CENG561 - HW2 / 2930279027, Burak TOPÇU

1) Alice ② → I will work all day → Bob

OR

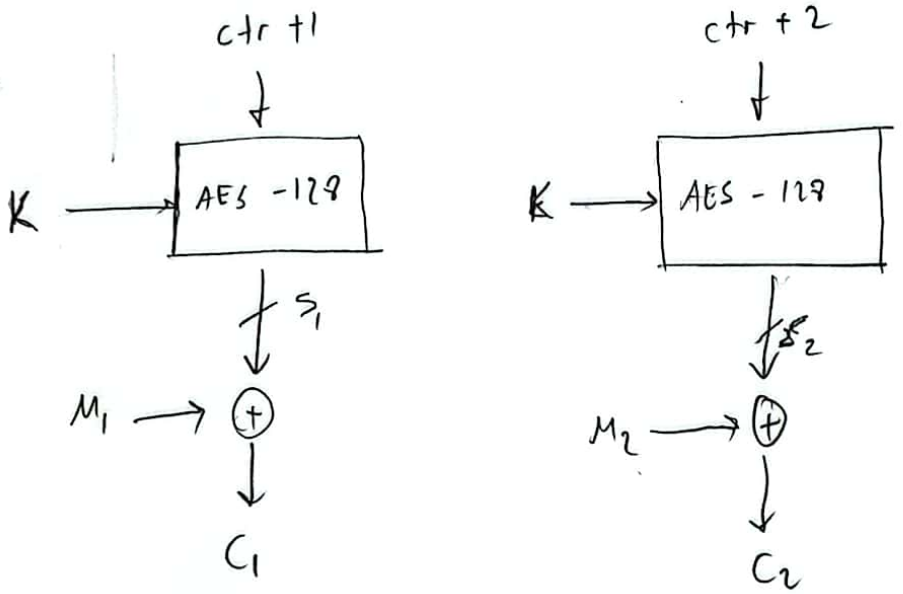
Alice ① → 10B + "We will meet at Maderen's Pub on 5th avenue" → Bob

Alice will send one of ① or ② to Bob in every morning.

① → 10B + 44 char = 10.8 bits + 46.8 bits + padding (3 blocks)
= 447 bits → 128 + 128 + 64 bits

② → 19 char. → = 152 bits → 128 + 24 bits (2 blocks)
↑ padding

Assume that we are using AES-128 with same key for each time.



where;
- $ctr = 0^{127}1$
- $K = \{0,1\}^{128}$
- $M_i = 128$ bit
- $M = M_1 \| M_2 \| \dots \| M_n$
- $S_i \Rightarrow 128$ bits

Note that for the ① message last block should be completed via message padding (fixed block size criterion). Similarly, last message block of the ②nd message needs to be completed to 128 bits.

Resultant $C_i = S_i \oplus M_i$

- Since Alice sends same message on every day; except for M_i of (2)nd message.

1) Attacker realizes that C_i's are identical (key is same)

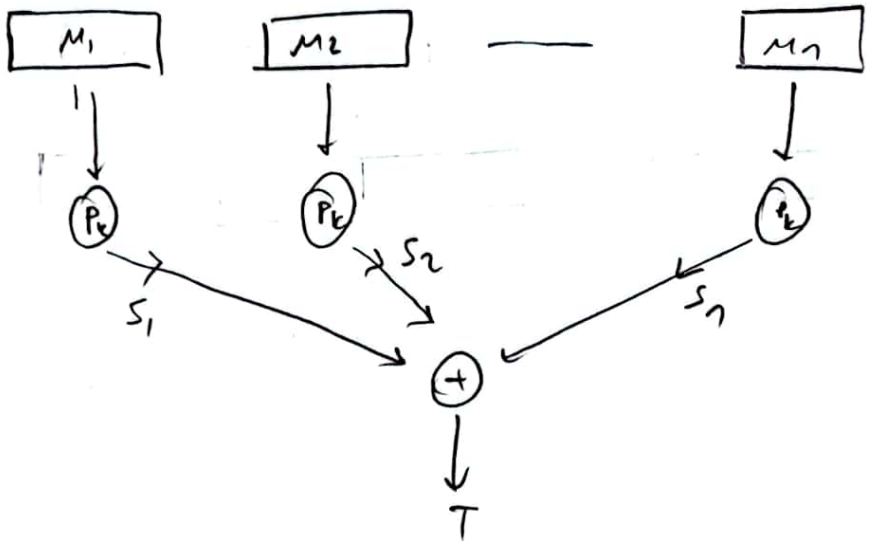
2) If ciphertexts are identical (even if they are created in counter mode, each message will be generated with repeated pattern of counters on each day), this is not IND-CPA secure.

3) Attackers can realize M_i with frequency of words then realize $S_i = M_i \oplus C_i$. After determining the S_i, attackers can exactly learn meeting dates.

→ To protect from those attacks (identical ciphertexts) Nonce-based CTR mode can be used.

With this method, S_i will change each time that results in different C_i for repeated M_i.

2) a)



$M = M_1 \| \dots \| M_n$

let's assume $P_k(M_i) = S_i$

$$S_1 \oplus S_2 \oplus S_3 \oplus S_4 = S_1 \oplus S_3 \oplus S_2 \oplus S_4$$

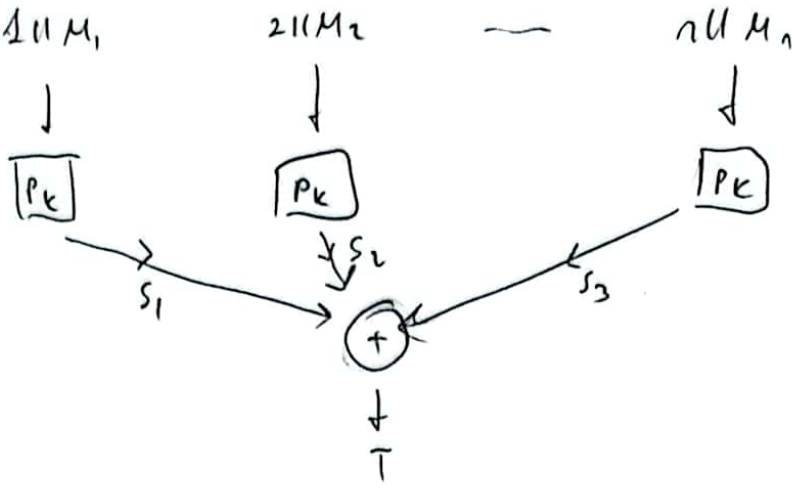
places of two message blocks are exchanged.

→ This is not secure because tag can be same for two different messages such that $M_x = M_1 \| M_2 \| M_3 \| M_4$ and $M_y = M_1 \| M_3 \| M_4 \| M_2$

→ Both M_x and M_y have the same tag which is not secure for authentication.

✓ fixed length for each block

2 b)



$T = S_1 \oplus S_2 \oplus S_3$

If the message $M = M_1 \| M_2 \| \cdots \| M_n$ is sent twice from sender to receiver, it will be sent with same tag used for authentication.

- This breaks UF-CMA secure as explained below:

1) Alice $\xrightarrow{C_1, T_1}$ Bob (where T_1 is obtained with above method.)

2) Alice $\xrightarrow{C_2, T_2}$ Adv $\xrightarrow{C_1, T_1}$ Bob

→ Adversary blocks the transmission of C_2, T_2, converts $C_2 \rightarrow C_1$ by bit flipping. since Adv knows that Tag for C_1 has already been verified.

This scenario breaks down UF-CMA because attacker can be verified by receiver because of the deterministic tag.