How can MAC ensure Data integrity?

Ch-5

MAC

1) What is message Authentication Code?

→ In cryptography, MAC is a short piece of information used for authenticating and integrity-checking a message. It ensures that the message is coming from the correct sender, has not been changed, the data transferred over a network is legitimate and doesn't contain harmful code.

Ex: ① Message creation:

— Alice's message: "Hello, Bob!"

② MAC Generation:

- Alice uses a secret key (shared with Bob) and a MAC algorithm to generate a MAC for the message.

- suppose secret key is "secret 123"

— " algo is "HMAC-SHA256".

- The MAC is "5d4140 . . ."

③ Message transmission:

Alice sends message + MAC

"Hello, Bob!" + "5d4140 . . . "

4) MAC Venification:

- Bob neciere msg + MAC
- genenate MAC using same seenet key and MAC algo
- if (neceived MAC == Bob's genenated MAC)
  - msg is fnom Alice
  - msg is not changed
- else
  - not fnom Alice / altened / modified

* What's Dictionany Attack?

→ a method used by attackens to guess passwonds with a dictionany list of common wonds / phnases used by businesses and individuals.

→ a type of bnute fonce attack

→ tnying out eveny possible wond in dictionany

* **What is social engineering attack?**

→ tactic of manipulating, influencing or deceiving a victim in order to gain control over a computer system or to steal personal or financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

* **What is pretexting attack?**

→ use of a fabricated story to gain a victim's trust and trick or manipulate them into sharing sensitive information, downloading malware, sending money to criminals or otherwise harming themselves or the organization they work for.

* **How Digital Certificate works?**

→ Digital certificates verify identities and enable secure, encrypted communication.

Steps: (i) A tnusted Centificate Authonity (CA) issues a digital centificate aften venifying the entity's identity.

(ii) the entity installs the centificate on its senven.

(iii) the senven pnesents the centificate to usen.

(iv) the usen's bnowsen venifies the contificate.

(v) If valid, a secuned, encnypted connection is established.

* what is the nole of CA (centificate Authonity)

→ CA is a tnusted anganization that issues digital centificates.

Role: 1) venifies identity of entities

2) cneates and signs digital centificate,

3) Enable secune communication between usens and bnowsens.

something fon something   Latin wond

* Quid Pno Quo Attack:

→ is a type of social engineening attack in which the attacken pnomises the victim a favon in exchange fon infonmation on othen benefits.

Ch-8

* GCD (2260, 812) using Eclidean Algo:

→ ① $a = 2260$, $b = 812$

$\therefore$ $a \div b = 2$, nem $= 636$

② $a = 812$, $b = 636$

~~812 %~~ $a \div b = 1$, nem $= 176$

③ $a = 636$, $b = 176$

$a \div b = 3$, nem $= 108$

④ $a = 176$, $b = 108$

$a \div b = 1$, nem $= 68$

⑤ $a = 108$, $b = 68$

$a \div b = 1$, nem $= 40$

* AES — Advanced Encryption Standard

(6) $a = 68$, $b = 40$, division $= 1$, rem $= 28$

(7) $a = 40$, $b = 28$, div $= 1$, rem $= 12$

(8) $a = 28$, $b = 12$, div $= 2$, rem $= 4$

(9) $a = 12$, $\boxed{b = 4}$, $\boxed{\text{div} = 3}$, $\boxed{\text{rem} = 0}$

∴ rem, $= 0$, so the GCD is b ~~[illegible]~~ $= 4$

* GCD (226, 12)

→ (i) $a = 226$, $b = 12$, div $= 18$, rem $= 10$

(ii) $a = 12$, $b = 10$, div $= 1$, rem $= 2$

(iii) $a = 10$, $\boxed{b = 2}$, div $= 5$, $\boxed{\text{rem} = 0}$

ans

* $\boxed{5^{31} \bmod 13}$ using repeated squaring:

→ $31 = 16 + 8 + 4 + 2 + 1$

$5^{31} = 5^{16+8+4+2+1}$

$= 5^{16} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \cdot 5^{1}$

$= (8 \times 12 \times 8 \times 12 \times 5) \bmod 13$

$= 7680 \bmod 13 = 8$

$5^{1} \bmod 13 = 5$

$5^{2} \bmod 13 = 12$

$5^{4} \bmod 13 =$

$(12 \times 12) \bmod 13$

$= 144 \% 13 = 8$

$5^{8} \bmod 13$

$= (8 \times 8) \% 13$

$= 12$

$5^{16} \bmod 13$

$= (12 \times 12) \bmod 13 = 8$

* Dexten wants to set up his own public and pnivate keys. He chooses $p = 23$, $q = 19$ with $e = 283$. Find d so that ed has a nemaindon of 1 when divided by $\boxed{(p-1)(q-1)}$

$\rightarrow \quad m = (p-1)(q-1) \quad = 22 \times 18 = 396$

$ed = 283\,d$, nem $= 1$, when divided by

$m = 396$

d	ed	nem (div by 396)
1	283	283
2	566	170
3	849	57
4	1132	340
5	1415	227
6	1698	114
7	1981	1

$\therefore$ for $\boxed{d = 7}$, $ed = 283 \times 7 = 1981$

has a nem of 1 when div by 396

* What's cryptanalysis ?

→ study and process of analyzing and decrypting ciphers, codes and encrypted text without using the real key.

→ analyze cryptographic system

→ understand/ identify weakness and vulnerabilities

*① Divide the plaintext into blocks of size $m = 3$.

Block 1 : BBC   Block 2 : ABC

Block 3 : BCA   Block 4 : A

(ii) After padding, Block 4 : AZZ

(iii) multiply each block by encryption key matrix :

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$$

B1 :

$$\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 9 \\ 25 \\ 41 \end{bmatrix} \rightarrow \begin{matrix} J \\ Y \\ P \end{matrix}$$

→ 41 mod 26 = 15

B2 : $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 8 \\ 20 \\ 32 \end{bmatrix} \rightarrow \begin{matrix} I \\ U \\ G \end{matrix}$

B 3 : $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \times \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 17 \\ 29 \end{bmatrix} \rightarrow \begin{matrix} F \\ R \\ D \end{matrix}$

B 4 : $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \times \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 15 \\ 39 \\ 63 \end{bmatrix} \rightarrow \begin{matrix} P \\ N \\ L \end{matrix}$

∴ Encrypted text: JYP IUG FRD PNL