U-6

Ciphen Block chaining

Q. How to detect whethen CBC can hide pattenns on not ? Descnibe the pnocess.

→ ① Encnypt a plaintext with nepeating pattenns using CBC mode with a symmetnic key and a nandom initialization vecton.

② Bneak the neseulting ciphentext into blocks.

③ Compane the ciphentext blocks fon any nepetitions.

If all ciphentext blocks ane unique, CBC mode successfully hides the pattenns. If any blocks ane identical, CBC mode fails to hide the pattenns effectively.

Q. Between CFB and OFB, which has a betten encnyption anchitectune ? why ?

→ CFB → ciphen Feedback	OFB → output Feedback
1) ciphentext feedback.	1) Key stneam genenated from initialization vecton.
2) Ennon pnopagates fon only one block. → If ennon in 1 block, it'll affect next block.	2) No ennon pnopagation. → If ennon in 1 block, it'll affect only that specific block.

So OFB better

CFB	OFB
3) Slighty slower performance → due to feedback loop	3) Faster as the key stream can be pre-computed.
4) Encryption can't be parallelized. Decryption can be	4) Both encryption and decryption can be parallelized.

Q) Hill cipher use and find cipher text

string = dog

$$\vec{x} = \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix}$$

Given, random matrix

$$K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$$

$$\vec{c} = K \cdot \vec{x} = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix}$$

$$= \begin{bmatrix} 3+28+30 \\ 9+42+24 \\ 6+14+18 \end{bmatrix} = \begin{bmatrix} 61 \\ 75 \\ 38 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 9 \\ 23 \\ 12 \end{bmatrix}$$

$\therefore$ cipher text = Jxm

Electronic codebook

Q) Why is ECB bad with images?

→ bad for encrypting images because it handles each block of data separately. This means that identical parts of the image will look the same even after encryption, making patterns in the original image visible in the encrypted version. As a result, repetitive structures and textures can still be seen, compromising security. (CBC is better) hides pattern

Q) Suppose the number of keys for substitution cipher is 26!. If we partition the plaintext into bigram, what'll be the no. of keys in the keyspace?

→ Total possible bigrams = 26 × 26 = 676
pair (AA, AB ... ZZ etc)

∴ Total keys = $(26!)^{676}$

In case of trigram $= (26!)^{26 \times 26 \times 26}$

Q) Disadvantages of substitution cipher:

1) It doesn't hide how often letters appear, so someone could guess which letters stand for which.

2) There are only a limited number of keys. making it easier to try them all and decode the message.

3) Doesn't hide pattern.

4) Not secured.

5) It's hard to keep the keys secret and make sure only the right people can decode the message.

Q) What's One-time pad?

→ one type of substitution cipher that is absolutely unbreakable.

→ uses a random key as long as the message for encryption, ensuring perfect secrecy through XOR operation,

Q) What is block cipher?

→ a cryptographic algorithm that encrypts fixed-size blocks of plaintext into ciphertext.

Briefly explain ECB and CFB modes of block ciphers.

→

ECB	CFB
1) encrypts each block of plaintext independently with the same key.	1) encrypts a plaintext block by XORing it with the output of the encryption of the previous cipher-text block (or initialization vector for the 1st block)
(2) Simple and straightforward. Faster.	(2) Slower than ECB
(3) Errors in 1 block does not affect others.	(3) Affects subsequent blocks until synchronization is restored.
(4) Parallelizable	(4) Not parallelizable.
(5) Reveals pattern	(5) hides pattern

text = TOM, find cipher using hill cipher.

$$k = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}, \quad x = \begin{bmatrix} 19 \\ 14 \\ 12 \end{bmatrix}$$

$$\therefore c = \begin{pmatrix} 19+28+60 \\ 57+42+48 \\ 38+14+36 \end{pmatrix} = \begin{bmatrix} 107 \\ 147 \\ 88 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 \\ 17 \\ 10 \end{bmatrix}$$

∴ cipher text = d r k

* Encrypt the text "CAB BCC ACC B" using block cipher with padding, $m = 3$

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

for the 1st block, $\vec{x} = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$

for " last ", $\vec{x}' = \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}$

→ After padding $B_1 = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$

$$B_2 = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}, \quad B_4 = \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}$$

$$K \cdot B_1 = \begin{bmatrix} 2+3 \\ 10+7 \\ 18+11 \end{bmatrix} = \begin{bmatrix} 5 \\ 17 \\ 29 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 17 \\ 3 \end{bmatrix} = \text{frd}$$

$$K \cdot B_2 = \begin{bmatrix} 1+4+6 \\ 5+12+14 \\ 9+20+22 \end{bmatrix} = \begin{bmatrix} 11 \\ 31 \\ 51 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 5 \\ 25 \end{bmatrix} = \text{LFZ}$$

$$K \cdot B_3 = \begin{bmatrix} 4+6 \\ 12+14 \\ 20+22 \end{bmatrix} = \begin{bmatrix} 10 \\ 26 \\ 42 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10 \\ 0 \\ 16 \end{bmatrix} = \text{kaq}$$

$$K \cdot B_4 = \begin{bmatrix} 1+6+9 \\ 5+18+21 \\ 9+30+33 \end{bmatrix} = \begin{bmatrix} 16 \\ 44 \\ 72 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16 \\ 18 \\ 20 \end{bmatrix} = \text{qsu}$$

Problem and solution of block cipher with padding mechanism:

→ can accidentally leak information about the length of the message or even parts of the message itself. To fix this, use standardized padding methods, like PKCS# 7, and double-check for mistakes during decryption.

→ encrypt it separately to protect length.

→ Always choose padding that adds the least amount of data possible.

ECB problem: leaks pattens, reveal info about plaintext, not suitable for sensitive info.

→ Identical plaintext blocks are encrypted into identical ciphertext blocks.

CFB problem: ① more complex, slower.

② Initialization vector is needed.

③ If error occurs in a block of ciphertext, it affects the subsequent blocks's decryption untill synchronization is restored, data corruption occurs

④ not suitable for large-scale data

Q. Why is padding used in encryption?

→ to ensure that plaintext message fills up the entire block size required by the encryption algorithm.

→ make efficient

→ prevent leakage of info

Q. 4 modes of block-cipher:

1. ECB (Electronic Codebook)
2. CBC (cipher-block chaining)
3. CFB (cipher feedback)
4. OFB (output feedback)

Q. Vigenère cipher uses a key that is as long as plain text, T or F?

→ False. It uses a key that is repeated to match the length of plaintext.

Q. AA's security test

1) verify encryption method used for pic
2) Test decryption
3) Test pin's strength
4) check access control

Q) **Encryption** | **Hashing**

Encryption	Hashing
① converts plaintext into ciphertext using a key.	① generates a fixed size hash value from input data.
② Allows decryption with the same key to retrieve the original plaintext.	② Hash values can't be reversed to obtain the original input.
③ Ensures only authorized parties can access and understand the data.	③ used for data validation, digital signatures and securely storing passwords.

Q) In CBC mode we can take advantage of pre computed IV. T or F?

→ False. CBC needs an IV that's random and unique for each encryption operation. It's not pre-computed or reused.

questions

Q. What are problems of security questions in password reset systems? Example.

easily guessable ← ① often predictable ② Limited security.

vulnerable system → ③ often unchanged answers

Ex: 2008, Sarah Palin's Yahoo account hacked.

The attacker used publicly available info to answer security questions

→ reset password

→ gain unauthorized access to private mails

~~ao~~ text = CBB BAC ABC B

After padding, $B_1 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$, $B_2 = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}$

$B_3 = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$ $B_4 = \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}$

$$K \cdot B_1 = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2+2+3 \\ 10+6+7 \\ 18+10+11 \end{bmatrix} = \begin{pmatrix} 7 \\ 23 \\ 39 \end{pmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 \\ 23 \\ 13 \end{bmatrix} = hxn$$

$$K \cdot B_2 = \begin{bmatrix} 1+6 \\ 5+14 \\ 9+22 \end{bmatrix} = \begin{bmatrix} 7 \\ 19 \\ 31 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 19 \\ 5 \end{bmatrix} = htf$$

$$K \cdot B_3 = \begin{bmatrix} 2+6 \\ 6+14 \\ 10+22 \end{bmatrix} = \begin{bmatrix} 8 \\ 20 \\ 32 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 20 \\ 12 \end{bmatrix} = ium$$

$$K \cdot B_4 = \begin{bmatrix} 1+6+9 \\ 5+18+21 \\ 9+30+33 \end{bmatrix} = \begin{bmatrix} 16 \\ 44 \\ 72 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16 \\ 18 \\ 20 \end{bmatrix} = qsu$$

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: (1) A trusted Certificate Authority (CA) issues a digital certificate after verifying the entity's identity.

(ii) the entity installs the certificate on its server.

(iii) the server presents the certificate to user

(iv) the user's browser verifies the certificate.

(v) If valid, a secured, encrypted connection is established.

* What is the role of CA (certificate Authority)

→ CA is a trusted organization that issues digital certificates.

Role: 1) verifies identity of entities

(2) creates and signs digital certificate,

(3) Enable secure communication between users and browsers.

something for something — Latin word

* Quid Pro Quo Attack:

→ is a type of social engineering attack in which the attacker promises the victim a favor in exchange for information or other benefits.

Ch-8

* GCD (2260, 812) using Euclidean Algo:

→ ① a = 2260, b = 812

∴ a ÷ b = 2, rem = 636

② a = 812, b = 636

~~812 % 0~~ a ÷ b = 1, rem = 176

③ a = 636, b = 176

a ÷ b = 3, rem = 108

④ a = 176, b = 108

a ÷ b = 1, rem = 68

⑤ a = 108, b = 68

a ÷ b = 1, rem = 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, b = 4, $\boxed{\text{div} = 3}$, $\boxed{\text{rem} = 0}$

∴ rem = 0, so the GCD is b = 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:

→ $31 = 16 + 8 + 4 + 2 + 1$

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

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

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

$= 7680 \bmod 13 = 8$

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

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

$5^{4} \bmod 13 =$

$(12 \times 12) \bmod 13$

$= 144 \% 13 = 8$

$5^{8} \bmod 13$

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

$= 12$

$5^{16} \bmod 13$

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

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

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

$ed = 283\,d$, rem $= 1$, when divided by $m = 396$

d	ed	rem (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 rem of 1 when div by 396

* What's $\boxed{\text{cryptanalysis}}$?

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

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

→ 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