

System and Network Security

Quiz - 1

2-Feb-2021

Raman Shukla

2020201098

1

a One Time Passwords (OTP) can be called ^{secure as} they have ^{time} factor

b

$$c \quad \frac{64}{2^{56}} = \frac{2^{-50}}{2^{56}} //$$

d DLL and transport

e Symmetric Key Encryption (Block Cipher)

f Yes, because we ~~use~~ ~~encryption~~ encrypt our keys before passing to the links/nodes ~~and~~ ~~it is~~ although we can't decrypt it at receiver end too.

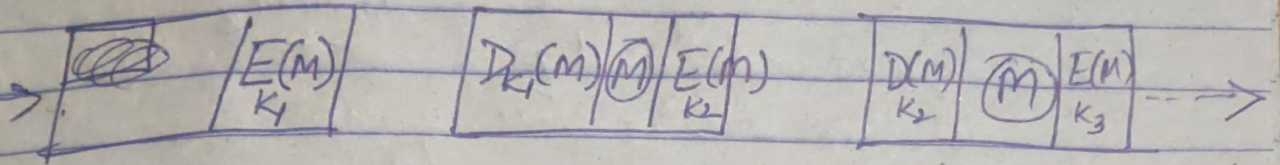
g Order of Substitution keys

h No.

i IDEA

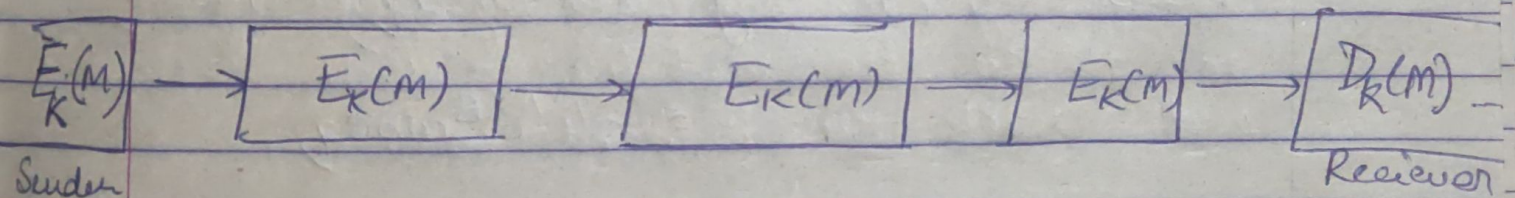
j MAC uses private key, Hash not.

② (b) Link by Link encryption is done at every link/node.



- It is easy to implement at hardware level.
- An attacker cannot decode just by looking at packets.
- But the Link/Node itself is vulnerable since it has the original decrypted message momentarily which can be exploited.

→ End-to-End encryption is where we encrypt the message at upper layers even before passing to the physical layers.



- It is very secure but routing information is not encrypted thus it is susceptible to traffic analysis.
- No node has the original content, only receiver/sender.

★ ★ Thus, if we combine both then :-

- ① Link-Link encryption will make traffic analysis impossible and by end-end there would be no vulnerable data at any node.
- ② Both algo can separately manage their keys too.

③ Lets say x_A and x_B are same :-

Alice :- $(\alpha^{x_A} \bmod q) \xrightarrow{\text{Hashkey}_A} \text{Bob}$

Bob :- $(\alpha^{x_B} \bmod q) \xrightarrow{\text{Hashkey}_B} \text{Alice}$

Now :- Alice :- $\boxed{(\overset{y_B}{\text{Hashkey}_B})^{x_A} \bmod q}$

Bob :- $\boxed{(\overset{y_A}{\text{Hashkey}_A})^{x_B} \bmod q}$

$$\begin{aligned} \text{Alice have final key} &= (\alpha^{x_B} \bmod q)^{x_A} \bmod q \\ &= \alpha^{x_B x_A} \bmod q \end{aligned}$$

$$\begin{aligned} \text{Bob have final key} &= (\alpha^{x_A} \bmod q)^{x_B} \bmod q \\ &= \alpha^{x_A x_B} \bmod q \end{aligned}$$

if both x_A and x_B are equal, then :- $\boxed{x_A = x_B = x}$

$$\begin{array}{ccc} \alpha^{2x} \bmod q & = & \alpha^{2x} \bmod q \\ \text{Alice} & & \text{Bob} \end{array}$$

Hence, Both Alice and Bob

would have same session key as well as $y_A = y_B$

$$\boxed{\alpha^x \bmod q = \alpha^x \bmod q}$$

eg:- Let say $\alpha(g) = (5)$
 $q = (23)$

$$X_A = X_B = X = 6$$

$$Y_A = \alpha^X \text{ mod } q = 5^6 \text{ mod } 23 = (8) = Y_A$$

$$Y_B = \alpha^X \text{ mod } q = 5^6 \text{ mod } 23 = (8) = Y_B$$

$$\text{Alice's session key} = (Y_B)^{X_A} \text{ mod } q = 8^6 \text{ mod } 23 = (13)$$

$$\text{Bob's session key} = (Y_A)^{X_B} \text{ mod } q = 8^6 \text{ mod } 23 = (13)$$

=

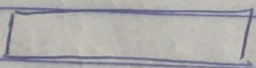
Hence, both Alice and Bob would have same

$$\text{key} = (13)$$

B=X

- (4a) Password guessing works both on the victim computer or other computer (if obtained the password file)
- Default Passwords are used by many Admin and they rarely change that
 - Some even have short length passwords which would take minutes-hours even in brute force attack
 - Most passwords are readable / likely passwords which is easily cracked by dictionary attack.
 - Some even have their phone no, birthdates embed in the password.

~~the~~ Attacker can enter using guest account or by any backdoor and try guessing password. or get the password file to their machine and crack the password there.

(4b)  Biometric Metric space

$$M = \{0, 1\}^V$$

We ~~can~~ use a distance function :-
which finds distance between two metric space :-

$$[M \times M \rightarrow N] \quad \text{Natural number}$$

Fuzzy extractor is a tuple :- (M, l, t)
where t is tolerance of error, and l is
the length of output string bits.

We have two Algo Gen and Rep :-

Gen takes Biometric input and generate
a secret key data.

(2a) Internal Error control :-

→ Sender first uses the PCS then sends the message to network.

→ The decryptor then also uses PCS.

→ The problem is that both sender and receiver must know the order in which they used PCS and encryption, otherwise they can't reproduce message.

→ External Error Control :-

We do PCS outside and publicly to handle the alteration in message.