## INS-Assignment-02

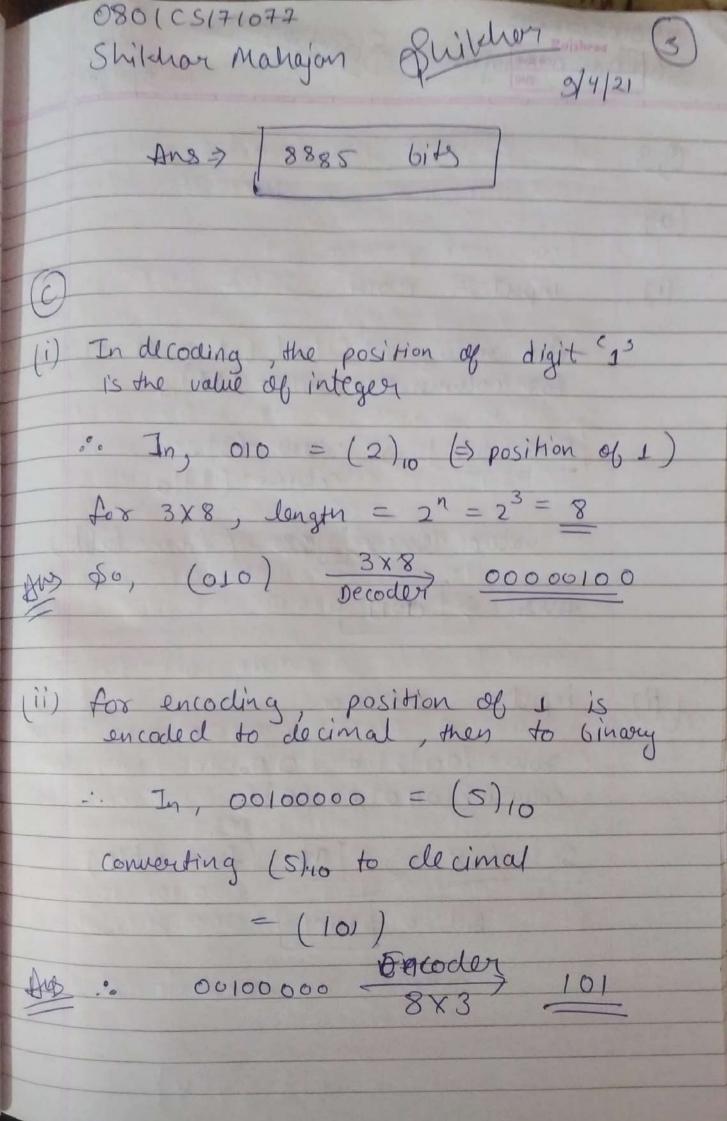
(a) Galois field is valid if in G(n) 7 n is of the form pr where, p is a prime number n is a whole number. i.e., n should be pourer of some perime number GF(12) = GF(3x22) = In-Valid GF (13) = GF(131) = Valid GF (16) = GF (24) = Valid 1(2) (3) GF (17) = GF (171) = Valid 14) (5) 4F (19) = 4F (191) = valid.

(2)  $100001 = \frac{1}{1.25} + 0.24 + 0.$ (1) 10 =) 1n1+0n0=1n 

(4) 00011

| 0801CS171077 0: War Rejohree 2 |  |  |
|--------------------------------|--|--|
| Shikhan Mahajan Shikhar 9/4/21 |  |  |
| 0                              | 7 0  |  |
|                                |  |  |
| 02                             | And the second s |  |
| 9                              |  |  |
| ii                             | (01001101) D (01001101) = 00000000   |  |
| (1)                            | (01001101) (+) (01001101)  |  |
| (ii)                           | (01001101) ( (10110010) = 11111111   |  |
| ( )                            | The state of the s |  |
| (iii)                          | (01001101) (D00000000) = 01001101  |  |
| 111                            | [0]00[]  |  |
| (iv)                           | (01001101) (1111111) = 10110010  |  |
|                                | (12N3-121) 3 to 12N  |  |
|                                |  |  |
| (6)                            | 104 - 4 (Sa) 1 - (B) 9 A (B)   |  |
| 10000                          | Ensollment No. = 0801CS171077  |  |
|                                | Rost Cin   |  |
| Photo:                         | last fine = n = 71077  |  |
| ALCOHOL:                       | Number of 6118 = 71072 # 0   |  |
| 1300                           | Number of 61ts = 71077 \$ 8<br>(assuming 8 6it char) = 568616  |  |
| 4000                           | <u> </u>   |  |
|                                |  |  |
|                                | => Size ob padding = 64 - (568616 %69) = 64 - 40   |  |
| 1861                           | = 64 - 40  |  |
|                                | = 24   |  |
| 20.1                           | No of blocks = (com  |  |
|                                | No. of 610cks = (568616 + padding  |  |
|                                | 164  |  |

= (568616 + 24)/64



|      | non mahayan Shikhan 3/4/21  |
|------|---|
| 0,3  |   |
| (a)  |   |
| (i)  | input = 11011)  |
|      | for now = 1st & last bit = 11 = (3)/0<br>for column = 1011 = (11)/0     |
|      | (S-3 66X) => YOW =(3) 10<br>Column = (11)10                             |
|      | value Ross (from table)   |
|      | Aus > aoil  |
| (ii) | input = 001100 $70w = (00)_2 = (0)_{10}$ $column = (0110)_{=} (6)_{10}$ |
|      | S-4 box => [3] (from table)   |
|      | Ans = [100]   |
|      |   |

0801 05171077 Shikhan 3/4/21 Shikhar Mahajan input = 000000 (111) row = (00/2 = (0),0 S-7 box > value = 43 (from table) Ans = 0100 (iv) input = 1111118  $7000 = (11)_2 = (3)_{10}$   $(0)umn = (11)_2 = (15)_{10}$ S-2 box > value = 98 (from table) Aug = (1001@) value binway value Yow column (b) So 0 110/ 1111 SI 1010 10 011) 0 53 0010 2 1100 4 0100 56 1101 13 57 input = 000000

EFOIE1821080 Shilahar Medigan Righan

9/4/21

No pattern is found neither in binary nor in decimal values.

ley with parity bit 0123 ABCD 2562 1456

Doop every 8th 614 0123 = 0000 000x 0010 001x ABCD = 1010 101x 1100 110x 0010 010/ 0110 0010 2562 = 1486= 0001 0106, 0101 0110

Key without parity 00 00000 0010001 1010101 1100110 0010010 011000] 0 00/010 0/0/0/1

Permutate a/c to parity bit doop table

P(1 = Co 0000110 0/0/0/0 0000110 1101100 10/0011 0110110 00 00001 1000000

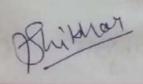
Shift left on both halves.

9= 0001100 1010/00 000 1101 10/1000 DI = 0100110 0000011 1101100 ()00 000)

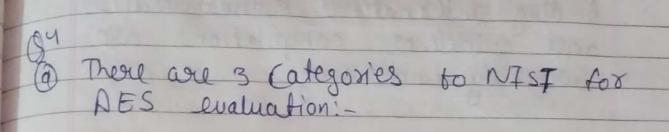
Now , resente by key Crenerate fail he

(Key = 1437 4013 3784)

0801CS171077 Shikhar Mahajan



9/4/21



- Algorithm: Algorithm and Implementation characteristics include flexibility, hardone and software suitability and addition features offered by a condidate algorithm.
- 6) Cost Cost includes likening of requirements
  computational efficiency and memory
  requirements.
- Security: Security is the paramount consideration in AES selection process and encompasses issues like the relatione occurring of I condidate compared to other, and the extinct to which algorithm output is indistinguishable from random permutation.
- E) Lightweight cryptography is an method that features a small tootprint and low computational complexity. It is aimed at expanding the applications to constrained davices and its related

0801CS171077 Shirthan Mahajan

Shirthar

S)4/21

binding international standardisations and quidelines compilations are currently underway

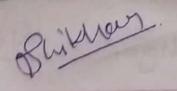
# Requirement in 21st Contrary

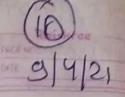
In the era of technology advancement all kinds of devices from powerful super computers and servers with high computating device are being connected via interest with these advancement it brings to the failure of convention cruptographic methods for the sake of sewrity and performance requirement appecially in resources constrained devices

Therebose, the cruptographic community has been working to design efficient algorithms that can be implemented on resource constrained devices without compromising security or performance and thus, there is need of hightweight cruptography in the worent 21st Century

0801 CS 171077 3/4/21 Blitchan Shikhar mahajan 99 for configuring firewall, there are steps: Aus Step 1 Secure your fixewall It an attacker is able to gain administrative access to your fixewall it is game over for your network. Therefore, sewing, your froewall is the first and impostant step of this process. update your fixewall to the latest fromware Delete, disable or rename user accounts and change all default passwords. for multiple administration, create addition administration accounts with Disable SNMP or configure it to use a secure community etting Step-2 Architect your fixewall zones and IP addresses In order to protect valuable ossets of

5801CS171077 SHKhar Mahajam





your network, you should first identy what the assets are. Then plan out of your retwork structure so that these assets can be grouped to gether and placed into networks based on similar sensitivity fevel and function

Step 3: Configure access control list

After establishing notwork on zones and the interfaces we should determine exactly which traffic needs to be able to flow in and out of each zones.

The Isaffic will be permitted using firewall rules called access control lists (ACL) which are applied to each interface of sub-interface on the firewall.

Make ACL's sporific to exact sowice and destination IP addresses and post numbers and make sure to there is dony all rule to filter out all upapproved Iraffic

080163171077 Shikhar Mahajon Blishor 9/4/21

Apply both inbound and outbound Acis only approved traffic is allowed into

Step-4 Configure your other fixewall services and logging.

If your fixewall is also capable of protocol (DMCP) server network time protocol (NTP) server etc. then go ahead and configure the services and disable all the extra services.

To fulfill PCI DSS requisements configure your fixewall to report your logging some and make sure that enough detail is include to satify requirement 10.2

Step-5 Test your fishwall configuration

In a test environment verify that your fixewall works as intended. Don't forget to nevity that your fisewall is blocked according to your ACL configurations.

0801 CS171677 Shikhar Mahajan Shirthan (2)

Testing your fixewall should include both vulnerability scaming and penetration testing.

## Short note on HPING

It is an open-source packet generalor and analyses for the TeP/IP protocol created by Antidez. It is one of the common tooks used for security and networks and was used to exploit the idle scanning technique invented by hping author and Now implemented in smap sewity scanning

The new version of uping is uping -3, is scriptable using the Tel language and implements an Ingine for string base, humansucadable description of TCP/IP packets
Sothat programmer can write scripts
related to low level TCP/IP packet
manipulation and analysis in a short

sold 1st block to the seports prophold

080165171077 Shikhan Mahajan

Shikhan

3/4/21

0910

AND SNORT :- It is a network bused intrusion detection system uniten in c longuage. It was developed in 1338 by martin Roesch. Now developed by CISCO. It is fall open source software It can also be used as packet sniffer to monitor the system in real time. The network admin can use it to watch all the incoming packets. It is based on library packet capture tool The rives are fairly easy to create and implement and it can be deployed in any kind of OS. and any kind of Network environment.

## features:

- Real time traffic monitor
- Packet logging Open source
- os fingerprinting
- Analysis of protocol
- Creates logs
- Content matching. Installed in any network environment

Shikhar Mahajan Blikhar (14) 9/4/21 Installation steps: -1 In Linux: Step-1: wget https:// www.snost.org/downlon /snort/snort -2.9.15.for.g2 step 2: two xuzt snort - 2.3.15-two.gz Step 3: Cel snort - 2.9.15 step-4: / configure - enable-source fixe ll make le sudo make install (2) In Windows. Step-1: Pownload SNORT installer From https://www.snort.org/downloads snort/snort\_29\_15\_Installer.ex Step-2: Execute the snort 2 9 15

Installer exe.

0801CS191077 Shikhou mahajan Shikhan (5)

use Database security Assessment Tool (DBSAT)

The database security Assessment tool is provided by oracle as a utility to help you chack for common database security issues as well as helping to identify sensitive data stoold in the database.

- · DBSAT analyses information on the database and the listner configuration is to identify configuration settings that may unnecessarily introduce exist.
- · DBSAT goes beyond simple configuration checking, examining user accounts, authorization control, Aire grained access and os file permissions.

  OBSAT applies rules to quickly assess
- to the arroant security status of a do DESAT recommends redemption activities
- that follow best practices to reduce or mitigate siste.

0801CS171077 Shiphon (16) Shikhan Mahajan # To Install Oracle DBSAT tool. · Extract degat zip on the target serum D'occate a disectory, where you will extract about file. mkdir -p /home/oracle/dbox @ Bxtxact DBSAT file in the disector unzip dbsat zip -d/home/oracle/ 3) Navigate to the disectory cd/ nome/ oracle/dbsat.

0801 CS 171078 Shikhar Mahajan Shilahar 9/4/21

Question - 5

(a) largest prime factor

(b) 100 = 5 [
$$2^2 \times 5^2$$
]

(c) 1,000 = 5 [ $2^3 \times 5^3$ ]

(d) 1,00,000 = 5 [ $2^6 \times 5^6$ ]

(e) 1,00,000 = 5 [ $2^6 \times 5^6$ ]

(f) 101 = prime itself

(g) 1,001 = 13 [ $7 \times 11 \times 13$ ]

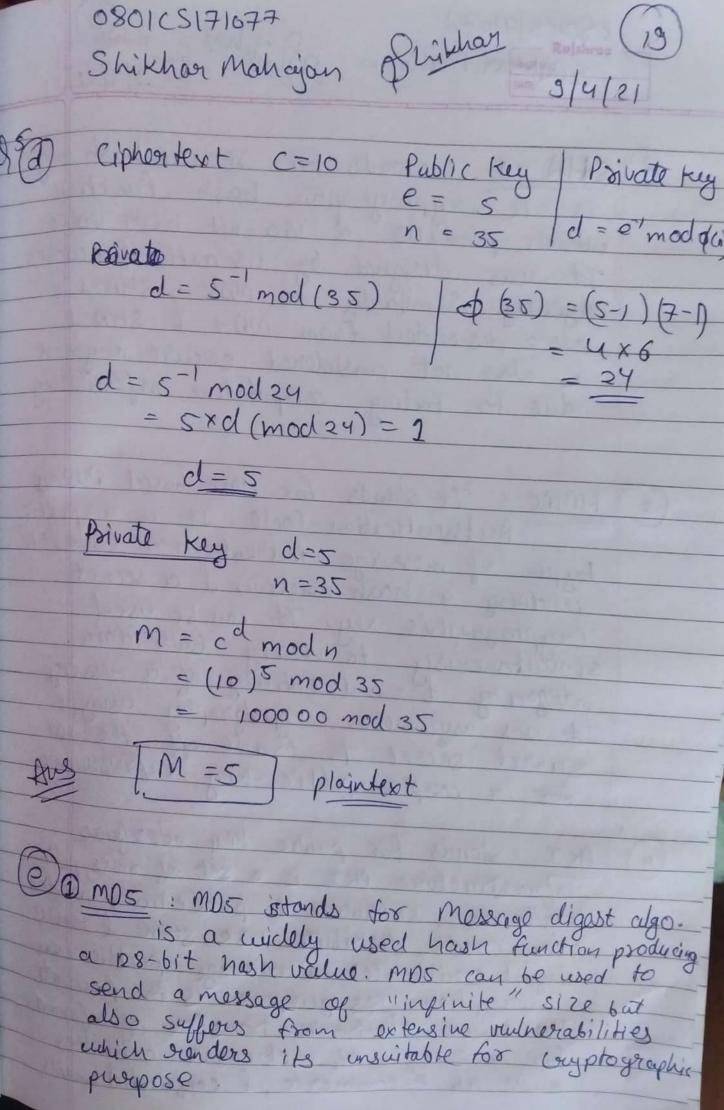
(g) 1,000 = 3051 [ $11 \times 3051$ ]

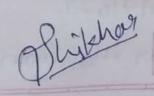
(10) 10,00,001 = 3201 [ $101 \times 350$ ]

(a) 
$$\phi(29) = 29 - 1 = 28$$
 [as 29 is prime  
(a)  $\phi(32) = \phi(2^5) = 2^5 - 2^7$  [as 32 is  $= 16$  [direct power of prime  
(3)  $\phi(80) = \phi(2^9 \times 5) = \phi(2^9) \times \phi(5)$ 

(3) 
$$\phi(80) = \phi(2^{4}xs) = \phi(2^{4}) \times \phi(s)$$
  
=  $(2^{4}-2^{3}) \times (s-1)$ 

Shildran Mahajan Shildran 9/4/21 (4) @ (100) = \$ (22x52) = \$ (22) X \$ (52)  $= (2^2-2^1) \times (5^2-5^1)$ = 2 x 20 = 40 (5) \$ (101) = 101-1 fas 101 1/2 px/mg 05 P = 13 Crinen, Ali'co = 79 mod 13 = 8 = N Bob = 73 mod 13 = 5=9 Private key > g a mod 13 = 83 mod 13





Ra (20) 9/4/21

2) SAIA -1: stands for secure hash algorism a cryptographic hash function which produces a 160-bit hash value. It was designed by us national security Agency. Similarly to MOS, SHA-1 is also descended from MD4 & SHA-1 is also not considered secure anymose due to failing computation infeasibility

HMAC: It stands for Hash based Message

Authentication Cocle. It is a specific
type of message Authentication Code (MA) involving a hoish function of a secret Cryptographic Key. It can be used integerity & authenticity of a message It uses asymmetric exprospraphy using a snared secret to trade off the need for a complex public-key infrastructure.

PKI : Stands for public key indexpass. infrastructure PKI is a set of roles, pollula hardware, software & procedures needed to create, distribute, use, store & revolve digital contificates & manage public long energyption. Its purpose is to fasciliate the secure electronic transfer of information for a range of network activities such as e-commerce, & confidential email.