CS Final 2021 Sol.

1- • One-time Pad is a CryptoSystem where the Key used for encryption is
  → as long as the message
  → generated in random fashion
  → used only once

• Encryption is given by $C = M \oplus K$ and decryption is given by $M = C \oplus K$ where $\oplus$ is bit-wise XOR

• It is unbreakable & exhibits Perfect Secrecy as it produces an output that bears no relationship with the Plaintext

2-

However,

main drawback
- → Key distribution & Protection are serious issues due to the length of the key and the use once constraint. thus, limited to applications where key is sent out-of-band (e.g. via real Person)
- → generating a large no. of random numbers is also a significant task

3-

$V = 2^{20}$ encryptions/sec

- Key is 40 bits long $\rightarrow$ 2^{40} Possible keys

Avg. # Encryptions needed $= 2^{39}$

$$t = \frac{2^{39}}{2^{20}} = 2^{19} \text{ seconds} = 145.6 \text{ hours}$$

$$\simeq 6 \text{ days}$$

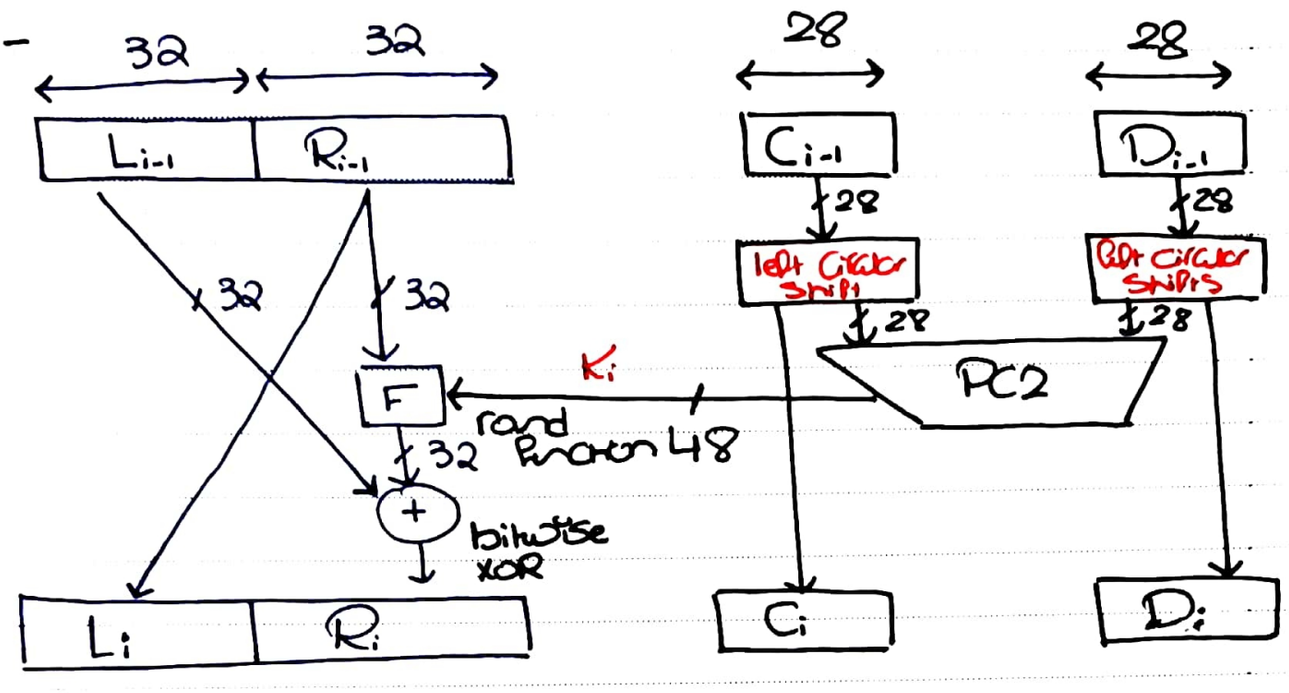
- When the useful time of the message is beyond 6 days (e.g., knowing missile locations in a cold war) meanwhile not practical apps about buying certain stocks in 24 hours.

- Key is 80 bits long $\rightarrow$ 2^{80} Possible keys

$$t = \frac{2^{79}}{2^{20}} = 79428564.86 \text{ Centuries}$$

- No scenario in which this would be practical

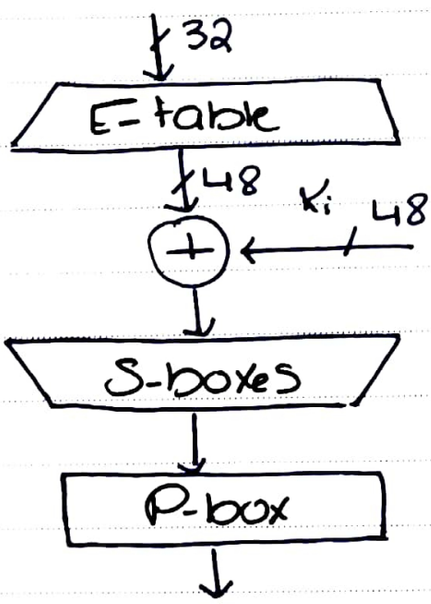
4-



#Annotate!

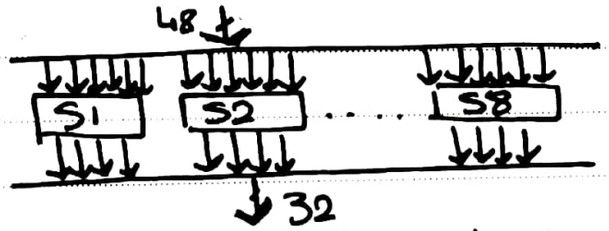
- PC2 discards specific 8 bit positions then applies a defined Permutation

- Round Function



- Duplicates some bits then applies a defined Permutation

- bitwise XOR



- Applies defined Permutation

- each box uses a matrix & 6 input bits to choose 4 bit element.

5-

- Rail Fence Cipher is a transposition cipher where to encrypt, the Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows (and vice versa for decryption)

- The Key is the no. of rails in the rail fence

e.g., to encrypt the Previous line with 3 rails

```
T     e     t     o     a     i     ...
  h   K   y   s   h   n   o   r   i   s   n   h
    e       i       e       P       l       t
```

→ then C = "Tetoai...." (row by row)

6- Modes of operation of DES

Electronic Codebook

- Secure transmission of single values/ short messages

Cipher block Chaining

- General Purpose block-oriented transmission
- authentication

Cipher Feedback

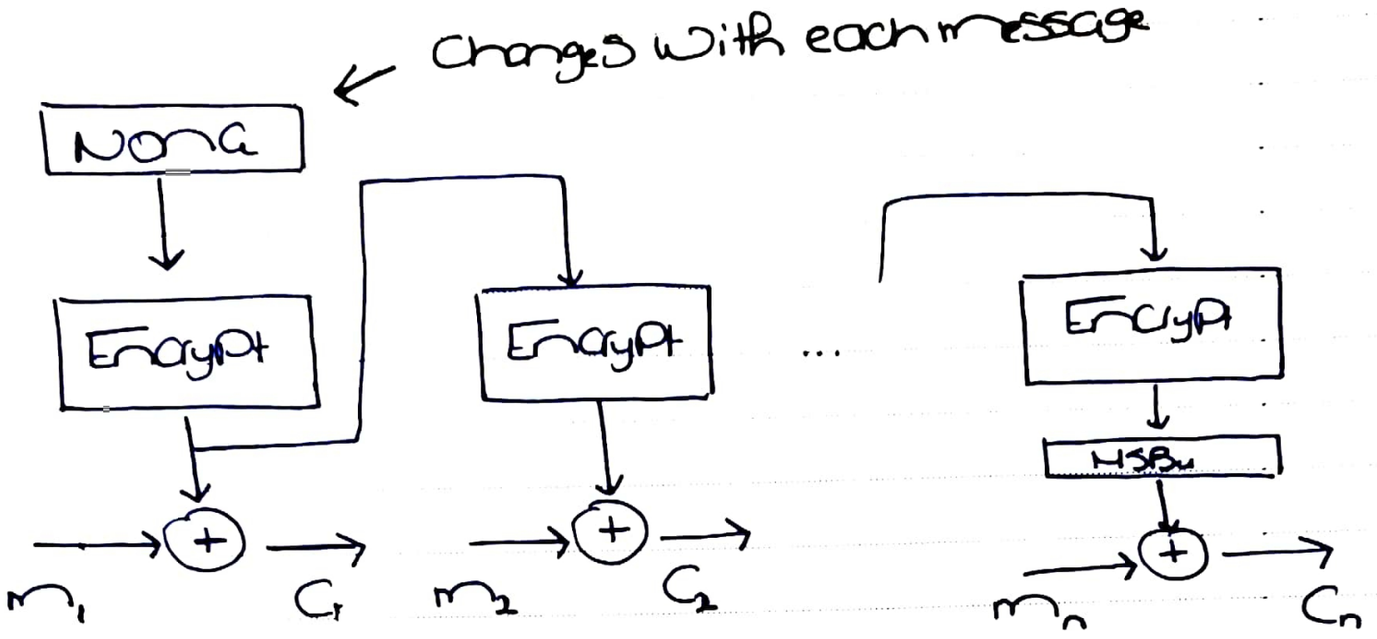
- General Purpose stream-oriented transmission over noisy channel
- authentication

Output Feedback

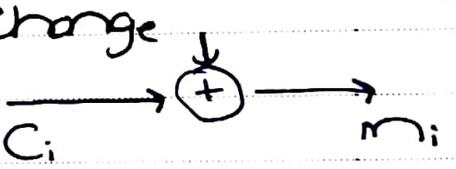
over noisy channel

- General Purpose block Oriented transmission @ high speed

7-



- ~~The message is Partioned into n b-bit blocks,~~ no need
- $M = m_1 \| m_2 \| \ldots \| m_n$ (each is b-bits; can be u<b bits)
- For decryption, only change



9-

HMAC Design Objectives

1- Directly use available hash functions (freely available & with no need for modification)

2- Allow replacibality of the hash function when another version is faster/more secure

3- Preserve the hash function's original performance

4- Be able to analyze the strength of the authentication mechanism based on hash func

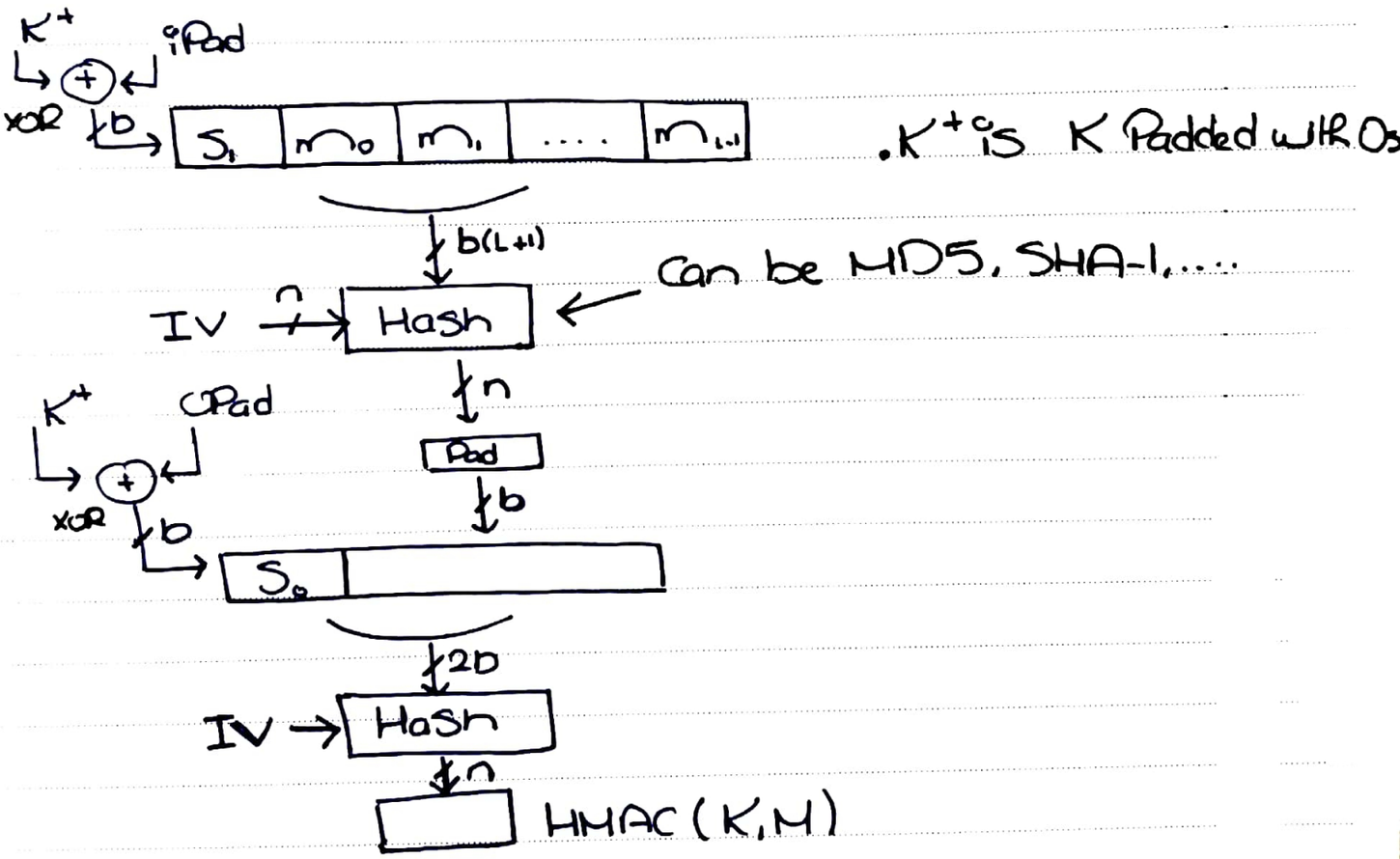
- Allow simple use & handling of keys

$$HMAC = H(S_o \| H(S_i \| M))$$

$$S_i = K^+ \oplus iPad \;,\; iPad = \underbrace{36\|36\|\ldots\|36}_{b/8}$$

$$S_o = K^+ \oplus oPad,\; oPad = 8C\|8C\|\ldots\|8C$$

$M = m_0 \| m_1 \| \ldots \| m_{L-1}$ each of size b bits



⇒ The extra overhead is 3 executions of the hash function's compression function F (one for S_i, one for S_o and one for the output from 1st hash)

8- Needham Equations:

acquiring session key:

$A \rightarrow KDC: \quad ID_A \| ID_B \| N_1$

$KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| N_1 \| [E(K_b, K_s \| ID_A)]])$

$A \rightarrow B: \quad E(K_b, K_s \| ID_A)$

challenge/response:

$B \rightarrow A: \quad E(K_s, N_2)$

- B knows K_s

$A \rightarrow B: \quad E(K_s, f(N_2))$

- B must be talking to A (fresh msg with K_s)

→ Suppose an old session key was leaked and that B doesn't keep track of old session keys then an adversary D can replay $E(K_b, K_s \| ID_A)$ and successfully impersonate A

$D \rightarrow B: \quad E(K_b, K_s \| ID_A)$

$B \rightarrow D: \quad E(K_s, N_2')$

$D \rightarrow B: \quad E(K_s, f(N_2'))$

Can be countered by using timestamps under proper clock synchronization

2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_A \| N_1 \| T \| E(K_b, K_s \| ID_A \| T)])$

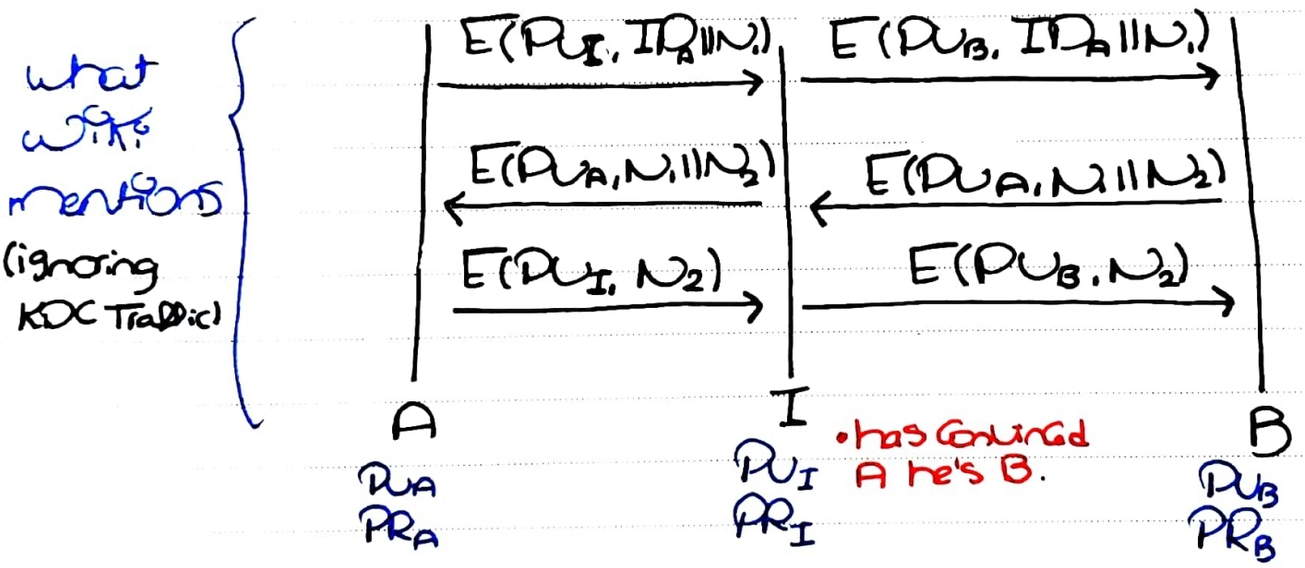
3. $A \rightarrow B: \quad E(K_b, K_s \| ID_A \| T)$

- then B must check that $|Now - T| < \Delta t_1 + \Delta t_2$

  - Now: time of session key generation
  - Δt_1: delay
  - Δt_2: synch.

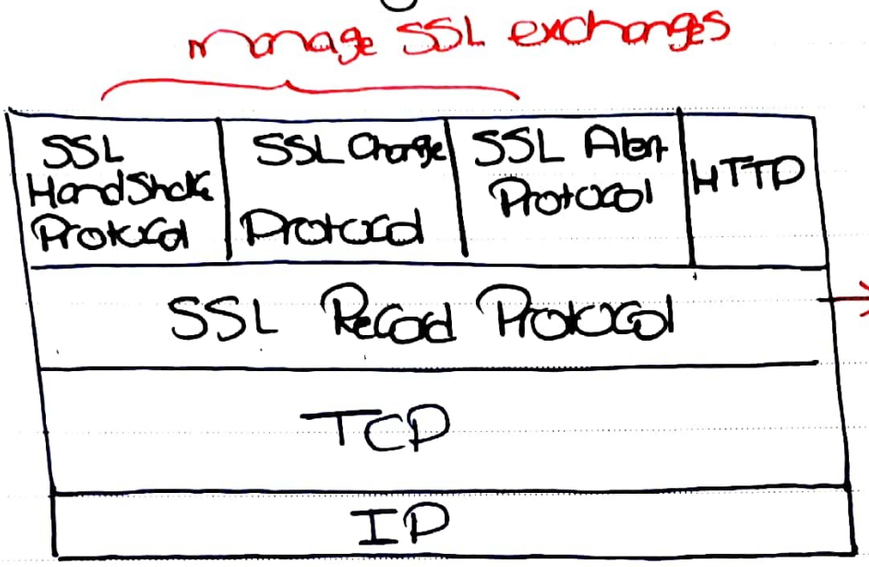
10- Needham suffers from man-in-the-middle attack:

→ Could not find a mention of this in the book but Wikipedia & research gate mention it for Needham-Schroeder Public Key Protocol (Pretty much Symmetric Key distribution using asymmetric Key: Public Key authority)



• Now B falsely believes that A is communicating with him when it's I.

11- SSL Stack Diagram

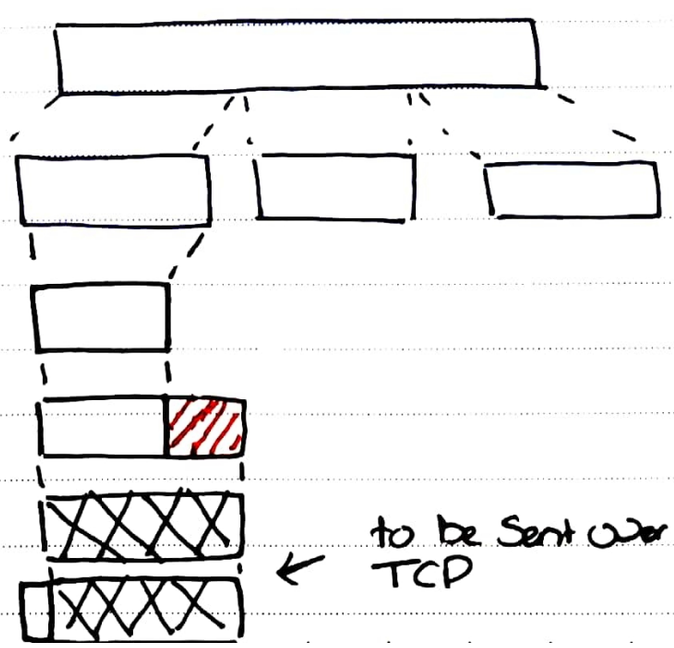


12. Confidentiality
→ through encryption of SSL Payloads

Keys def. in handshake *

Message Integrity
→ through message authentication code

Operation of SSL record Protocol:



Fragmentation

Compression

ADD MAC

Encrypt

Append Header
- type
- version
- length

13. RSA Question

Key Generation

Choose $n = pq$ $\quad p \neq q$, Large Primes
Compute $\phi(n) = (p-1)(q-1)$
Choose e such $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$
→ Public Key is $\{e, n\}$

Compute $d = e^{-1} \bmod \phi(n)$
→ Private Key is $\{d, n\}$

To send a message $M < n$: #encrypt

$$C = M^e \bmod n$$

to receive: # decrypt

$$M = C^d \bmod n$$

14. Diffie-Hellman Methodology

Global Elements: Large Prime q, one of its Primitive roots α

Alic	Bob
• generate random $X_A < q$	• generate random $X_B < q$
• Compute $Y_A = \alpha^{X_A} \bmod q$	• Compute $Y_B = \alpha^{X_B} \bmod q$
→ make it Public (exchange)	→ make it Public
• Compute $K = Y_B^{X_A} \bmod q$	• Compute $K = Y_A^{X_B} \bmod q$

Derivation:

$$K_B = Y_B^{X_A} \% q = (\alpha^{X_B} \% q)^{X_A} \% q$$

$$= \alpha^{X_B X_A} \% q$$

$$K_A = Y_A^{X_B} \% q = (\alpha^{X_A} \% q)^{X_B} \% q$$

$$= \alpha^{X_A X_B} \% q$$

Clearly $K_A = K_B$ and hence they compute the same Shared Key

16. $q = 71$ $\alpha = 7$ # global elements

Alice

$X_A = 5 < q$

$Y_A = 7^{5 < X_A}_{\to \alpha} \% 71_{\to q}$

$= 7^4 \cdot 7 \% 71$

$= 51$

$K = Y_B^{X_A} \% q = 4^5 \% 71$

$= 30$

Bob

$X_B = 12 < q$

$Y_B = 7^{12 < X_B}_{\to \alpha} \% 71_{\to q}$

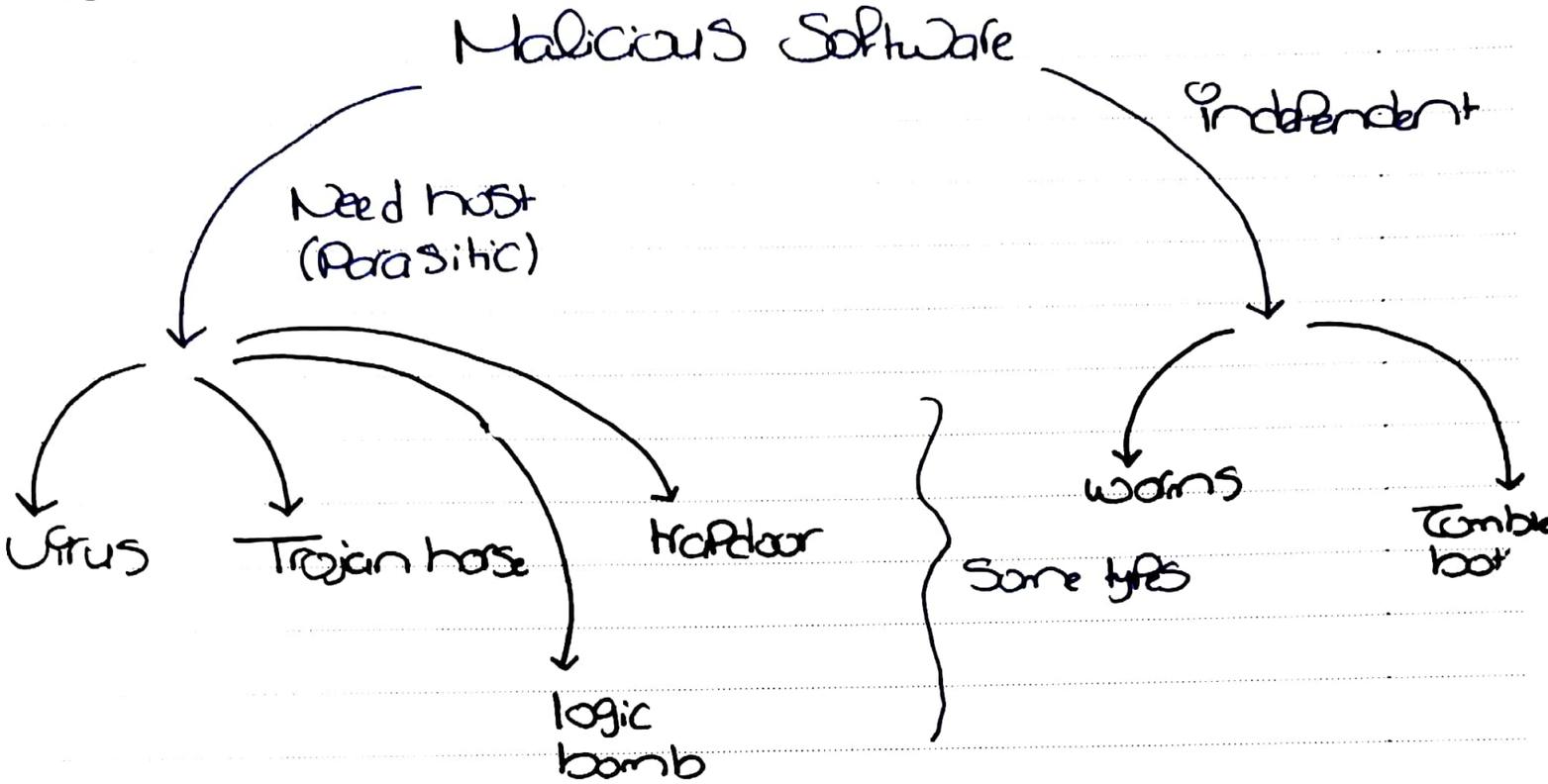
$= (7^4)^3 \% 71$

$= 4$

$K = Y_A^{X_B} \% q$

$= (51^3)^4 \% 71 = 30$

15.



Virus: Piece of software that can infect other programs by modifying them (inject routines that perform harmful effect / copies of the virus)

Trojan Horse: Apparently useful program with hidden code that when triggered performs harmful effect.

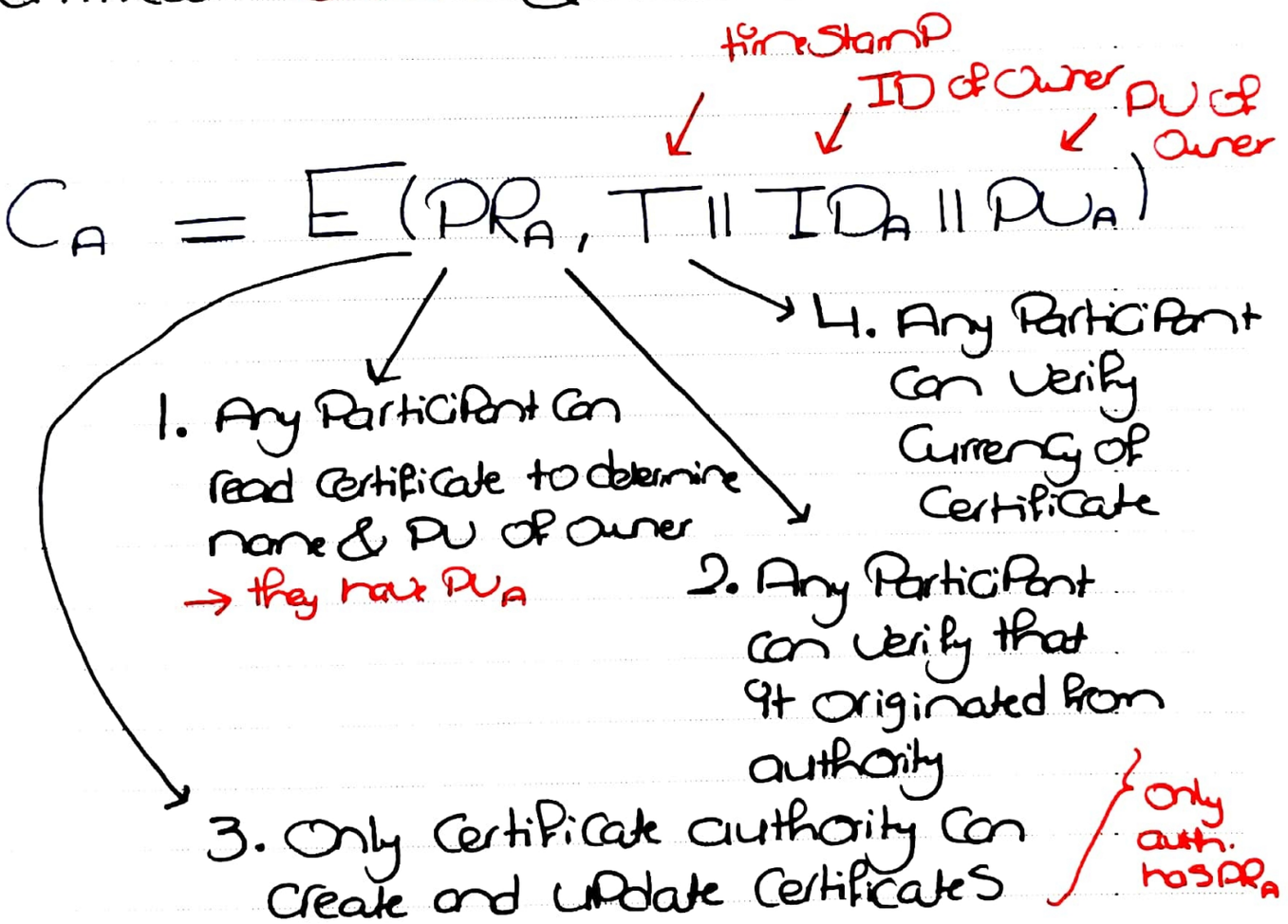
Logic Bomb: Code embedded in a legit program that is set to explode when certain conditions are met.

Trap door: Secret entry point to the program that allows access without going through usual security procedures

Worms: Program that can replicate itself and send copies from computer to computer across network connections

Zombie, bot: Program activated on infected machine to launch attacks on other machines.

16- Certificate Content & requirements



17-

A record of ongoing activity by users. It consists of a sequence of audit tokens each containing info about an event being audited.

- They are a fundamental tool for intrusion detection:
  - → used in the Profile-based approach of statistical anomaly detection where
    - Analyze audit records over a period of time to determine profile of avg. user
    - Analyze new audit records by applying a (statistical) test to determine deviation from average behaviour.

after considering quantative metrics to measure behaviour

  - → used in the anomaly detection approach of rule-based detection
    - Automatically generate rules based on analysis of past audit records
    - Observe current behaviour and see if it conforms with rules

18-

- A Honey Pot is a decoy system designed to divert potential attackers away from critical systems.

Designed to

- Divert attackers from accessing critical systems
- Collect information based on attacker's activity
- encourage them to stay on it for long enough for admins to respond.

How is it used? // An attempt

→ A decoy system is filled with fabricated info that a legitimate user wouldn't access but that an intruder would.

→ the system is instrumented with sensitive monitors & event loggers that detect access and collect attacker activity info.

→ Meanwhile, admins log & track the attacker.

19-

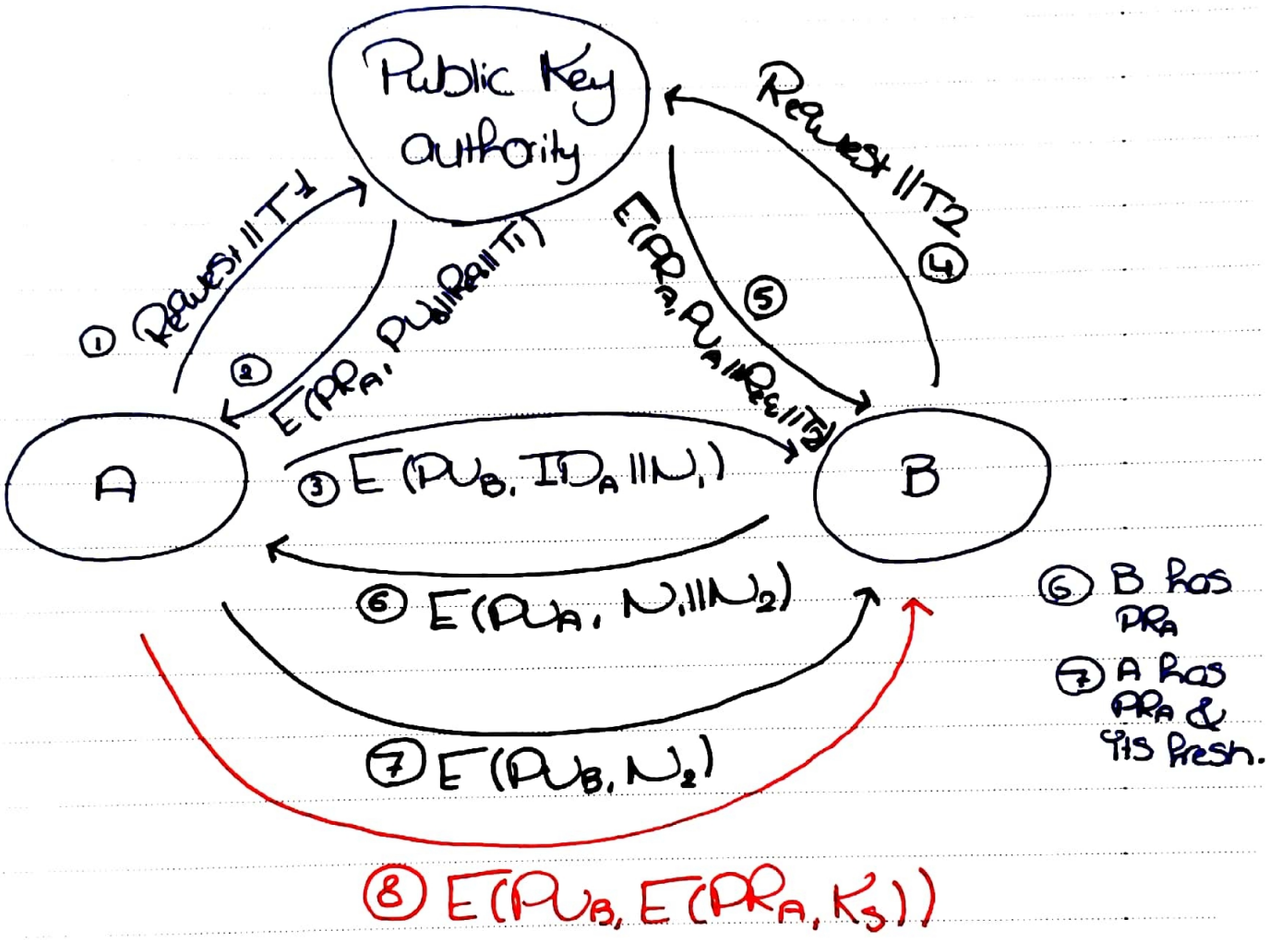
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

For each pair

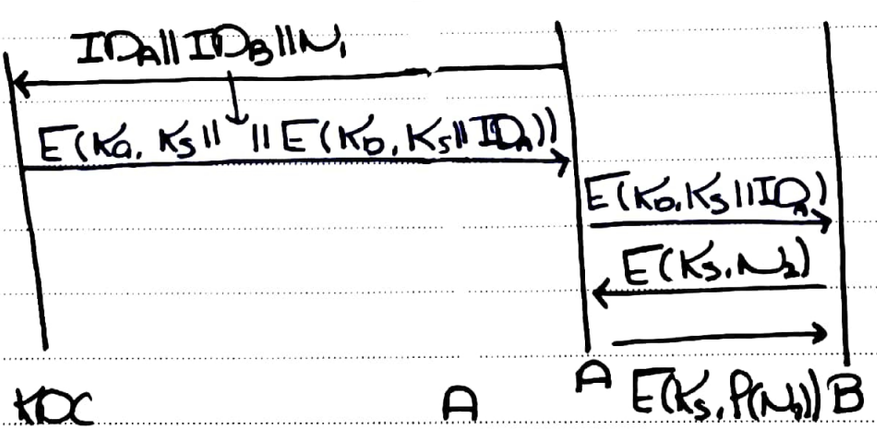
- Same row
  - Shift right by 1.
- Same column
  - Shift down by 1
- Form a box
  - Take the other 2 corners

→ If any pair has duplicate letters insert X in the middle then form pairs again.

20- Assuming it meant "without having each other's Public Keys"



→ If they don't have Public Keys in the sense that we should consider Symmetric Key distribution using Symmetric encryption then



21- Types of Intruders

Masquerador
- Outsider
- Not authorized to use the System
- exploits legitimate user account by penetrating access controls

Misfeasor
- Insider
- legitimate user
- access data/resources for which such access is unauthorized

Clandestine User
- Insider or outsider
- Try first seize supervisory control of the system then use it to evade auditing, access controls, SPRs audit Colec

22- Intrusion Detection Techniques

Statistical anomaly detection

1. Collect data of legit behaviour overtime
2. Apply Statistical tests on observed behavior to detect intrusion.

Rule-based detection

- Define a set of rules that decide if given behav. is that of an intruder.

23-

→ Is x^3+x^2+1 a Prime Polynomial (Irreducible)

* Should be not divisible by x or $x+1$
  - Clearly not divisible by x

$$
\begin{array}{r|l}
x^2 & \\
\hline
x+1 & x^3+x^2+1 \\
 & x^3+x^2 \\
\hline
 & 1 \leftarrow \text{has remainder}
\end{array}
$$

  - It's divisible by neither, hence a Prime Polynomial (not reducible)

→ How about x^3+1
  - Clearly not divisible by x

$$
\begin{array}{r|l}
x^2+x+1 & \\
\hline
x+1 & x^3+0x^2+1 \\
 & x^3+x^2 \\
\hline
 & x^2+1 \\
 & x^2+x \\
\hline
 & x+1 \\
 & x+1 \\
\hline
 & 0 \leftarrow \text{No rem.}
\end{array}
$$

} Divisible by $(x+1)$ Hence reducible in GF(2)

| 24)
| In CTR, OFB Can PreProcess
| → encrypt Prev output/counter

25-

gcd(4321, 1234)

$4321 = 3 \times 1234 + 619$

$1234 = 1 \times 619 + 615$

$619 = 1 \times 615 + 4$

$615 = 153 \times 4 + 3$

$4 = 1 \times 3 + 1$

$\because \gcd(3, 1) = 1$

$\gcd(4321, 1234) = 1$

26- $n = 3599 \quad e = 31 \quad d = ??$

- Need to factorize n, look for Primes below $\sqrt{3599} = 60$
  → 59 is a solution

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29...

$n = pq = 59 \times 61, \quad \phi(n) = 58 \times 60 = 3480$

$d = 31^{-1} \bmod 3480$

→ need gcd(3480, 31)

$3480 = 112 \times 31 + 8$

$31 = 3 \times 8 + 7$

$8 = 1 \times 7 + 1$ $\qquad$ $\gcd(7,1) = 1$

$1 = 8 - 7$

$= 8 - (31 - 3 \times 8) = 4 \times 8 - 31$

$= 4 \times (3480 - 112 \times 31) - 31$

$= 4 \times 3480 - 449 \times 31$ ← the inverse of $e = 31$ under mod $\varphi(n) = 3480$

$= (-449 + 3480) \bmod 3480$

$= 3031$ ← $d = e^{-1} \bmod \varphi(n)$

27- $C = M^e \bmod n$

28- ECB used for short data as it exposes structural repetition.

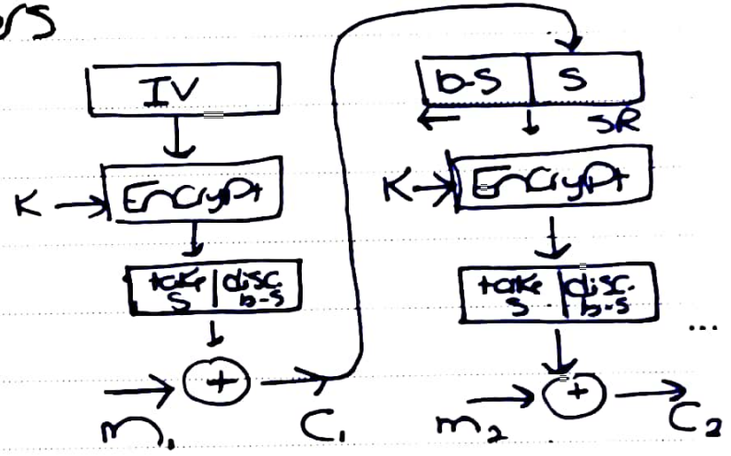
29- DES round key size is 48 bits input data size is 64 bits

30 - 8 - Sboxes

T/F:

1- For B only to read, encrypt with B's Public Key

2- CFB is a block ciphermode that can generate stream ciphers



3- False, It doesn't give a way to recover the data (disclosure not possible regadless to authorized or not)

4- False, for the same reason as 3

Write the Scientific term #Solved