2

SL.NO:CAA176329

SRI SIVASUBRAMANIYA NADAR COLLEGE OF ENGINEERING

(An Autonomous Institution, Affiliated to Anna University, Chennai)
Rajiv Gandhi Salai (OMR), Kalavakkam – 603 110

THEORY EXAMINATIONS

74%

Register Number	205001085		
Name of the Student	V. Sabasivasan		
Degree and Branch	BE CSE	Semester	V
Subject code and Name	UCS1505 Cryptographic techniques.		
Assessment Test No.	II	Date	19/10/2022

Details of Marks Obtained									
Part A		Part B				Part C			
Question No.	Marks	Question No.	(a) Marks	(b) Marks	Total Marks	Question No.	(a) Marks	(b) Marks	Total Marks
1	2	7	4		4	10			
2	2					11	7		7
3	0	8	6		6				
4	2					12	10		10
5	2	9				13			
6	2								
Total (A)	10	Total (B)			10	Total (C)			17
Grand Total (A+B+C)	37			Marks (in words)	Three	Seven			
Signature of Faculty									

SSN

PART-C

(12) $x \equiv 1 \bmod 3 \rightarrow (1)$

$x \equiv 4 \bmod 5 \rightarrow (2)$

$x \equiv 6 \bmod 7 \rightarrow (3)$

Chinese Remainder Theorem

⇒ It is an algorithm used on equations which have single variable but have different module.

⇒ The equations are in the format,

$$x = a \pmod m$$

Solution:

$$x = (a_1 M_1 M_1' + a_2 M_2 M_2' + \dots a_n M_n M_n') \bmod M$$

From equations (1), (2), (3).

$a_1 = 1$ | $m_1 = 3$

$a_2 = 4$ | $m_2 = 5$

$a_3 = 6$ | $m_3 = 7$

$\Rightarrow M = m_1 m_2 m_3 = 3 \times 5 \times 7$

$\boxed{M = 105}$

$\Rightarrow M_1 = M/m_1 = 105/3 = 35$

$\Rightarrow M_2 = M/m_2 = 105/5 = 21$

$\Rightarrow M_3 = M/m_3 = 105/7 = 15$

$\Rightarrow M_1 \times M_1^{-1} \equiv 1 \bmod m_1$

$35 \times M_1^{-1} \equiv 1 \bmod 3$

$\boxed{M_1^{-1} = 2}$

$\Rightarrow M_2 \times M_2^{-1} \equiv 1 \bmod m_2$

$21 \times M_2^{-1} \equiv 1 \bmod 5$

$\boxed{M_2^{-1} = 1}$

$\Rightarrow M_3 \times M_3^{-1} \equiv 1 \bmod m_3$

$15 \times M_3^{-1} \equiv 1 \bmod 7$

$\boxed{M_3^{-1} = 1}$

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (1(35)(2) + 4(1)(21) + 6(15)(1)) \bmod 105$$

$$= (70 + 84 + 90) \bmod 105$$

$$= 244 \bmod 105$$

$$\boxed{x = 34}$$ //

SSN

(11) ~~What is~~ (5)

Double DES:

PART-A

(1) Diffusion and Confusion:

⇒ It is a technique used in substitution-permutation networks. For a truly random permutation, changing the first bit of input would be expected to affect the bytes of the output

⇒ A diffusion step is introduced where the bits of output are permuted using mixing permutation. This confusion / diffusion steps together called a-round are repeated multiple times.

(5) gcd (1076, 1970)

= gcd (1076, 894)

= gcd (182, 894)

= gcd (182, 712) = gcd (182, 530)

= gcd (182, 348) = gcd (182, 166)

= gcd (16, 166) = gcd (16, 150)

= gcd (16, 134) = gcd (16, 118)

= gcd (16, 102) = gcd (16, 86)

= gcd (16, 70) = gcd (16, 54)

= gcd (16, 38) = gcd (16, 22)

= gcd (16, 6) = gcd (10, 6)

= gcd (4, 6) = gcd (4, 2)

= gcd (2, 2)

= 2 ///

(2) Avalanche effect:

In any block cipher, a small change in input must affect every bit of output. To induce avalance effect in SPN, two properties holded.

i) The S-boxes are designed so that changing an input would result in changing the other bits.

ii) The mixing permutations are designed so that bits output by any S-box affect the input of S-boxes in next round.

(3) Fermat's Little Theorem:

$$a^{p-1} \bmod p = 1$$

where p is prime number and

$$\gcd(a, p) = 1$$

(4)

DES	AES
DES stands for Data encryption standard.	AES stands for Advanced Encryption standard.
Bit oriented	Byte oriented.
Key length = 128 bits, 192 bits and 256 bits	Key length = 56 bits.
Structure based on substitution-permutation network.	Structure based on Feistel network.

(6) Algebraic structures.

i) Groups
ii) Fields
iii) Rings.

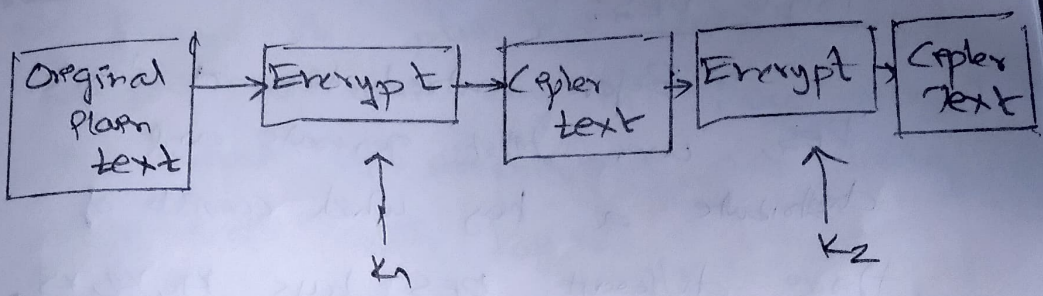
PART-C

(11) Double DES:

⇒ Double DES is an encryption approach which uses two examples of DES on same plain text. It provides different keys to encode the plain text.

⇒ Double DES is easy to implement. Double DES uses two keys K_1 and K_2. It can implement DES on original plain text using K_1 to get the encrypted feild text.

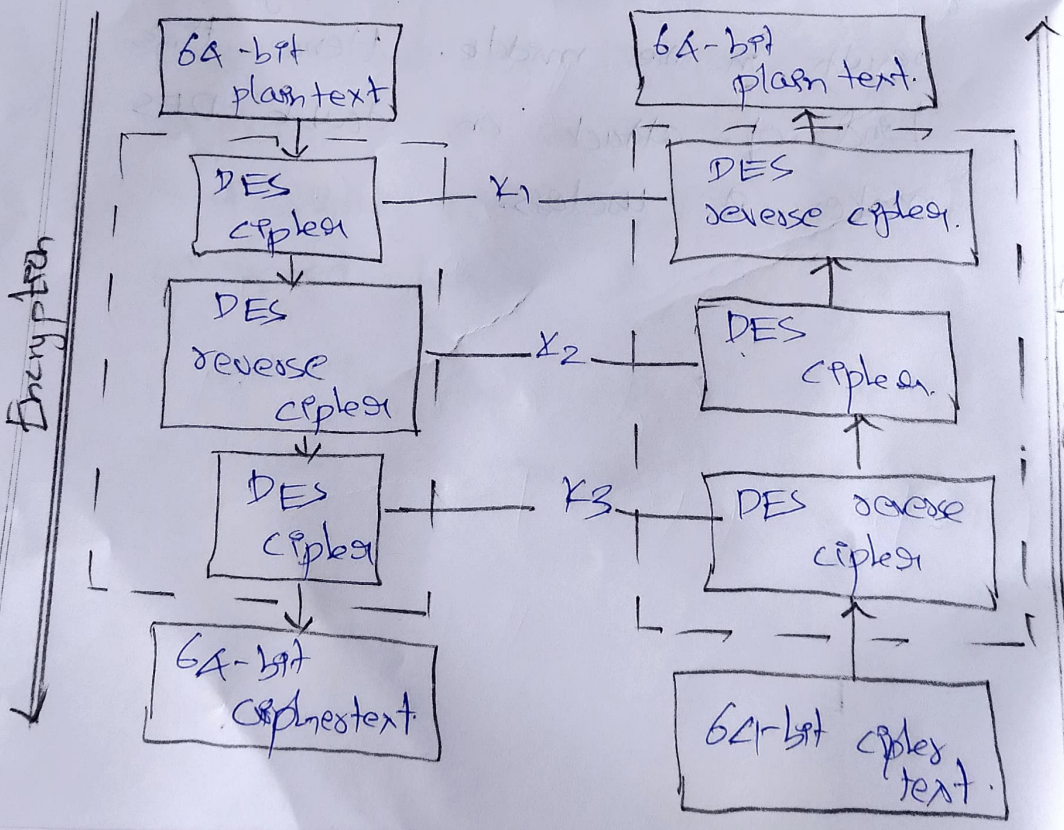
⇒ The final output is the encryption of encrypted plain text.



⇒ It introduced the term of meet-in the-middle attack. This attack contains encryption from one end, decryption from the other and connecting the results in the middle. Hence this kind of attack on double DES makes it useless.

Triple DES:

⇒ Before introduction of triple DES, user first generate and distribute a key which consists of three different DES keys K1, K2, K3. This means that the key length is 3x 56 = 168 bits. The encryption scheme of triple DES is as follows,



⇒ Encrypt the plain text blocks using single DES with key K_1. Now decrypt the output of ~~the~~ previous step using single DES with key K_2.

⇒ Finally encrypt the output of previous step using single DES with key K_3

⇒ The final output will be ciphertext.

⇒ Decryption of ciphertext is a reverse process.

⇒ Triple DES provides backwards compatibility with DES.

⇒ Triple DES are more secure than single DES and double DES.

~~but slow~~

SSN

PART-B

(6) Euler's Totient function:

(i) $\phi(440)$

$\Rightarrow \phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots$

$\Rightarrow 440 = 2^3 \times 11 \times 5.$

$\therefore \phi(440) = 440\left(1-\frac{1}{2}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{5}\right)$

$= 440\left(\frac{1}{2}\right)\left(\frac{10}{11}\right)\left(\frac{4}{5}\right)$

$= 160 //$

(ii) $\phi(27)$

$\Rightarrow 27 = 3^3$

$\Rightarrow \phi(27) = n\left(1-\frac{1}{p}\right)$

$= 27\left(1-\frac{1}{3}\right) = 27\left(\frac{2}{3}\right)$

$= 18 //$

(iii) $\phi(231)$

$\Rightarrow 231 = 11 \times 7 \times 3.$

$\Rightarrow \phi(231) = 231\left(1-\frac{1}{11}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{3}\right)$

$= 231\left(\frac{10}{11}\right)\left(\frac{6}{7}\right)\left(\frac{2}{3}\right)$

$= 120//.$

---

(7) Message Authentication Code (MAC)

⇒ Message Authentication Code is a cryptographic checksum on data that uses a key to detect both accidental or intentional modification on data.

⇒ MAC requires two inputs : a message and a secret key only to the messenger.

SSN

MAC	One-Way Hash
Small plain text to authenticate a message.	Specific type of MAC that involves cryptographic hash functions and a cryptographic key.
Stands for Message Authentication Code.	Stands for Hash based Message Authentication Code
Plaintext is passed to receiver along with a tag attached to PT.	Each plaintext is passed as an input to a hash function to provide a unique hash value