B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE), Section- 36 & 38

Dr. Laxmidhar Biswal

April 14, 2025

Compare and contrast various types of security controls

1 Chapter 04

  - Introduction
- Substitution Techniques
  - Caesar Cipher
  - Playfair Cipher
  - Hill Cipher
  - Vigenère Cipher
- Block Cipher
  - DES
  - AES
  - Deffie-Hellman Key Exchange
- Asymmetric Cryptography
  - RSA
  - Tools
  - Obfuscation
  - Hashing
  - Salting
  - Digital Signatures
  - Key Stretching
  - Blockchain

Introduction/Motivation

Computer network security relies heavily on cryptography to protect data transmitted over networks from unauthorized access and tampering. It ensures that sensitive information, such as passwords, personal data, and financial transactions, remains secure during transmission. Protocols like SSL/TLS utilize cryptographic techniques to establish encrypted connections over the internet, thereby safeguarding websites and online communications. Additionally, technologies such as Virtual Private Networks (VPNs) and firewalls employ cryptographic tools to enable secure remote access and defend internal networks against external threats. Collectively, cryptography and network security measures form the foundation of modern secure communication systems.

Explain the importance of using appropriate cryptographic solutions

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a system that uses public and private keys to secure digital communication. It ensures encryption, authentication, and data integrity through digital certificates issued by trusted Certificate Authorities (CAs). PKI is widely used in HTTPS websites, digital signatures, and secure emails to build trust and protect sensitive information online.

- public keys
- private keys
- certificates
- key escrow mechanisms

Explain the importance of using appropriate cryptographic solutions

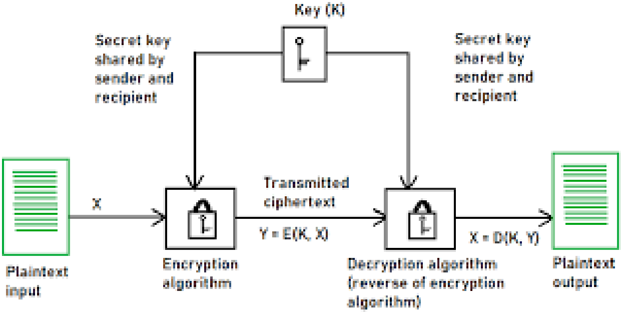

Key (K)
Secret key shared by sender and recipient
Secret key shared by sender and recipient
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure: Simplified model of symmetric encryption

Explain the importance of using appropriate cryptographic solutions

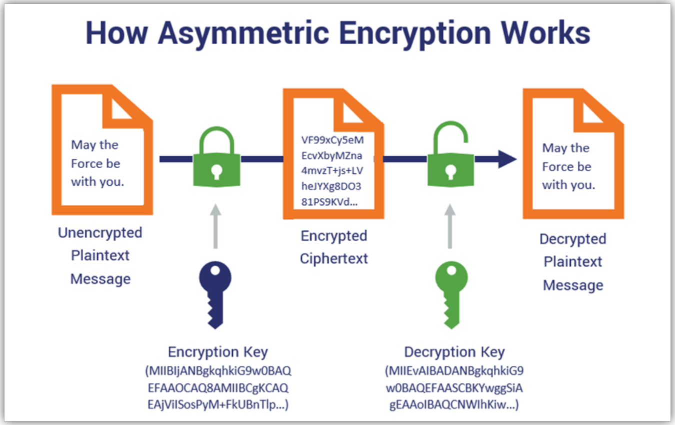

How Asymmetric Encryption Works
May the Force be with you.
Unencrypted Plaintext Message
VF99xCy5eM EcvXbyMZna 4mvzT+js+LV heJYXg8DO3 81PS9KVd...
Encrypted Ciphertext
May the Force be with you.
Decrypted Plaintext Message
Encryption Key
(MIIBIjANBgkqhkiG9w0BAQ EFAAOCAQ8AMIIBCgKCAQ EAjVilSosPyM+FkUBnTlp...)
Decryption Key
(MIIEvAIBADANBgkqhkiG9 w0BAQEFAASCBKYwggSiA gEAAoIBAQCNWIhKiw...)

Figure: Simplified model of asymmetric encryption

Explain the importance of using appropriate cryptographic solutions

Encryption

Encryption is a technique that transforms readable data (plaintext) into an unreadable format (ciphertext) using a specific algorithm and key. This process ensures that the data remains secure and can only be decoded by those with the correct key, protecting it from unauthorized access.

Encryptions can be classified as follows:

- Symmetric encryption: Same key for encryption and decryption.
- Asymmetric encryption: Different keys for encryption and decryption.

Explain the importance of using appropriate cryptographic solutions

Keywords related to Cryptography

- **plaintext**: Plaintext is usually plain readable text is used as an input for the encryption process or as the output for the decryption process.
- **ciphertext** : Ciphertext is encrypted text transformed from plaintext using an encryption algorithm, unreadable that can only be read if you know the key.
- **enciphering**/encryption:
  - "Encipher" and "encrypt" have the same meaning. "Encipher" is the older term, while "encrypt" is the modern term.
  - Enciphering is a form of encryption focused on transforming text, while Encryption includes more complex and secure techniques to protect digital data.

Explain the importance of using appropriate cryptographic solutions

Keywords related to Cryptography

- **deciphering** / decryption:
  - Deciphering/Decryption is the reverse process of enciphering/encryption, converting ciphertext back into plaintext.
  - Deciphering is associated with classical ciphers (e.g., Caesar cipher or Vigenère cipher), which typically involve character-level transformations.
  - And whereas decryption is used in modern cryptography with algorithms like AES, RSA, and ECC to ensure the secure and accurate retrieval of the original data.
- cryptography: Cryptography uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties.
- cryptoanalysis: Cryptanalysis involves analyzing the characteristics of encrypted messages to identify potential

Explain the importance of using appropriate cryptographic solutions

Keywords related to Cryptography

- cryptology: Cryptology is the science that focuses on ensuring secure and often secret communication and data storage. It includes both cryptography, which involves creating secure systems, and cryptanalysis, which is the study of breaking those systems.

The five key ingredients of the symmetric encryption model are

- plaintext
- Encryption Algorithm
- Secret Key
- Ciphertex: random, unreadable sequence
- Decryption Algorithm

Explain the importance of using appropriate cryptographic solutions

Types of Classical Enciphering

1. **Substitution ciphers**: A substitution cipher is an encryption technique where units of plaintext are substituted with ciphertext using a predefined method and a key. In this approach, characters in the plaintext are transformed into different characters, numbers, or symbols based on the given key.
2. **Transposition ciphers**: A transposition cipher is a cryptographic technique that rearranges the order of characters in plaintext to generate ciphertext. Also referred to as a permutation cipher, this method of encryption alters the positions of the characters, ensuring that the original message is disguised.

Explain the importance of using appropriate cryptographic solutions

Substitution Techniques

- Caesar Cipher
- Playfair Cipher
- Hill Cipher
- Poly alphabetic/Vigenère Cipher
- Vernam cipher

Explain the importance of using appropriate cryptographic solutions

Caesar Cipher

It is an ancient cryptographic technique that shifts each character in a plaintext message by a predetermined number of positions, as determined by a key value. Julius Caesar used this method in private communications around 58 BC.

- Write A to Z in chronology order, assign number using Mod 26, *i.e.*, A, ...Z, will be assigned as 0,.......25.
- Write the plaintext and assign Mod 26 values to each alphabet of the plaintext(P(x)).
- Note the value of Key(k), x; where x is the position of each alphabet in plain text.
- Find Encrypted text/message(E(x))=(x+k)mod26,*i.e.*, *k* position right-shifting
- For Decryption: P(x) = (x-k)mod26

Explain the importance of using appropriate cryptographic solutions

Example-1

Plaintext: HELLO, Key(k)=3,find E(x)/Encrypted text?

Alphabets from plain text	Mod26 value of Alphabet(x)	Key=k	(x+k)mod26	E(x)
H	7	3	(7+3=10)mod26=10	K
E	4	3	(4+3=7)mod26=7	H
L	11	3	(11+3=14)mod26=14	O
L	11	3	(11+3=14)mod26=14	O
O	14	3	(14+3=17)mod26=17	R

So the ciphertext of plaintext : HELLO will be given by ”KHOOR”

Advantage & Disadvantage:

The Caesar Cipher is easy to implement, making it simple and widely understood. However, it has a very small key space (only 26 possible keys), which makes it vulnerable to brute-force attacks. An attacker can easily try all keys to break the cipher.

Explain the importance of using appropriate cryptographic solutions

Playfair Cipher

1. The Playfair Cipher uses a 5×5 matrix (key table) of letters for encryption.
2. Letters I and J are considered the same to fit 25 letters in the matrix.
3. The matrix is filled by:
   - First placing the unique letters of a keyword (in order).
   - Then filling in the remaining unused letters of the alphabet.
4. The plaintext is encrypted two letters at a time (digraphs).
5. Duplicate letters in a pair (e.g., ”LL”) are separated by inserting an ‘X’ (e.g., ”LX”). For case ’XX’, Q will be inserted instead of X.
6. It’s a classical symmetric encryption technique, offering better security than simple substitution ciphers.

Explain the importance of using appropriate cryptographic solutions

Encryption rule of Playfair Cipher

1. If both letters are in the same row, replace each with the letter to its right (wrap around if needed). *i.e.*, $M(r,c) \rightarrow C(r,(c+1) mod 5)$, where r and c present row and column numbers of key-matrix corresponding to the plaintext alphabet.
2. If both are in the same column, replace each with the letter below it (wrap around if needed).
3. If in different rows and columns, replace each with the letter in the same row but opposite corner (rectangle rule).

1. Playfair cipher also known as Playfair square or the Wheatstone-Playfair cipher.
2. Charles Wheatstone created the technique in 1854, but it is named after Lord Playfair to promote the use of it.

Explain the importance of using appropriate cryptographic solutions

Question and Answer

Key = **GOOD STUDENTS**;
Plaintext = **THE SCHEME REALLY WORKS**
Write encrypted and decrypted messages.

- Check if the key contains any repeated letters, spaces, or special characters. If so, remove them and rewrite the key.
- key= GODSTUEN
- Now append the remaining letters of the alphabet not already in the key, skipping J.
- Fill the 5x5 matrix as follows:

G	O	D	S	T
U	E	N	A	B
C	F	H	I/J	K
L	M	P	Q	R
V	W	X	Y	Z

Explain the importance of using appropriate cryptographic solutions

Cont...

- Check the plaintext and rewrite the plaintext as per the rule stated above.
- plaintext = THESCHEMEREALLYWORKS
- Add 'X' in between two 'LL'. Add extra 'X' for making pair.
  plaintext=THESCHEMEREAL'X'LYWORKS'X'

Plaintext digraphs:

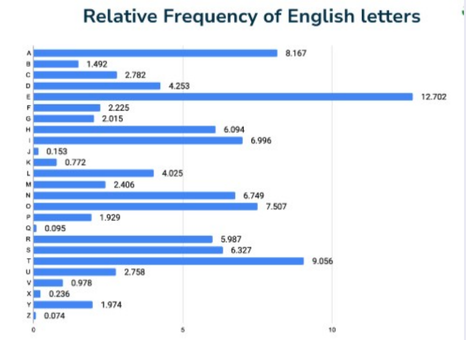
TH	ES	CH	EM	ER	EA	LX	LY	WO	RK	SX

Ciphertext: Using Encryption Rule

DK	AO	FI	FW	BM	NB	PV	QV	OE	ZR	DY

Explain the importance of using appropriate cryptographic solutions

Monoalphabetic Cipher



Explain the importance of using appropriate cryptographic solutions

Hill Cipher

- Unlike monoalphabetic ciphers, the Hill cipher is a polygraphic substitution cipher based on linear algebra.
- It was developed by Lester S. Hill in 1929.
- It is a block cipher of two or three letter, or any size.
- The value of n, the block size, depends on the key matrix, not on the plaintext.
- The key must be a square matrix of size $(n \times n)$. Therefore, the plaintext is divided into blocks of (n) letters.
- For example, if the key is a 3×3 matrix, then n=3, and 3 plaintext is encrypted in groups of letters.
- In case the key size is not a square, the key would be padded or trimmed to make the length a perfect. square.

Explain the importance of using appropriate cryptographic solutions

Hill Cipher

- Fill $n \times n$ key matrix by row-wise.
- Rewrite the $n \times n$ matrix by replacing each alphabet with its *modulo* 26 value.
- Consider each n alphabet of plaintext, and form a $n \times 1$ matrix with its equivalent *modulo* 26 values.
- Find Encryption: C = KP mod 26.
- Find Decryption: P =$K^{-1}C$

Question and answer

Given: Key = HILL; Plaintext = `HELP`. Find cipher text.

Ans.: Converting letters to numbers (A=0, B=1, ..., Z=25):

$$\mathtt{H} = 7, \quad \mathtt{I} = 8, \quad \mathtt{L} = 11$$

Explain the importance of using appropriate cryptographic solutions

Cont..

So the key matrix K is: $\mathrm{K} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

- Take plaintext: HELP
  $\mathtt{H} = 7, \quad \mathtt{E} = 4, \quad \mathtt{L} = 11, \quad \mathtt{P} = 15$
- Group into group of n: HELP → HE, LP.
- **Encrypting HE**: $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 7 \cdot 7 + 8 \cdot 4 \\ 11 \cdot 7 + 11 \cdot 4 \end{bmatrix}$
  $= \begin{bmatrix} 81 \\ 121 \end{bmatrix} \mod 26 = \begin{bmatrix} 3 \\ 17 \end{bmatrix} \Rightarrow \mathtt{D} \;\; \mathtt{R}$

- **Encrypting LP**: $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 7 \cdot 11 + 8 \cdot 15 \\ 11 \cdot 11 + 11 \cdot 15 \end{bmatrix}$

$= \begin{bmatrix} 197 \\ 286 \end{bmatrix} \mod 26 = \begin{bmatrix} 15 \\ 0 \end{bmatrix} \Rightarrow \mathtt{P} \;\; \mathtt{A}$

Explain the importance of using appropriate cryptographic solutions

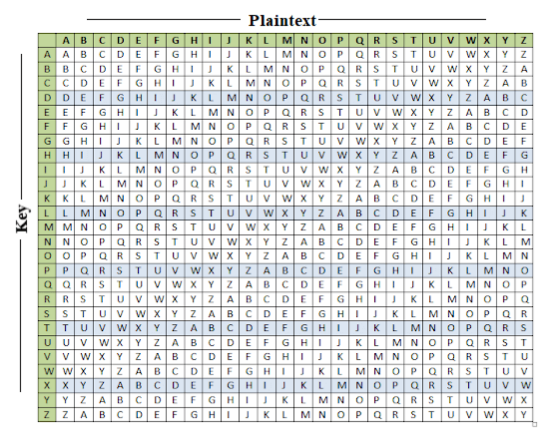
Vigenère Cipher

The Vigenère Cipher and the Caesar Cipher are similar in that both shift letters of the plaintext. However, while the Caesar Cipher shifts all letters by a fixed number, the Vigenère Cipher shifts each letter by a different amount based on a keyword.

- Choose a keyword
- Repeat the keyword to match plaintext length
- Convert letters to numbers
- Apply shift (encrypt or decrypt)
- Convert numbers back to letters

Explain the importance of using appropriate cryptographic solutions

Vigenère Cipher



Plaintext

Key

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Explain the importance of using appropriate cryptographic solutions

Question

Plaintext: ATTACK; Key: KEY. Write an encrypted message.

Ans.: Plaintext: ATTACK

Keyword : KEYKEY (repeat to match the plaintext length)

Letter Type	A	T	T	A	C	K
Plaintext (0–25)	0	19	19	0	2	10
Key (K, E, Y, K, E, Y)	10	4	24	10	4	24
Sum mod 26	(0+10)=10	(19+4)=23	(19+24)=43 mod 26=17	(0+10)=10	(2+4)=6	(10+24)=34 mod 26=8
Ciphertext	K	X	R	K	G	I

Final Ciphertext: `KXRKGI`

Explain the importance of using appropriate cryptographic solutions

Transposition ciphers

- Railfence ciphers
- Columnar Transposition Cipher

Railfence ciphers

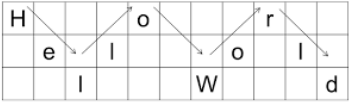
The Rail Fence Cipher is a transposition cipher — it rearranges the characters of the plaintext into a zigzag pattern across multiple "rails" (rows), and then reads the result row-by-row to produce the ciphertext.

- Choose the number of rails (key), say k.
- Write the message in a zigzag pattern across the rails.
- Read row-by-row to get the ciphertext.
- Spaces ( ), commas (,), periods (.), etc., are placed in the zigzag pattern in order, just like letters.

Explain the importance of using appropriate cryptographic solutions

Example:

Original Message: Hello World



H				o				r		
	e		l				o		l	
		l				W				d

Encrypted Message: Horel ollWd

Columnar Transposition Cipher

A transposition cipher that rearranges the plaintext into a grid (matrix) and then reads the characters column-by-column using a permutation key.

- Write the plaintext row-wise into a grid with columns defined by the key length.

Explain the importance of using appropriate cryptographic solutions

Cont...

- If needed, pad the message with dummy characters (e.g., 'x') to fill the grid.
- Rearrange the columns according to the key (a permutation of column indices).
- Read column-by-column to get the ciphertext.

Example

The Plaintext: "Section 36, 38 of ITER",
Key (Permutation): (2,3,1)

Explain the importance of using appropriate cryptographic solutions

Cont..

- Input: "Section 36, 38 of ITER"
  Length = 22 character
- Coloumn size=3
  Smallest multiple of 3 $\geq 23 \rightarrow 24$ characters.
- We'll pad with dummy letters (X) to make the message fit a grid with 3 columns.
  So we add 2 padding character: "X"
  Final plaintext: "Section 36, 38 of ITERXX"
  Length $= 24 \rightarrow 8$ rows $\times$ 3 columns

Explain the importance of using appropriate cryptographic solutions

Cont..

Row	Col 1	Col 2	Col 3
1	S	E	C
2	T	I	O
3	N	(space)	3
4	6	,	(space)
5	(space)	3	8
6	(space)	O	F
7	(space)	I	T
8	E	R	X

Reordered Table (Columns 2, 3, 1)

Row	New Col 1 (old Col 2)	New Col 2 (old Col 3)	New Col 3 (old Col 1)
1	E	C	S
2	I	O	T
3	(space)	3	N
4	,	(space)	6
5	3	8	(space)
6	O	F	(space)
7	I	T	(space)
8	R	X	E

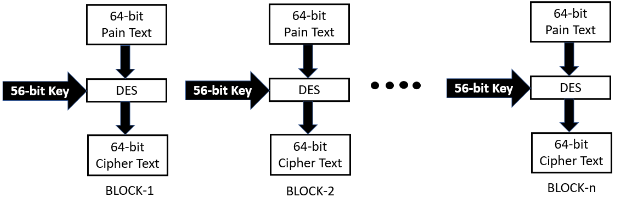
Explain the importance of using appropriate cryptographic solutions

Data Encryption Standard

- DES is a symmetric-key block cipher, and Devolped by IBM Team in the year 1970.
- DES is a block cipher with a 56-bit key length.
- DES encrypts data in blocks of size of 64 bits each, i.e., takes 64 bits of plain text and provides 64 bits of cipher text.
- DES consists of 16 round Feistel structures, each of which is called a round.

Explain the importance of using appropriate cryptographic solutions

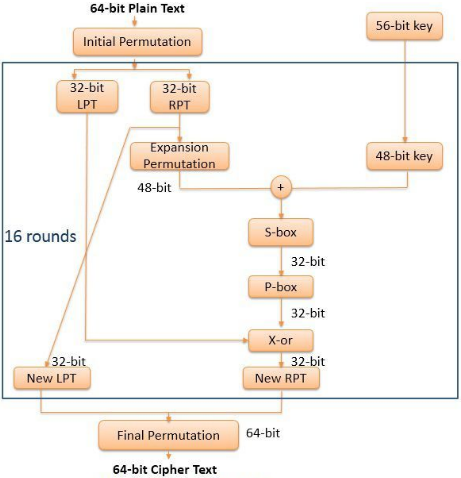
Data Encryption Standard



- Convert all plain text to binary data with the help of ASCII code.
- Each alphabet replaced with 8-bit binary equivalent data
- Append zeros('0') to incase the plain text size is less than 64.

Explain the importance of using appropriate cryptographic solutions

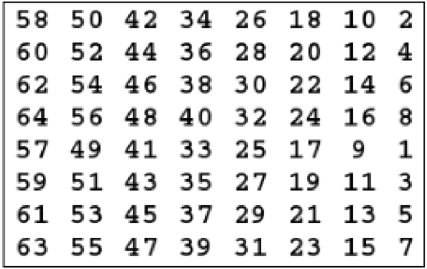
Data Encryption Standard



Data Encryption Standard

Explain the importance of using appropriate cryptographic solutions

Initial Permutation from plain text



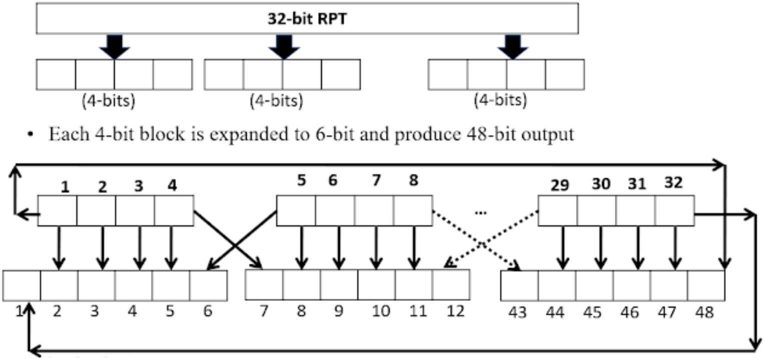
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

The first bit information of IP is equal to the 58th bit position value of the original plain text. And likeways.........

- splitting of permuted block into left and right plain text of each 32 bits as LPT(L_0) and RPT(R_0).

Explain the importance of using appropriate cryptographic solutions

RPT's 32 bit to 48 bit expainision

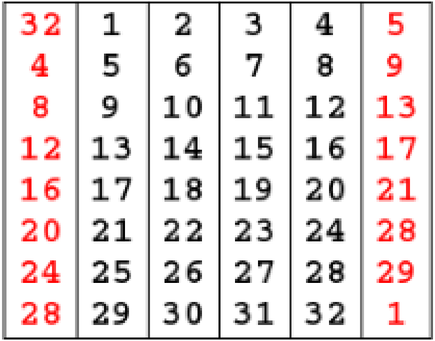


- Each 4-bit block is expanded to 6-bit and produce 48-bit output

Rewrite the same in tabular format as follows:

Explain the importance of using appropriate cryptographic solutions

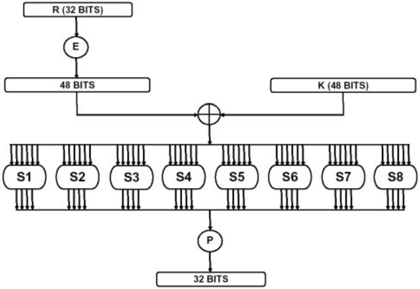
RPT's 32 bit to 48 bit expanision



32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	28
24	25	26	27	28	29
28	29	30	31	32	1

First bit of RPT(E) is the value of 32nd bit position of original RPT.

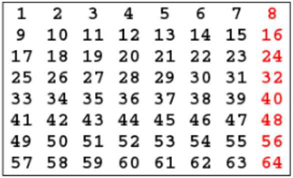
Explain the importance of using appropriate cryptographic solutions



Generation of 48 bit Subkey

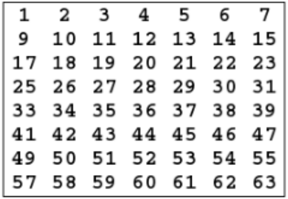
- Originally key size 64 bit. But, 56 out of 64 bits of key is used for the generation of key for the different round.
- 56 bits out of 64 bits can be formed by discarding the parity bit, i.e., the bit position 8,16, 24, 32, 40, 48, 56, 64

Explain the importance of using appropriate cryptographic solutions



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Figure: 64-bit Key and Discard of 8 pairity bits

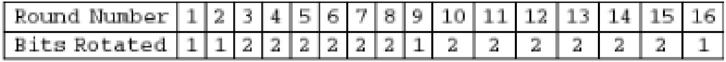


1	2	3	4	5	6	7
9	10	11	12	13	14	15
17	18	19	20	21	22	23
25	26	27	28	29	30	31
33	34	35	36	37	38	39
41	42	43	44	45	46	47
49	50	51	52	53	54	55
57	58	59	60	61	62	63

Figure: 56 bit key

Explain the importance of using appropriate cryptographic solutions

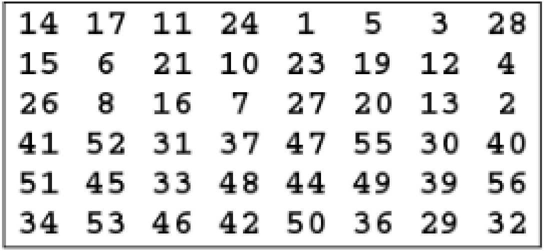
- Like splitting of permuted Plain text into LPT and RPT, now the 56-bit permuted key split into C0 and D0 of each 28 bit.
- In each round, a circular shift to the left is performed C_{i-1} and D_{i-1} by 1 or 2 bits. See the table below:



Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Explain the importance of using appropriate cryptographic solutions

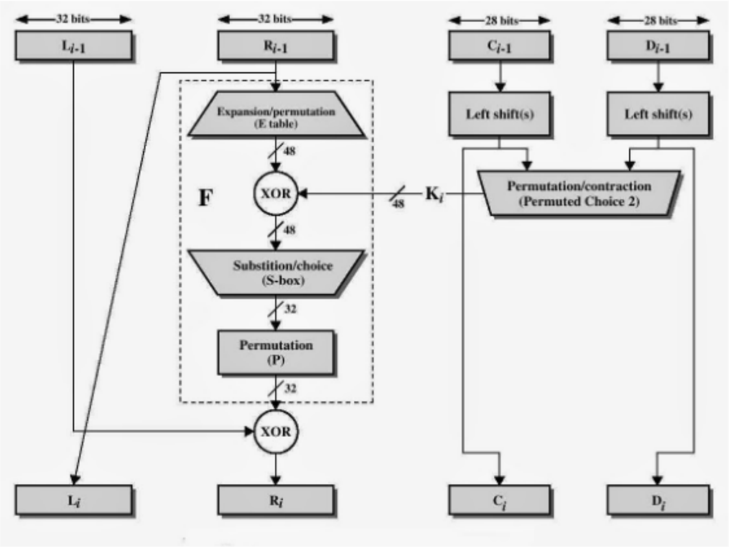
- Rotate both C_{i-1} and D_{i-1} separately as per the table.
- Find another permuted keys of 48 bits of subkeys, i.e., K_i from the combined $C_i + D_i$ whose bit positions are considered as 1 to 56:



14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Figure: Compression table, i.e., 56 bits to 48 bits

Explain the importance of using appropriate cryptographic solutions



Explain the importance of using appropriate cryptographic solutions

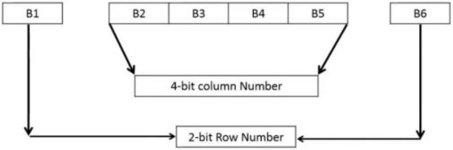
XOR operation and S-box

- Perform a bitwise XOR operation between $R_{i-1}(E)$ and K_i which resulting in another 48-bit value, *i.e.*, $K_i \oplus R_{i-1}(E)$.
- Split 48 bits into 8 groups of each of 6 bits, *i.e.*, , *i.e.*, $K_i \oplus R_{i-1}(E) = A_1A_2A_3A_4A_5A_6A_7A_8$.
- Apply the S-table to each A_i containing 6 bits,*i.e.*, $B_{i1}B_{i2}B_{i3}B_{i4}B_{i5}B_{i6}$.
- Consider the first and last bits of each group, *i.e.*, AF to determine the row number in the S-table by converting them to their equivalent decimal value. The remaining 4 middle bits,*i.e.*, $BCDE$ are considered the column number.
- Extract the corresponding value from the S-1 table using the identified row and column numbers.

Explain the importance of using appropriate cryptographic solutions

S-box & Permutation

- S-boxes is to introduce confusion and non-linearity into the encryption process.
- Convert the extracted number into its 4-bit binary equivalent. By following this process, the 48-bit value is transformed into a 32-bit. An example with S-box is given below:



Explain the importance of using appropriate cryptographic solutions

S-box & Permutation

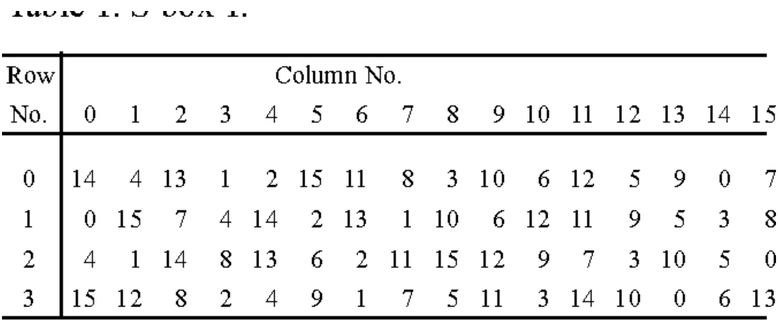


Table 1. S-box 1.

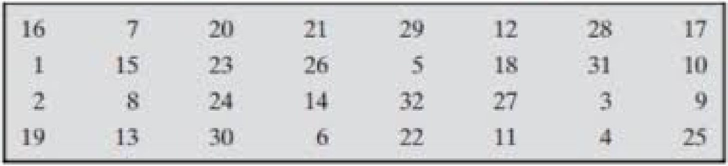
Row	Column No.															
No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Figure: S-box

Explain the importance of using appropriate cryptographic solutions

S-box & Permutation

(d) Permutation Function (P)



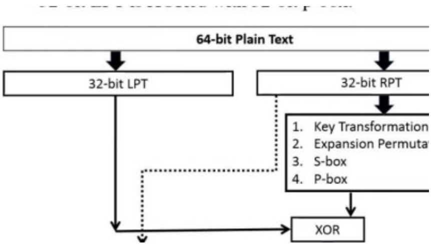
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

XOR And SWAP Operation

- That the output of P-box XORed with L_0 resulting as R_1.

Explain the importance of using appropriate cryptographic solutions

S-box & Permutation



XOR And SWAP Operation

- That the output of P-box XORed with L_0 resulting as R_1.
- And the SWAP L_0 with R_0 which resulting in as L_1

Explain the importance of using appropriate cryptographic solutions

Round-2(Input)

- $L_1 = R_0$
- $R_1 = XOR(L_0, Output_{P-box})$
- $C_1 =$Left Shifted C_0, $D_1 =$Left Shifted D_0

Cipher text/Encrypted data

- Find K_1 to $K_1 6$ by repeating the process by using input C_{i-1}, D_{i-1}.
- Find L_{16} and R_{16}
- Cipher text/Encrypted data $= L_{16} + R_{16}$.

Explain the importance of using appropriate cryptographic solutions

Question-01

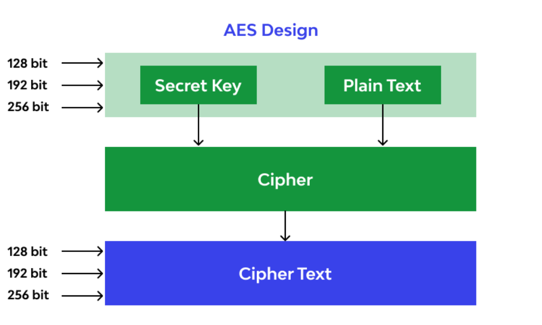
Given : Plain Text, M = (0123456789ABCDEF)Hex, K_1 = (1B02EFFC7072)Hex Determine the output after first stage using DES

Question-02

Given : 64 bit key input, K = (133457799BBCDFF1)Hex, Determine 48 bit key for DES round 1 operation (i.e. K1).

Explain the importance of using appropriate cryptographic solutions

Advanced Encryption Standard



Explain the importance of using appropriate cryptographic solutions

Advanced Encryption Standard

- AES is a Block Cipher. And developed by the National Institute of Standards and Technology (NIST) in 2001.
- AES is also known as Rijndael Encryption algorithm.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.
- Stronger and faster than Triple-DES.
- An ideal block cipher requires the encryption to be injective and surjective (bijective).
- Each plaintext maps to a unique ciphertext and each ciphertext maps to a unique plaintext.

Explain the importance of using appropriate cryptographic solutions

AES

- AES operates on **128-bit** blocks of data, which is equivalent to **16 bytes**.
- These 16 bytes are denoted as: M_0, M_1,M_2, . . . , M_{15}
- If the plaintext is **less than 16 bytes**, it is padded using the character **'Z'** until it reaches exactly 16 bytes.
- Both the **plaintext** and the **key** are arranged into a **4×4 grid (state matrix)**, filled **column-wise**.

Plaintext Matrix

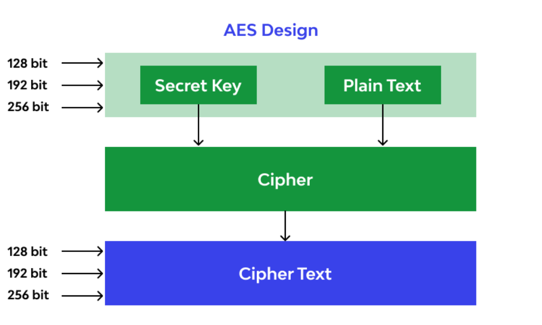
$$\begin{bmatrix} M_0 & M_4 & M_8 & M_{12} \\ M_1 & M_5 & M_9 & M_{13} \\ M_2 & M_6 & M_{10} & M_{14} \\ M_3 & M_7 & M_{11} & M_{15} \end{bmatrix}$$

Key Matrix

$$\begin{bmatrix} K_0 & K_4 & K_8 & K_{12} \\ K_1 & K_5 & K_9 & K_{13} \\ K_2 & K_6 & K_{10} & K_{14} \\ K_3 & K_7 & K_{11} & K_{15} \end{bmatrix}$$

Explain the importance of using appropriate cryptographic solutions

Advanced Encryption Standard



AES Design

128 bit

192 bit

256 bit

Secret Key

Plain Text

Cipher

128 bit

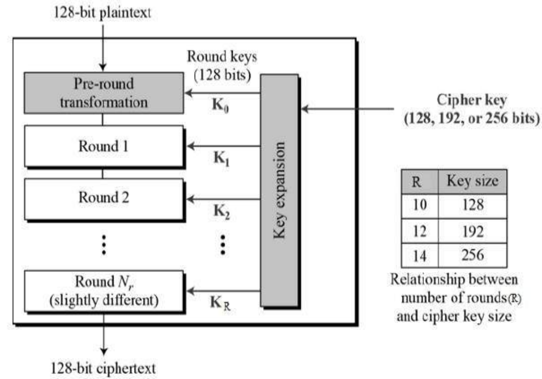
192 bit

256 bit

Cipher Text

Explain the importance of using appropriate cryptographic solutions

Advanced Encryption Standard



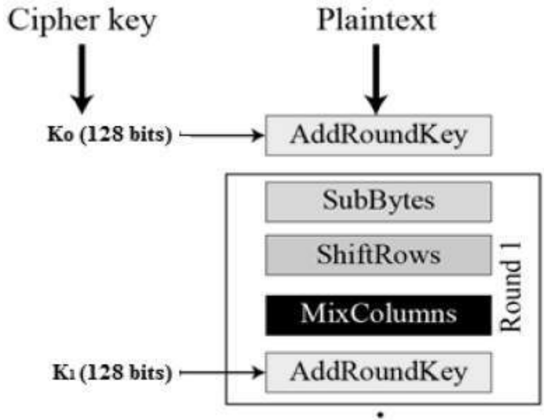
R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

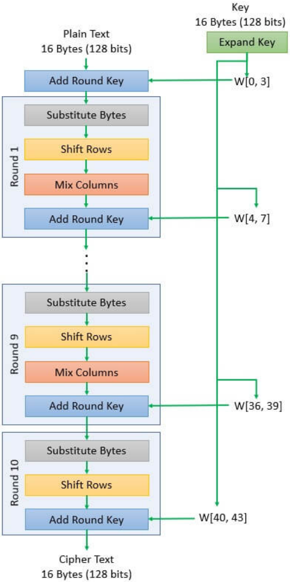
Explain the importance of using appropriate cryptographic solutions

Advanced Encryption Standard

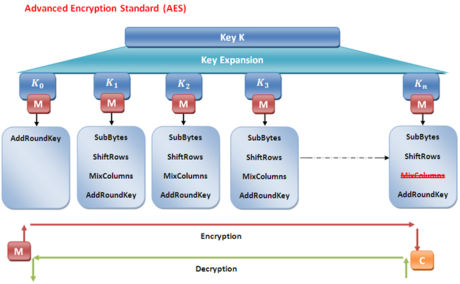
Each round comprises four sub-processes, except for the pre-round transformation and the last round.



Explain the importance of using appropriate cryptographic solutions



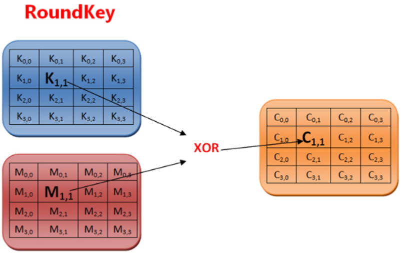
Explain the importance of using appropriate cryptographic solutions



Step-1, AddRoundKey (AES)

- XOR each byte of the **state** with the corresponding byte of the **round key**: $C_{i,j} = M_{i,j} \oplus K_{i,j}$
- Applied:
  - **Once before** the first round.
  - **At the end** of each round.

Explain the importance of using appropriate cryptographic solutions



$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

$M_{0,0}$	$M_{0,1}$	$M_{0,2}$	$M_{0,3}$
$M_{1,0}$	$M_{1,1}$	$M_{1,2}$	$M_{1,3}$
$M_{2,0}$	$M_{2,1}$	$M_{2,2}$	$M_{2,3}$
$M_{3,0}$	$M_{3,1}$	$M_{3,2}$	$M_{3,3}$

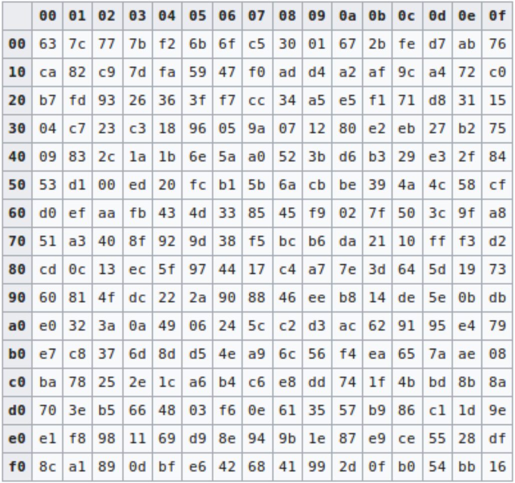
$C_{0,0}$	$C_{0,1}$	$C_{0,2}$	$C_{0,3}$
$C_{1,0}$	$C_{1,1}$	$C_{1,2}$	$C_{1,3}$
$C_{2,0}$	$C_{2,1}$	$C_{2,2}$	$C_{2,3}$
$C_{3,0}$	$C_{3,1}$	$C_{3,2}$	$C_{3,3}$

Round-Key to SubByte/S-box

- Non-linear substitution step using the S-box.
- Each byte of the state($C_{i,j}$) after AddRoundKey can be written in the Hex decimal form, which results in it as $(xy)_{16}$ is replaced with its corresponding S-box value.
- x and y represent the row and column number of S-box.

Explain the importance of using appropriate cryptographic solutions

SubByte/S-box

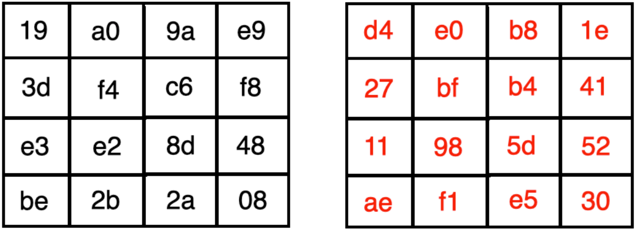


	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Explain the importance of using appropriate cryptographic solutions

SubByte/S-box

Example of Mapping:



19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Figure: Input & output of S-box

Explain the importance of using appropriate cryptographic solutions

Row Shifting

- Left circular shifts are applied to rows:
  1. Row 0: No shift
  2. Row 1: Shift by 1 byte
  3. Row 2: Shift by 2 bytes
  4. Row p: Shift by p bytes
- Enhances diffusion by rearranging byte positions.

Original Matrix (Before ShiftRows)

$$\begin{bmatrix} \mathrm{d4} & \mathrm{e0} & \mathrm{b8} & \mathrm{1e} \\ 27 & \mathrm{bf} & \mathrm{b4} & 41 \\ 11 & 98 & \mathrm{5d} & 52 \\ \mathrm{ae} & \mathrm{f1} & \mathrm{e5} & 30 \end{bmatrix}$$

Matrix After ShiftRows

$$\begin{bmatrix} \mathrm{d4} & \mathrm{e0} & \mathrm{b8} & \mathrm{1e} \\ \mathrm{bf} & \mathrm{b4} & 41 & 27 \\ \mathrm{5d} & 52 & 11 & 98 \\ 30 & \mathrm{ae} & \mathrm{f1} & \mathrm{e5} \end{bmatrix}$$

Explain the importance of using appropriate cryptographic solutions

Mix column

MixColumns is a diffusion operation in AES that mixes the bytes of each column in the State matrix using matrix multiplication in a finite field with 256 elements, i.e., GF(2^8) (Galois Field).

- To build GF(2^8), we need an irreducible polynomial of degree 8 over GF(2).
- In AES, the chosen irreducible polynomial P(x) = $x^8 + x^4 + x^3 + x + 1$(binary: 100011011, hex:0x11B).
- That the above-mentioned P(x) is an irreducible polynomial as it has no root(α) for either value of 0 or 1, *i.e.*, $P(x)|_{x=\alpha\in\{0,1\}} \neq 0$.
- That the irreducible means it can't be factored further. And it is also required for the arithmetic operation in modulo-2.

Explain the importance of using appropriate cryptographic solutions

Cont...

- Even though there exist multiple numbers of degree 8 irreducible polynomial exist. Then a question arises why we choosen $x^8 + x^4 + x^3 + x + 1$?
- It is also primitive, meaning that it generates all non-zero elements of GF(2^8) through successive powers.
- It is very efficient to implement in both hardware and software.
- $x^8 + x^4 + x^3 + x + 1 \equiv 0 \mod (x^8 + x^4 + x^3 + x + 1)$ $\Rightarrow x^8 = x^4 + x^3 + x + 1 \mod (x^8 + x^4 + x^3 + x + 1)$
- In Galois fields of modulo-2, both '+' and '-' are same. And '+' can be replaced by $\oplus$(bitwise XOR).
- $x + x = 0, 1 + 1 = 0, x^2 + x^2 = 0, x^k + x^k = 0$
- $x^8 + x^4 = x^3 + x + 1 \mod (x^8 + x^4 + x^3 + x + 1)$

Explain the importance of using appropriate cryptographic solutions

Cont...

- That the output matrix from the row shift operation will go for matrix multiplication with a fixed matrix M in GF(2^8) where all literals of matrix are in hexadecimal, i.e, $02 \rightarrow (02)_{16}$:

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

Explain the importance of using appropriate cryptographic solutions

Cont...

- $s_{0,0}^{'} = 02 \times s_{0,0} + 03 \times s_{1,0} + 01 \times s_{2,0} + 01 \times s_{3,0}$
  $\Rightarrow s_{0,0}^{'} = 02 \times s_{0,0} \oplus 03 \times s_{1,0} \oplus 01 \times s_{2,0} \oplus s01 \times s_{3,0}$
  Where $'+' \rightarrow \otimes$
- Let's calculate for the example taken in row shifting:
  $s_{0,0}^{'} = 02 \times d4 \oplus 03 \times bf \oplus 01 \times 5d \oplus 01 \times 30$
- $02 \times d4 = (0000\ 0010) \times (1101\ 0100) \mod p(x)$ where p(x) is the irreducible polynomial of degree 8.
  $= x \times (x^7 + x^6 + x^4 + x^2) = x^8 + x^7 + x^5 + x^3 \mod p(x)$
  $= (x^4 + x^3 + x + 1) + x^7 + x^5 + x^3 = x^7 + x^5 + x^4 + x + 1$
  Where $x^3 + x^3 = 0$ and $x^8 = x^4 + x^3 + x + 1$
  $= x^7 + x^5 + x^4 + x + 1 = (1011\ 0011) = b3$
- Similarly, others can be determined as 03 × bf = da, 01x 5d =5d, and 01x 30 =30.

Explain the importance of using appropriate cryptographic solutions

Cont...

- $s'_{0,0} = 02 \times d4 \oplus 03 \times bf \oplus 01 \times 5d \oplus 01 \times 30$
  $= b3 \oplus da \oplus 5d \oplus 30$
  $= 10110011 \oplus 11011010 \oplus 01011101 \oplus 00110000 = 04$
- The remaining literals of the matrix can be calculated using the same procedure.

Explain the importance of using appropriate cryptographic solutions

Diffie-Hellman Key Exchange

- Diffie–Hellman (DH) Key Exchange securely shares cryptographic keys over an insecure channel without their conversation being transmitted over the internet.
- The goal of Diffie-Hellman key exchange is to securely generate and share a key for symmetric encryption.
- It's a core part of secure protocols like SSL/TLS and SSH, VPN. SSL – Secure Sockets Layer; TLS – Transport Layer Security; SSH – Secure Shell; VPNs-Virtual private networks.
- It is also known as exponential key exchange.

Explain the importance of using appropriate cryptographic solutions

Steps of DH Key exchange

- Let two end users, Alice and Bob, both are agreed to share a secret key over an insecure channel.
- Consider p and q, such that p is a prime number and q is a generator of p and primitive root modulo p. And p is a large number and q is small number.
- Choose two personal keys as a and b for Alice and Bob respectively.
- Now compute public key from the both ends as:
  - Alice: $a^* = q^a mod\ p$
  - Bob: $b^* = q^b mod\ p$
- Now public key received at other ends is given by:
  - Alice will receive b^*
  - Bob will receive a^*

Explain the importance of using appropriate cryptographic solutions

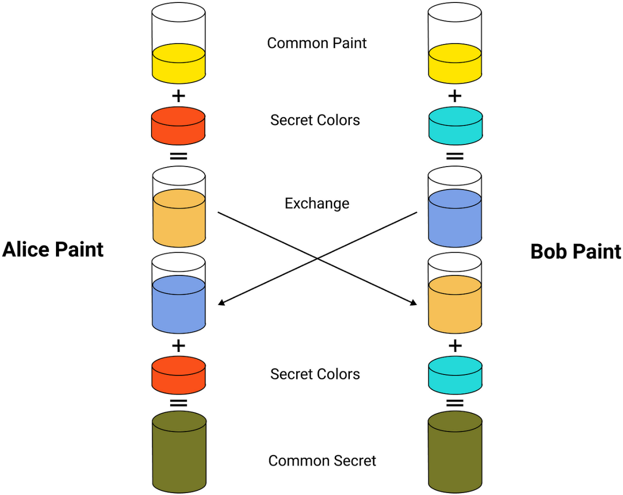
Steps of DH Key exchange

- The encryption and decryption key to be used at the end user(s) can be calculated as follows: $x = {b^*}^a mod\ p = {a^*}^b mod\ p$

Advantage and limitation of DH Key exchange

- Forward Secrecy: New keys can be generated for each session, so compromising one key doesn't affect others.
- Scalable: Efficient even with many participants—only a few exponentiations per party are needed.
- No Prior Trust Needed: Works without pre-shared secrets, ideal for first-time communications.
- Vulnerable to MITM Attacks: Lacks built-in authentication.

Explain the importance of using appropriate cryptographic solutions



Explain the importance of using appropriate cryptographic solutions

Short note on primitive root

A number g is called a **primitive root of modulo** n if powers of g generate all numbers that are coprime to n under modulo n arithmetic.

- That is, $g^1, g^2, ..., g^k$ should produce all numbers from 1 to $n - 1$ that are coprime to n, without repetition. Where $k = p - 1$.
- $2^k \equiv 1 \; mod \; p$.
- For example, 3 can be a primitive root of modulo 17, and whereas 2 and 4 can't be a primitive root of modulo 17.
- The private keys, *i.e.*, a, b must be less than p, *i.e.*, $1 < a, b < p$.

Explain the importance of using appropriate cryptographic solutions

Question-01

Consider p=17, α= 3 (3 is primitive root of 17). A and B discrete private keys a=15and b=12. Find the secret key used for encryption and decryption.

Ans.: $a^{*} = 3^{15} mod\ 17 = 6$ and $b^{*} = 3^{12} mod\ 17 = 4$
At Encryption end: $x = {b^{*}}^{a} mod\ 17 = 4^{15} mod\ 17 = 13$
At Decryption end: $x = {a^{*}}^{b} mod\ 17 = 6^{12} mod\ 17 = 13$
$\Rightarrow x = 13$ is used as key for the encryption and decryption.

Question-02

Consider p=353, α= 3 (3 is primitive root of 353). A and B discrete private keys a=97and b=223. Find the secret key used for encryption and decryption.

Explain the importance of using appropriate cryptographic solutions

RSA Algorithm

RSA (Rivest–Shamir–Adleman) is a classic and widely used example of public-key cryptography (also known as asymmetric cryptography).

- Two keys are used:
  - Public Key – used to encrypt data; shared openly.
  - Private Key – used to decrypt data; kept secret by the owner.
- RSA relies on the computational hardness of factoring large prime numbers.
- Application: Secure data transmission, Digital signatures, SSL/TLS (for HTTPS websites), Email encryption (e.g., PGP)

Explain the importance of using appropriate cryptographic solutions

RSA Algorithm's step by step

- **Select two large primes:** p and q
- **Compute modulus:** $n = p \times q$
- $n > m$ where m is the plaintext message.
- **Compute Euler's totient:** $\phi(n) = (p-1)(q-1)$
- **Choose public exponent:** e such that

$$1 < e < \phi(n) \quad \text{and} \quad \gcd(e, \phi(n)) = 1$$

(Common choice: $e = 65537$)

- **Compute private key:** $ed \equiv 1 \mod \phi(n)$
  $d \equiv e^{-1} \mod \phi(n)$ (*i.e.*, $d \cdot e \equiv 1 \mod \phi(n)$)

Explain the importance of using appropriate cryptographic solutions

RSA Algorithm's ....

- **Public Key:** (n, e); **Private Key:** n, d
-
    - Encryption: $c \equiv m^e \mod n$
    - Decryption: $m \equiv c^d \mod n$

Question

Perform encryption and decryption using the RSA algorithm for the following:

$$p = 3;\ q = 11;\ e = 7;\ M = 5$$

Ans.: Find:

$$n = p \cdot q = 3 \cdot 11 = 33 \tag{1}$$

$$\phi(n) = (p-1)(q-1) = 2 \cdot 10 = 20 \tag{2}$$

$$gcd(e, (n)) = 1 \tag{3}$$

Explain the importance of using appropriate cryptographic solutions

Ans........

Now, we need to compute $d = e^{-1} \mod \phi(n)$
From RSA: $ed \equiv 1 \mod \phi(n)$
Now choose smallest k, for which $ed = k\phi(n) + 1$, *i.e.*, e is a factor of $k\phi(n) + 1$.
So, $d = \frac{k.\phi(n)+1}{e} \equiv e^{-1} \mod n$.
Now, $e = 7$(given); $\phi(n) = 20$(calculated);
by iteration, for $k = 1$, the $e = 7$ becomes a factor of $1.20 + 1 = 21$. From this, $d = 21/7 = 3 \mod 20$.

- **Public key** = (33,7) and **Private Key** = (33,3)
- **Plaintext=M=5**, find encrypted message.
- **Encrypted Message=C=** $M^e \mod n = 5^7 \mod 33 = 14$
- **Decrypted Message=Plaintext=** $C^d \mod n = 14^3 \mod 33 = 5$...**Ans.**

Explain the importance of using appropriate cryptographic solutions

Tools

Tools used in data security and encryption that help protect sensitive information, ensure data integrity, and secure digital communications. Let's discuss four networkworthy tools as follows:

- TPM
- HSM
- Key management system
- Secure enclave

Explain the importance of using appropriate cryptographic solutions

TPM (Trusted Platform Module)

- A TPM is a hardware-based security component integrated into computers and devices.
- It generates, stores, and manages cryptographic keys in a secure environment.
- TPMs improve system security by ensuring the integrity of boot processes, enabling hardware-based authentication, and supporting encryption operations.
- TPM checks if your computer starts up the right way and protects it from being tampered with.

Explain the importance of using appropriate cryptographic solutions

HSM (Hardware Security Module):

An HSM is a special physical device that keeps important cryptographic keys safe and helps with secure tasks like encrypting and decrypting data. It's built to protect sensitive information from hackers or even internal and external misuse. HSMs are often used by banks, hospitals, and online businesses to make sure their data stays private and secure.

Key Management System (KMS):

A KMS is a software tool that helps safely create, store, and manage cryptographic keys. It keeps track of when to update, share, or revoke these keys. KMS makes sure that only the right people can access the data, helping keep information secure during things like encryption, decryption, and digital signatures.

Explain the importance of using appropriate cryptographic solutions

Secure Enclave:

A secure enclave is a special, protected part of a computer's processor that keeps sensitive information—like fingerprints, passwords, or secret keys—safe from hackers and harmful software. It works separately from the main system so that even if the rest of the device is attacked, the data inside the enclave stays protected. This feature is used in modern devices (like iPhones with Apple's T2 chip) to make sure your private data stays private.

Explain the importance of using appropriate cryptographic solutions

Obfuscation:

Obfuscation is a way of hiding how software really works from hacking, to safeguard intellectual property and reverse engineering by making its code or data harder to read or understand. It's like turning clear instructions into a puzzle, so that hackers or competitors can't easily figure out how it works or steal it. This helps protect sensitive parts of a program and makes it tougher to break into or copy. A few techniques of this kind:

- Steganography
- Tokenization
- Data masking

Explain the importance of using appropriate cryptographic solutions

Steganography

- Technique of hiding secret data within ordinary files (e.g., images, audio, video).
- Like placing a secret note inside an innocent-looking envelope.
- How It Works: Makes subtle changes to files that are not easily noticeable.
- Objective: To conceal information from unauthorized access or detection.
- Applications:
  1. Covert communication
  2. Digital watermarking
  3. Protecting sensitive data in a hidden format

Explain the importance of using appropriate cryptographic solutions

Tokenization

- Converts sensitive data into unique, meaningless tokens.
- Tokens replace real data during transactions to enhance security.
- Tokens hold no real value, so even if stolen, they're useless.
- Application:
    1. Widely used in payment systems and data protection frameworks.
    2. Reduces risk of data breaches
    3. Keeps original data secure
    4. Ensures safe data handling and compliance

Explain the importance of using appropriate cryptographic solutions

Data masking

- Replacing sensitive data with fake but realistic values.
- To protect privacy while allowing data use in testing or analysis.
- Like wearing a mask — identity hidden, but appearance looks real.
- Use Case: Healthcare data can be masked by replacing names and IDs for research.
- Advantages:
  1. Prevents data leaks
  2. Keeps data format intact
  3. Supports secure data sharing
  4. Ensures regulatory compliance

Explain the importance of using appropriate cryptographic solutions

Hashing

A hash function is a mathematical function that takes an input (of any length) and transforms it into a fixed-length string of characters.

- Input: Can be of any length (short text, long file, etc.)
- Output: Always of fixed length (e.g., 128-bit for MD5, 256-bit for SHA-256)
- This process is like compressing a large balloon into a compact ball — simplifying and reducing the input while preserving uniqueness.
- Each input generates a unique "fingerprint" (hash). Even a minor change in input gives a very different hash.
- Collision Resistance: It is very difficult to find two different inputs that produce the same hash value.

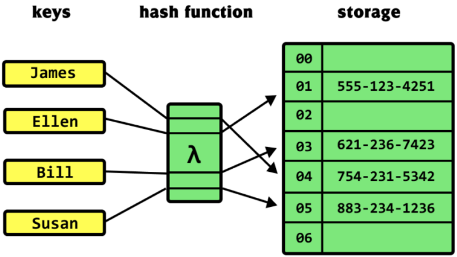
Explain the importance of using appropriate cryptographic solutions

Hashing

- Use Cases:
  1. Password Storage: Passwords are stored as hash values (not actual text).
  2. Digital Signatures: Ensures message authenticity and sender verification.
  3. Digital Signatures: Ensures message authenticity and sender verification.
  4. Data Integrity Checks: Helps detect whether data has been tampered with.
- Hash Value: The output produced by a hash function is called a hash value or message digest.

Explain the importance of using appropriate cryptographic solutions

Hashing



00	
01	555-123-4251
02	
03	621-236-7423
04	754-231-5342
05	883-234-1236
06	

Explain the importance of using appropriate cryptographic solutions

Salting

- Adding random data (salt) to passwords before hashing.
- Enhances password security by making each hash unique, even for identical passwords.
- Defense Against:
  1. Rainbow table attacks
  2. Brute-force attacks
- The salt is combined with the password, then the result is hashed and stored.
- Advantages: Adds unpredictability, making it much harder for hackers to crack hashed passwords.

Explain the importance of using appropriate cryptographic solutions

Digital Signatures

- A digital signature is the electronic version of a handwritten signature, uniquely tied to the signer and the document.
- Objective: Ensures authenticity, integrity, and non-repudiation of digital documents.
- How It Works:
  1. The signer uses their private key to generate a unique signature.
  2. This signature is attached to the document.
  3. The recipient uses the public key to verify it.
- Confirms the document was not tampered with. And also proves the signer's identity and involvement.

Explain the importance of using appropriate cryptographic solutions

Digital Signatures

- Advantages:
  1. Provides a secure, tamper-evident way to verify digital documents.
  2. Widely used in secure communications, contracts, and digital certificates.

Explain the importance of using appropriate cryptographic solutions

Key Stretching

- A cryptographic technique that transforms a simple password into a longer, more secure key.
- Objective is to to slow down brute-force or dictionary attacks by increasing the time needed to guess passwords.
- How It Works: Repeatedly applies a hashing algorithm to make password cracking computationally expensive.
- Effect: Increases the time and effort required for hacking attempts.
- Different Techniques:
  1. PBKDF2: Applies a hash function multiple times to slow down key derivation.
  2. Bcrypt: Adds salt and uses multiple hashing rounds to secure passwords.

Explain the importance of using appropriate cryptographic solutions

Blockchain

- A digital, decentralized ledger made of linked data batches called blocks.
- Initially created for Bitcoin, but now used across various sectors.
- Structure: Each block contains data and a hash. Blocks are linked to form a chain, ensuring continuity and security.
- Decentralization: Data is distributed across many computers (nodes). Tampering requires altering every copy, making it nearly impossible.
- Proof of Work:
  1. To add a block, a computer must solve a cryptographic puzzle.
  2. This ensures consensus and security before data is accepted.

Explain the importance of using appropriate cryptographic solutions

Blockchain

- Applications Beyond Cryptocurrency:
  1. Financial transactions
  2. Medical records
  3. Property ownership
- Example: Inheritance of a house: If deeds are stored on the blockchain, siblings can verify ownership through the public ledger.

Explain the importance of using appropriate cryptographic solutions

Open Public Ledger

- It is defined as a digital record of all transactions in a blockchain network, visible to all participants.
- Everyone in the network can view, verify, and audit transactions in real time.
- Decentralization:
  1. Not controlled by a single authority.
  2. Multiple copies are stored across network nodes (computers).
- Security: Highly tamper-resistant due to cryptography and decentralization.
- Transaction Recording: Transactions are broadcast to the network. Verified by participants based on blockchain rules.

Explain the importance of using appropriate cryptographic solutions

Open Public Ledger

- Consensus Mechanisms: Methods like Proof of Work (PoW) or Proof of Stake (PoS) ensure participants agree on valid transactions.
- Immutability & Chronological:
  1. Once added, a transaction is permanent.
  2. Each block links to the previous one, ensuring a chronological and tamper-proof chain.
- Transparency:
  1. Anyone can verify transactions.
  2. Promotes trust and accountability in the network.

Explain the importance of using appropriate cryptographic solutions

Certificates

- Certificates means digital certificate here, acts like a digital passport, ensuring secure online interactions.
- Used to verify identities and encrypt communications.
- Core Elements of Certificate Systems:
  - Certificate Authorities (CAs) Role: Validate digital identities using cryptographic keys. Different types of CAs as follows:
    1. Online CA: Fast, real-time verification (less secure).
    2. Offline CA: Operates in isolation (more secure).
    3. Public CA: Secures internet websites (e.g., DigiCert).
    4. Private CA: Used within internal networks.
  - Root of Trust Root Key:
    1. The base of all trust in a Public Key Infrastructure (PKI).
    2. Root Certificate: Self-signed and used to validate all issued certificates.
    3. Devices trust a certificate if it traces back to a trusted

Explain the importance of using appropriate cryptographic solutions

Certificates

- CRLs (Certificate Revocation Lists):
  - Lists revoked, expired, or compromised certificates.
  - Maintained and published by CAs.
  - Users check serial numbers against the CRL.
  - Can be large and slower to access.
- OCSP (Online Certificate Status Protocol):
  1. Offers real-time certificate validation.
  2. Queries CA server for the current status (valid, revoked, expired).
  3. Faster than downloading CRLs.
- Types of Certificates:
  - Self-signed Certificates:
    1. Signed by the same entity that issues it.
    2. Not trusted by browsers/public users.
    3. Useful for internal use (e.g., development/testing servers).

Explain the importance of using appropriate cryptographic solutions

Certificates

- Types of Certificates:
  - Third-party Certificates:
    1. Issued by trusted CAs (e.g., GlobalSign, Thawte).
    2. Globally recognized and ideal for commercial websites.
- Certificate Lifecycle:
  - CSR (Certificate Signing Request):
    1. A file created when requesting a certificate from a CA.
    2. Includes: Name, domain, public key, and certificate purpose.
    3. Like a blueprint for the certificate.
- Wildcard Certificates: Secures multiple subdomains under a single domain.
- Example:
  1. *.securityplus.training
  2. Covers: web.securityplus.training, mail.securityplus.training, etc.

References

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End