09/11/22.

Assignment - 1.

(1.) Show that the Caesar cipher and Vigenère cipher defined over the 128-character ASCII character set are easy to break by doing a chosen-plaintext attack. How much plaintext is needed to recover the key for each of the ciphers?

Ans.)

Caesar Cipher:- → It works by shifting an Alphabet to 3 Places to the right.

Ex:- If; Alice $\xrightarrow{C = E(\text{"APPLE"})}$ Bob

Then the message that Bob will recieve is, "DSS OH".

→ Here the plaintext that is needed to recover the key would be of the same length as the ciphertext.

→ But if we are considering the scenario where the intruder would be able to break the cipher by doing a chosen-plaintext attack over the 128-character ASCII set is, that the ASII character is set to the Alice's message and then accordingly the ASCII character is also set to the Bob's message and it is verge easy for Charlie to identify the key, i.e by shifting 3 Places. and hence can be easily broken.

→ Therefore the Plaintext that is needed to recover the key would be as the same length of the ciphertext, if we consider the 128-character ASCII set, then the Plaintext would be 128 characters, based on the ciphertext.

Vigenère Cipher:-

→ The Encryption of a character $m \in \mathcal{E}$ is, $\boxed{C = (m + K) \bmod 128}$ for some $K \in \mathcal{E}$.

→ Accordingly, knowing the encryption 'C' of an arbitrary $m \in \mathcal{E}$ allows to compute the key $\boxed{K = (C - m) \bmod 128}$ and hence can be easily broken.

→ As we know, that the vigenère cipher consists of 't' independent caesar ciphers, hence it can be broken by obtaining the encryption of a message of length 't' and applying the above attack to each of the characters.

∴ The Plaintext that is needed to recover the key is the same as caesar cipher; i.e., 128 characters, if we are considering 128-character ASCII set, based on the cipher text.

(2) Consider the case where the Caesar cipher and Vigenère cipher are defined over the 26-character English Alphabet. How much plain-text is needed to recover the key for each of the ciphers?

Ans:)

Caesar Cipher:- → It works by shifting an Alphabet to 3 Places to the right.

EX:- If; Alice $\xrightarrow{C = E(\text{"APPLE"})}$ Bob

then the message that Bob will Recieve is,

"DSSOH."

Hence it is easily broken by the intruder because, the shifting is in the range of 26 character's.

→ Therefore, the plaintext that is needed to recover the key would be as the same length as that of cipher text. So, as there are 26 Alphabets, the plaintext would be 26 characters long.

Vigenère Cipher:-

→ we Identify the alphabet $\{A, B, \ldots, Z\}$ with the set $\mathcal{E} = \{0, 1, \ldots, 25\}$.

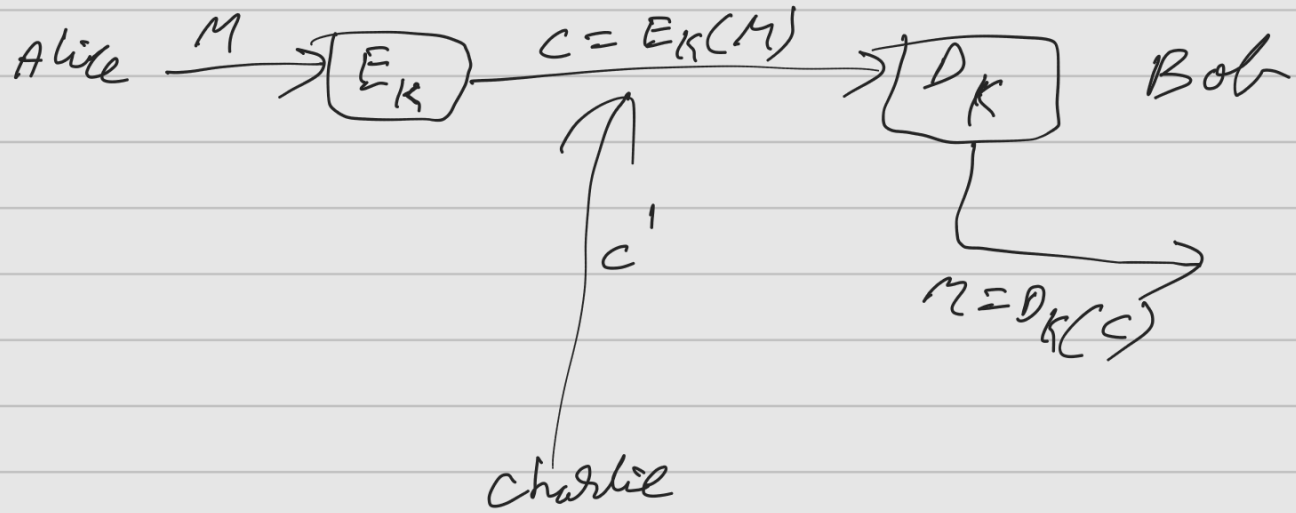
→ The Encryption of a character $m \in \mathcal{E}$ is, $\boxed{C = (m + K) \bmod 26}$. for some $K \in \mathcal{E}$.

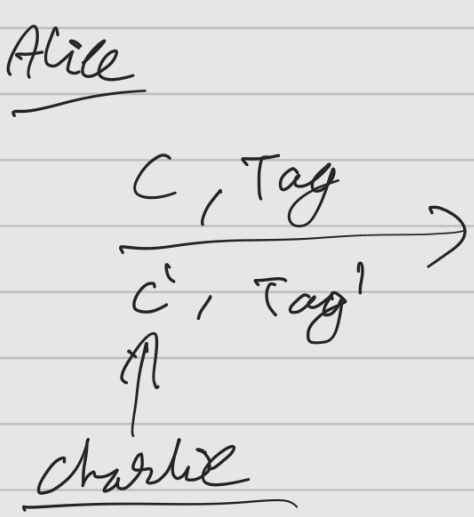
→ Accordingly, Knowing the encryption 'C' of an arbitrary $m \in \mathcal{E}$ allows to compute the key, $\boxed{K = (C - m) \bmod 26.}$ and hence can be easily broken.

→ As we know, that the vigenère cipher consists of 't' independent caesar ciphers, hence it can be broken by obtaining the encryption of a message of length 't' and applying the above attack to each of the characters.

∴ The Plaintext that is needed to recover the key is the same as caesar cipher; i.e., 26 characters as the length of the cipher and plaintext would be same to recover the key.

(3) **MAC:-** → It provides data authenticity and Integrity.





$D_K(C') \rightarrow M'$

$Mac(K, M') = Tag''$

$Tag'' \neq Tag'$.

→ Even if Charlie tries to modify the Tag and also the ciphertext, Bob will still be able to detect when he decrypts with the shared key 'K' and uses the 'M'' to generate the TAG, so when Bob does that and the generated TAG and the TAG he received will be different.

Therefore, the attack will always fail as Bob can identify if the TAG / Ciphertext is modified.

(4) CBC Mode of Encryption:-

(a) Assume that Alice is encrypting all the blocks, and Bob is decrypting them, draw the corresponding diagram for Bob's decryption.

Ans:) Let 'IV' be the initialization vector and 'K' be the key.

The Decryption is as follows;

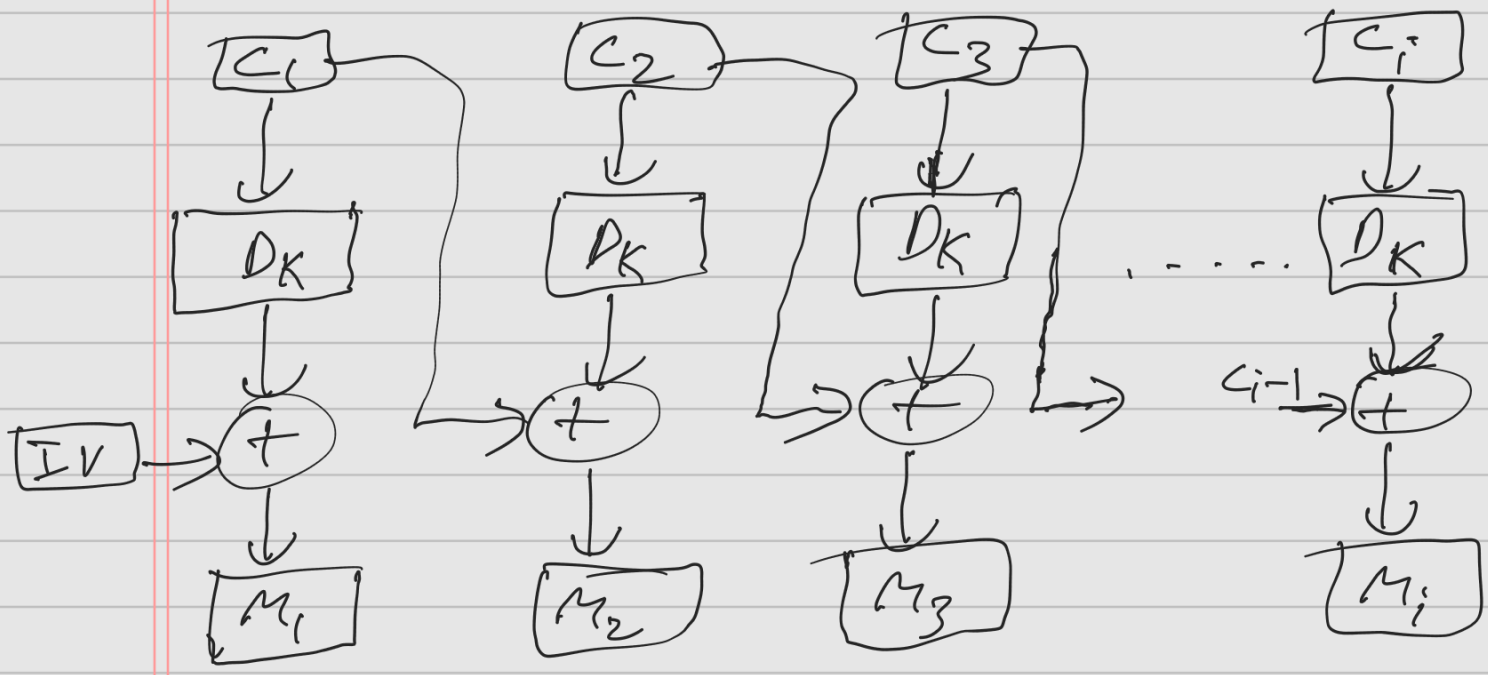
$$M_1 = IV \oplus D[C_1, K]$$

$$M_2 = C_1 \oplus D[C_2, K]$$

$$M_3 = C_2 \oplus D[C_3, K]$$

$$\vdots$$

$$M_i = C_{i-1} \oplus D[C_i, K]$$



(b.) → In the CBC mode, if the adversary tampers with even one block of cipher text then all the corresponding ciphertext blocks will be

Providing the wrong Plain Texts when decrypted using the tampered cipher text, because as shown in the above diagram the ciphertext from the Previous block is used to decrypt the plaintext of the next block.

→ From the given question, if Charlie tampers block C_1 and changes it to C_1', then bob won't be able to decrypt even one of the blocks correctly.

(c.) → In CBC mode, the initialization vector (IV) - randomness is fed into the first block either that is for encryption (or) decryption.

→ But in this case of decryption, if the IV is mangled, then Bob won't be able to decrypt the first block, i.e., C_1 (from the above diagram) correctly, and the remaining blocks will be decrypted correctly as all the remaining blocks except for the first block uses the previous ciphertexts to decrypt and not the IV (as shown in the diagram)

References:-

1.) https://www.researchgate.net/figure/Encryption-and-Decryption-process-using-CBC-mode_fig2_327382004

2.) https://sandilands.info/crypto/ClassicalCiphers.html#x14-540006.4

3.) https://cs.wellesley.edu/~cs110/reading/cryptography.html