATRHTGPRYETEFETEOAAT.

2] Row Transposition Ciphers.

Example: p = attack postponed until two am K = 3 4 2 1 5 6 7

3	4	2	1	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

C = ~~AOI~~ TTNA APTM TSUO AODW COIX KNLY PETZ.

Modern Product Ciphers - substitution followed by transposition. Ex: Rotor Machines

- Rotor Machines - Enigma, Allied Hagelin, Japanese Purple. (WW2)
  3 cylinders → $26^3 = 17576$ alphabets
- Four rotor enigma coding machine - Bombe, 1943 Ohio

Steganography - hides existence of message, high overhead cost

Topic ..... Date .....

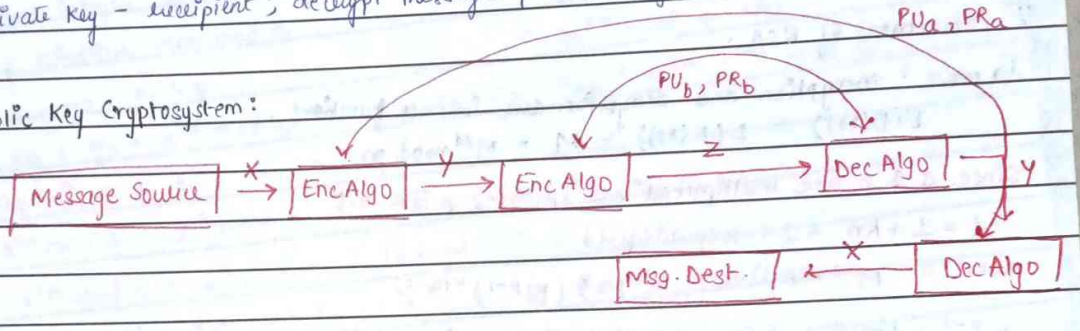
Public Key Cryptography :

1976 ; 2 keys - public & private ; parties are not equal ; key distribution and digital certificates / signatures — Whitfield Diffie & Martin Hellman

1] public key - anyone ; encrypt messages & verify signatures

2] private key - recipient ; decrypt messages & create signatures

→ Public Key Cryptosystem :



Applications :

Algorithm	Enc/Dec	Digital sign.	Key Exchange
RSA	✓	✓	✓
Elliptic Curve	✓	✓	✓
Diffie Hellman	X	X	✓
DSS	X	✓	X

Requirements : infeasible to find dec key ; easy to compute algo ; one for enc one for dec.

Trapdoor one-way function - enc with public key is easy, dec with pvt key is hard

Modular Arithmetic

$a = b \pmod n$ ↔ there is a q s.t $a - b = qn$

b is the remainder after dividing a by n. $(23 = 8 \bmod 5)$

$(a \bmod n + b \bmod n) = (a+b) \bmod n$

$(ab) \bmod n = (a \bmod n \times b \bmod n) \bmod n$

Multiplicative inverse : n ≥ 1, a & n are relatively prime

$ax = 1 \bmod n$

$a = 3 \quad x = 2 \quad n = 5$

$6 = 1 \bmod 5$

Fermat's Little Theorem : p is prime, ∀a

$a^{p-1} = 1 \bmod p$

Chinese Remainder Thm : p, q prime, ∀a, x

$x = a \bmod p$ & $x = a \bmod q$ iff $x = a \bmod pq$

Teacher's Sign. .....

RSA Algorithm: vulnerable to CCA

1977, Rivest Shamir Adleman - MIT, security due to cost of factoring large numbers (1024 bits)

$O(e^{\log n \log\log n \log\log n})$ operations

1) pick 2 large (100 digit) primes p & q
2) $n = p \times q$
3) Select d that is prime to $(p-1)(q-1)$
4) $ed = 1 \bmod (p-1)(q-1)$, find e
5) (d,n) is public key, (e,n) is private key.

$E(M) = M^e \bmod n = C$

$D(C) = C^d \bmod n = M$

Euler's Thm: $a^{\phi(n)} \bmod n = 1$ $\quad \gcd(a,n) = 1$

Correctness of RSA:

To prove: encryption and decryption are inverse functions.

$E(D(M)) = D(E(M)) = M = M^{ed} \bmod n$

Since d & e are multiplicative inverses, $\exists K$ s.t

$ed = 1 + Kn = 1 + K(p-1)(q-1)$

$Med = M^{1+K(p-1)(q-1)} = M * (M^{p-1})^{K(q-1)}$

$M^{p-1} = 1 \bmod p$ (Fermat's Little Thm) $\Rightarrow$ $Med = M(1)^{K(q-1)} \bmod p = M \bmod p$

$Med = M(1)^{K(p-1)} \bmod q = M \bmod q$

By Chinese Remainder Thm: $M^{ed} = M \pmod p \pmod q = M \bmod pq = M \bmod n$

Example: $p = 11$ $q = 13$ $M = 42$ a) public key b) private key c) ciphertext

Select e: $\gcd(\phi(n), e)$.

$n = p \times q = 11 \times 13 = 143$

$\phi(n) = (p-1)(q-1) = 10 \times 12 = 120 = 3 \times 2 \times 2 \times 2 \times 5$

Let's take $d = 7$, find e?

$e * 7 = 1 \bmod 120$ $\quad \therefore e = 103$

(a) $(d,n) = (7,120)$

(b) $(e,n) = (103,120)$

$E(M) = M^d \bmod n = 42^7 \bmod 143 = 81$

$D(C) = C^e \bmod n = 81^{103} \bmod 143 = 42$

Example: $p = 11$ $q = 3$ $M = 7$ a) public key b) private key c) ciphertext

$n = p \times q = 11 \times 3 = 33$

$\phi(n) = (p-1)(q-1) = 10 \times 2 = 20$

prime d s.t $1 < d < \phi(n) = 3, 7, 11, 13, 17, 19$.

Let $d = \phi^3$ find e? $\quad ed = 1 \bmod \phi(n)$

$e \times 3 = 1 \bmod 20$ $\quad \therefore e = 7$

(a) $(d,n) = (3,33)$

(b) $(e,n) = (7,33)$

$E(M) = M^d \bmod n = 7^3 \bmod 33 = C = 13$

$D(C) = C^e \bmod n = 13^7 \bmod 33 = M = 7$

Topic ..... Date .....

Diffie-Hellman Key Exchange:

Williamson 1970, DH 1976, public exchange of secret keys; based on exponentiation in a finite field; security - difficulty of computing discrete logarithms.

1) large prime integer q
2) a being primitive root mod q
3) Secret Key no: $x_A < q$
4) public key: $y_A = a^{x_A} \bmod q$

K_{AB} = shared session key
$= y_A^{x_B} \bmod q$ (B)
$= y_B^{x_A} \bmod q$ (A)

$Z_A = Z_B = K_{AB} = a^{x_A}, a^{x_B} \bmod q$

Example: $Z_A = K_{AB} = ?$ $q = 11$ $a = 2$ $x_A = 9$ $x_B = 4$

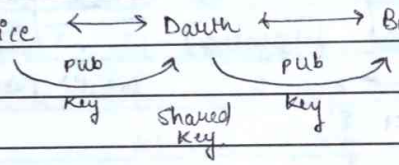
$y_A = a^{x_A} \bmod q = 2^9 \bmod 11 = 512 \bmod 11 = 6$

$y_B = a^{x_B} \bmod q = 2^4 \bmod 11 = 16 \bmod 11 = 5$

$Z_A = K_{AB} = y_B^{x_A} \bmod q = 5^9 \bmod 11 = 9$ } $Z_A = Z_B$.

$Z_B = K_{AB} = y_A^{x_B} \bmod q = 6^4 \bmod 11 = 9$ }

MITM:



Elliptic Curve Cryptography:

- smaller bit sizes; x, y & coeffs

elliptic curve is a single element = O

$y^2 = x^3 + ax + b$ (cubic) $P + Q = R$ (reflection) $O = -O$ (additive identity)

$P(x, y)$ then $-P = (x, -y)$ $P + (-P) = P - P = O$ $Q + Q = 2Q = -S$

Security: Pollard Rho method

prime curves $E_p(a,b)$ binary curves $E_{2^m}(a,b)$

EC logarithm problem: $Q = kP$, easy given kP, hard given Q

Pros: shorter key length, better security, performance

Cons: newer field, not perfect

Pseudorandom Number Generation (PRNG) based on Asymmetric Encryption:

random output ; slower ; short bit sequence

Micali - Schnorr PRNG using RSA

Key Exchange:

Key distribution ; Key Agreement ; Key Management ; Public Announcement ; Publicly available directory ; Public Key Authority ; Certificate ; X.509 v3 DS

Message Authentication DS:

MAC, HMAC, MD5, SHA, RIPEMD-160, DS

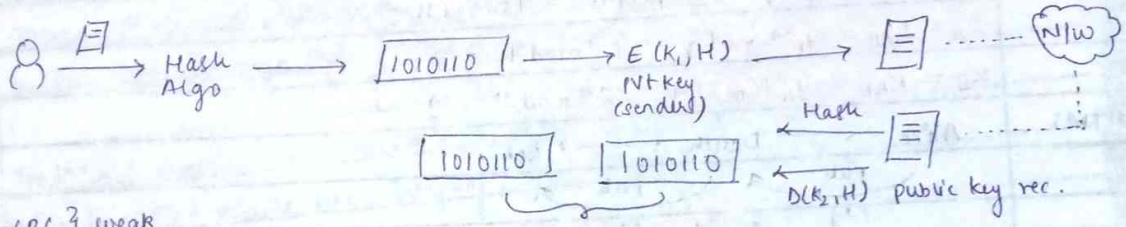
↳ + enc. authentication

Msg + MAC (1) — sym enc

MAC (2) — Sym enc.

Shared key(s) — MAC || S — hash → Hash + M (3)

Hash + M (4) — enc



XOR, CRC } weak

Bday Attack: 64-bit ?

msg = x → h(x) = y ↓

$2^{m/2} \rightarrow x$

$2^{m/2} \rightarrow y$ } prob of same

prob > 0.5

Req of Hash: variable inp, fixed o/p,

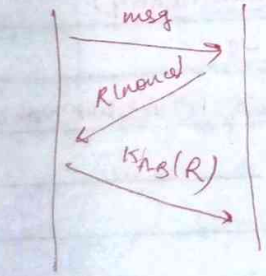
H(y) = x — (1) y = ? Pseudorandomness

H(y) = H(x) (2)

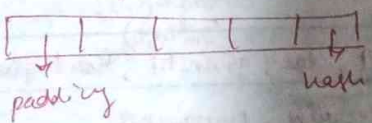
(x, y) → H(y) = H(x) ← CR

→ BF, preimage attack, collision resistance

hash strength → $2^{m/2}$



Block Cipher as Hash:



64-bit bday attack

MD5: RFC1321

(1) padding

(2) 512-bit blocks

(3) MD = A|B|C|D (32-bit)

16 words 4 rounds. 16 steps.

(4) o/p size 64-bit

SHA

o/p size: 160-bit

SHA512 — (1) Compute: 1024-bit block 80 rounds

SHA3 — 2012

Security, flexibility, scalability.

Topic ..... Date.....

UNIT 5 : NETWORK FORENSICS

Defn: Obtaining & analyzing digital information often as evidence in civil, criminal, or administrative cases — Computer Forensics. — inculpatory / exculpatory

- Network Forensics
- Data Recovery
- Disaster Recovery

Digital Evidence :

Locard's Principle ; forensic soundness ; Admissibility ; Authenticity

where ? - filesystems, RAM, physical storage, slack space, unallocated space, layer

NF challenges: Access to IP addresses, Data Integrity, High Speed Data Transmission, Data Extraction location, Data privacy, Data storage

Traditional Forensics - non-volatile data, disk, event logs, registry

↓ Live Forensics - volatile data, integrity, RAM memory.

Challenges: access to the system, minimize impact, footprints, timely

1. Retrieval 2. Imaging 3. Analysis.

Tools: binwalk, bulk extractor, hash deep, magic rescue, guymager, pdfid, autopsy

Attacks: SSL Authentication, Ping flood, buffer overflow, SQLi

Attack log Generation.

identical to real log file

timestamp : attack type : protocol : source IP : dest IP : country : Threat level : freq

$$\text{Danger level} = \frac{(\text{Freq}/\text{Time}) + \text{Threat level}}{2}$$

→ Severe, High, Elevated, Guarded, Low

upper limit confidence interval = threshold/baseline

OSCAR - Methodology

Obtain ~~Evidence~~ Info, Strategize, Collect, Analyze, Report.

Teacher's Sign. .....

Teacher's Sign. .....

Topic ..... Date .....

UNIT 2 - PENETRATION TESTING

Defn: evaluation of strengths of all security controls, procedural, operational and technological controls; any organization processing & storing private information; performed on a regular basis; PCIDSS Section 11.3; HIPAA sec 8.

External v/s Internal Overt v/s Covert

Phases:

1] **Reconnaissance & Information Gathering:**
discover information about target without making contact with them/it.
whois; google; browsing; OSINT.

WHOIS: Domain name, registrant, Administrative contact, Technical contact, Name Servers.
→ extracting info; ~~nslookup~~, ~~superscan~~, ~~GetAcct~~, ~~SNMP port scan~~.

2] **Network Enumeration & Scanning:**
discover existing n/w, live hosts, services running on these hosts.
nmap; autoscan; DNS Querying; traceroute.

3] **Vulnerability Testing & Exploitation:**
check hosts for known vulnerabilities & their severity, whether or not these can be exploited.
Nessus, OpenVAS, login checks, ~~bruteforce~~, Metasploit, Core Impact.
Fuzzing, 0day prog. analysis, post exploitation techniques → severity

4] **Reporting:**
organize & document information; Dradis
host, services, hazards, risks, recommendations.

PTES: Penetration Testing Execution Standard
baseline fundamentals for performing a penetration test.

Teacher's Sign. .....

Date.....

PTES Phases:

1] Engagement - scope & terms ; goals ; expectations ; total access
2] Intelligence Gathering - OSINT ; probe an organization ; test web apps
3] Threat Modelling - where ; what (firm) ; what (target)
4] Vulnerability Analysis - port scans ; banner grabbing ; info from OSINT .
5] Exploitation - brute force ; good testers v/s bad testers .
6] Post Exploitation - target specific systems , critical infrastructure , valued information
7] Reporting - executive summary , presentation , findings , remediate security holes .

Vulnerability Scanners:

automated tools to identify security flaws ; fingerprinting ; scan the OS .
a pentest cannot be completely automated ; business knowledge .
first phase of active hacking ; locate target systems
↳ Enumeration : identify names, comp names, shares

Port n/w Vulnerability

Well known Port Nos : C:\Windows\system32\drivers\etc\services .

CEH Scanning Methodology : check for live systems (ping) → check for open ports (nmap) → Scan beyond IDS → perform banner grabbing → scan for vulnerabilities → draw n/w diagrams → prepare proxies .

More Tools - IPEye , IPSecScan , hping , SNMP

Ping Sweep Techniques:

ICMP scanning ; live hosts & systems ; ICMP Echo request ; Echo Reply
Tools - Pinger, Friendly Pinger , WS_Ping_Pro
Drawbacks - firewall , IDS alerts , system must be ON
Solutions - port scanning .

Nmap Command Switches:

Ping sweeps , port scanning , service identification , IP detection , OS detection
OS - linux, unix, windows .

open / filtered / unfiltered ports
SYN+ACK (RST) ↔ (ICMP error)

-sT , -sS , -sF , -sX , -sN , -sP , -sU , IDLE

War Dialing Techniques :

automatically scan a list of phone numbers to search for modems , computers , bulletin board systems
remote-access servers & modems (PAP)
Tools : THC-Scan , PhoneSweep , TeleSweep .

Topic ..... Date.....

Banner Grabbing & OS Fingerprinting.

determine OS running on a remote target system through response headers.

Tools - Solarwinds, Queso, Harris Stat, Cheops, Netcraft, HTTrack

Active: specially crafted packets; database; TCP stack; IDS detection

Passive: error messages; sniffing n/w traffic; page extension; URL accurate

Scanning Anonymously:

Proxy: intermediary b/w hacker & victim; through; hide attack; connections ~~→ Sockschain~~.

Tunnel: tunnel a blocked protocol through an allowed protocol (HTTPort, TunnelID)

SNMP Enumeration:

application layer; UDP to manage n/w devices

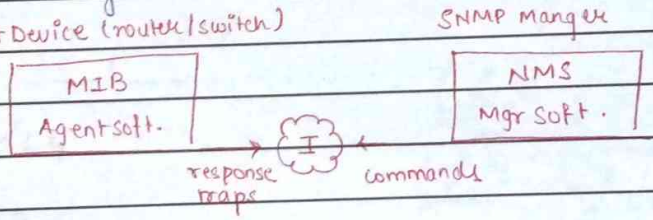
user acc, pwd, group, sys names, device.

community strings → read, read/write

Managed device: host having SNMP service enabled (n/w devices) Tools - SNMPUtil, # IPN/w Browser.

Agent: software running on managed device; convert info into SNMP compatible format

N/w Mgmt Sys: software; monitoring n/w devices; comms with agent



Security Operations Centre (SOC):

detecting, analyzing & responding to cybersecurity incidents in an org.

Need: proactive TI, MTTD/MTTR, Compliance, Scalability/Flex, Improved IR

Benefits: Real time monitoring & alerting, proactive security, compliance, effective IR, comprehensive views, customer responsibility.

Teacher's Sign. .....

protocol

Securing Incident & Event Management (SIEM):

real time analysis of security alerts generated by n/w hardware & application

Importance - detection & respone, compliance, log mgmt, TI, IR, cost effective

components - Event correlation & Normalization, Alerting, Reporting, Investigation

Benefits - improved threat detection & respone; reduced risk; IRM; cost savings; improved viability & control; enhanced TI.

MITD/MITR - real time, automated, centralized, analyses

Compliance & Risk Mgmt - assessment, auditing, accountability, planning, execution

* Ip Internet protocol

10.11.12.13

.12
.12

11111111

00001010

10.11.12.0

10.0.0.0

10.11.0.0

192.168.1.0

10.0.0.0
172.16.0.0

0/24
0/18
0/8

255.255.255.0

11111111

10.0.0.0/24

10.0.0.0/16

192.168.18.0/24

192.168.18.0/18

1.0.0.0

11111111.0000.0000.0000

131-255

131

255.0.0.0

255.255.255.0

111/1111.11111111.111111.0000

0.1

192.168.1.1

192.168.18.63

64

127.0.0.0

0-126 A
128-172 B
172.16.22 C

192.--

192.168.2.1

3.1

8.8.8.8

127.56.120.3

115.13.2.1

115.13.49.3

69.23.4.4

69.13.16.58

12.16.13.15

N H

129.16.13.2

N H

193.10.13.2

N H

128
64
32
16
130

111

0-7