Shikhar Mahajan

0801CS171077

Shikhar

09/04/21

INS - Assignment - 02

Q1

(a) Galois field is valid if in $G(x)$

→ x is of the form p^n

where, p is a prime number

n is a whole number.

i.e., x should be power of some prime number

(1) $GF(12) = GF(3 \times 2^2) =$ In-Valid

(2) $GF(13) = GF(13^1) =$ Valid

(3) $GF(16) = GF(2^4) =$ Valid

(4) $GF(17) = GF(17^1) =$ Valid

(5) $GF(19) = GF(19^1) =$ valid.

(b)

(1) $10 \Rightarrow 1x^1 + 0 \cdot x^0 = \boxed{x}$

(2) $100001 \Rightarrow 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$

$= \boxed{x^5 + 1}$

(3) $10010 \Rightarrow 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0$

$= \boxed{x^4 + x^1} = x(x^3 + 1)$

(4) $00011 \Rightarrow 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$

$= \boxed{x + 1}$

(5) $1001101 \Rightarrow 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$

$= \boxed{x^6 + x^3 + x^2 + 1}$

0801CS171077

Shikhar Mahajan Shikhar

DATE 9/4/21

Q2

(a)

(i) $(01001101) \oplus (01001101) = \underline{\underline{00000000}}$

(ii) $(01001101) \oplus (10110010) = \underline{\underline{11111111}}$

(iii) $(01001101) \oplus (00000000) = \underline{\underline{01001101}}$

(iv) $(01001101) \oplus (11111111) = \underline{\underline{10110010}}$

(b)

Enrollment No. = 0801CS171077

last five = n = 71077

Number of bits = 71077 * 8
(assuming 8 bit char) = $\underline{568616}$

$\Rightarrow$ size of padding $= 64 - (568616 \% 64)$
$= 64 - 40$
$= \underline{\underline{24}}$

No. of blocks $= (568616 + \text{padding}) / 64$

$= (568616 + 24) / 64$

0801CS171077

Shikhar Mahajan Shikhar

9/4/21

Ans ⇒ $\boxed{8885 \text{ bits}}$

(c)

(i) In decoding, the position of digit '1' is the value of integer

∴ In, 010 = $(2)_{10}$ (⇒ position of 1)

for 3x8, length = $2^n = 2^3 = \underline{\underline{8}}$

Ans So, (010) $\xrightarrow[\text{Decoder}]{3\times 8}$ $\underline{\underline{00000100}}$

(ii) for encoding, position of 1 is encoded to decimal, then to binary

∴ In, 00100000 = $(5)_{10}$

converting $(5)_{10}$ to decimal

= (101)

Ans ∴ 00100000 $\xrightarrow[8\times 3]{\text{Encoder}}$ $\underline{\underline{101}}$

0801CS171077
Shikhar Mahajan   Shikhar

4
DATE 9/4/21

Q3

(a)

(i) input = 110111

for row = 1st & last bit = 11 $= (3)_{10}$
for column = 1011 $= (11)_{10}$

$\boxed{\text{S-3 box}}$ ⇒ row $= (3)_{10}$
column $= (11)_{10}$

value ⇒ $\boxed{3}$ (from table)

Ans ⇒ $\boxed{0011}$

(ii) input = 001100

row $= (00)_2 = (0)_{10}$
column $= (0110)_2 = (6)_{10}$

S-4 box ⇒ $\boxed{9}$ (from table)

Ans = $\boxed{1001}$

0801CS171077

Shikhar Mahajan Shikhar

9/4/21

(iii) input = 000000

row = $(00)_2 = (0)_{10}$

column = $(0000)_2 = (0)_{10}$

S-7 box ⇒ value = 4 (from table)

Ans = $\boxed{0100}$

(iv) input = 111111

row = $(11)_2 = (3)_{10}$

column = $(1111)_2 = (15)_{10}$

S-2 box ⇒ value = 9 (from table)

Ans = $\boxed{1001}$

(6)

	row	column	value	binary value
S0	0	0	14	1101
S1	0	0	15	1111
S2	0	0	10	1010
S3	0	0	7	0111
S4	0	0	2	0010
S5	0	0	12	1100
S6	0	0	4	0100
S7	0	0	13	1101

$\boxed{\text{input} = 000000}$

0801CS171077
Shikhar Mahajan   Shikhar

9/4/21

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

(c) key with parity bit
0123 ABCD 2562 1456

Drop every 8th bit

0123 = 0000 000~~1~~ 0010 001~~1~~
ABCD = 1010 101~~1~~ 1100 110~~1~~
2562 = 0010 010~~1~~ 0110 001~~0~~
1456 = 0001 010~~0~~ 0101 011~~0~~

Key without parity 0000000 0010001
1010101 1100110 0010010 0110001
0001010 0101011

Permutate a/c to parity bit drop table

DC1 = C0 0000110 0101010 0000110 1101100
D0 1010011 0110110 0000001 1000000

Shift left on both halves.

C1 = 0001100 1010100 0001101 1011000
D1 = 0100110 1101100 0000011 0000001

Now. Permute by key Generate table

Ans

$\boxed{\text{Key} = 1437\ 4013\ 3784}$

0801CS171077

Shikhar Mahajan Shikhar

9/4/21

Q4

(a) There are 3 Categories to NIST for AES evaluation:-

(1) Algorithm :- Algorithm and Implementation characteristics include flexibility, hardware and software suitability and addition features offered by a candidate algorithm.

(2) Cost :- Cost includes lisensing of requirements computational efficiency and memory requirements.

(3) Security :- Security is the paramount consideration in AES selection process and encompasses issues like the relative security of 1 candidate compared to other, and the extinct to which algorithm output is indistinguishable from random permutation.

(b) Lightweight cryptography is a method that features a small footprint and low computational complexity. It is aimed at expanding the applications to constrained devices and its related binding international standardisation and guidelines compilations are currently underway

Requirement in 21st Century

In the era of technology advancement all kinds of devices from powerful super computers and servers with high computating device are being connected via internet. with these advancement it brings to the failure of conventional cryptographic methods for the sake of security. and performance requirement especially in resources constrained devices.

Therefore, the cryptographic 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 lightweight cryptography in the current 21st Century

0801CS171077
Shikhar Mahajan Shikhar (9)

9/4/21

Q9

Ans⇒ for configuring firewall, there are 5 steps:-

Step 1 Secure your firewall

If an attacker is able to gain administrative access to your firewall it is 'game over' for your network. Therefore, securing your firewall is the first and important step of this process.

Update your firewall to the latest firmware

1. Delete, disable or rename user accounts and change all default passwords.
2. for multiple administration, create addition administration accounts with limited privilages.
3. Disable SNMP or configure it to use a secure community string

Step-2 Architect your firewall zones and IP addresses

In order to protect valuable assets of

your network, you should first identify what the assets are. Then plan out your network structure so that these assets can be grouped together and placed into networks based on similar sensitivity level and function

Step 3: Configure access control lists

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

The traffic will be permitted using firewall rules called access control lists (ACL) which are applied to each interface & sub-interface on the firewall.
Make ACL's specific to exact source and destination IP addresses and port numbers and make sure there is "deny all" rule to filter out all unapproved traffic

Apply both inbound and outbound ACL's to each interface on firewall so that only approved traffic is allowed into and out of each zone.

Step-4 Configure your other firewall services and logging.

If your firewall is also capable of acting as a dynamic hosts configuration protocol (DHCP) server, network time protocol (NTP) server etc. then go ahead and configure the services and disable all the extra services.

To fulfill PCI DSS requirements configure your firewall to report your logging server and make sure that enough detail is include to satify requirement 10.2

Step-5 Test your firewall configuration

In a test environment, verify that your firewall works as intended. Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations.

0801CS171077
Shikhar Mahajan Shikhar. (12)
9/4/21

Testing your firewall should includ both vulnerability scanning and penetration testing.

Short note on HPING

It is an open-source packet generator and analyser for the TCP/IP protocol created by Antirez. It is one of the common tools used for security auditing and testing of firewalls. and networks and was used to exploit the idle scanning technique invented by hping author. and Now implemented in nmap security scann

The new version of hping is hping-3, is scriptable using the TCl language and implements an engine for string base, human-readable description of TCP/IP packets So that programmer can write scripts related to low level TCP/IP packet manipulation and analysis in a short tree.

0801CS171077

Shikhar Mahajan Shikhar 9/4/21

Q10

Ans) SNORT :- It is a network based intrusion detection system written in C language. It was developed in 1998 by martin Roesch. Now developed by CISCO. It is free 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 rules are fairly easy to create and implement and it can be deployed in any kind of OS. and any kind of Network environment.

Features:

1 Real time traffic monitor
2. Packet logging
3. Open source
4. OS fingerprinting
5. Analysis of protocol
6. Creates logs.
7. Content matching.
8. Installed in any network environment.

0801CS171077
Shikhar Mahajan Shikhar

9/4/21

Installation steps :-

① In Linux:

Step-1: wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz

Step 2: tar xvzf snort-2.9.15.tar.gz

Step 3: cd snort-2.9.15

Step-4: ./configure -enable-sourcefire && make && sudo make install

② In Windows.

Step-1: Download SNORT installer from https://www.snort.org/downloads/snort/snort_2_9_15_Installer.exe

Step-2: Execute the snort_2_9_15_Installer.exe.

0801CS171077
Shikhar Mahajan

Shikhar

9/4/21

Q11

Ans=> ## Database security Assessment Tool (DBSAT)

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

- DBSAT analyses information on the database and the listner configuration is to identify configuration settings that may unneccesarily introduce risk.
- DBSAT goes beyond simple configuration checking, examining user accounts, authorization control, fine grained access control, key management, auditing policies and OS file permissions.
- DBSAT applies rules to quickly assess to the current security status of a db. and produce finding in all the areas.
- DBSAT recommends redemption activities that follow best practices to reduce or mitigate risk.

0801CS171077
Shikhar Mahajan

Shikhar.

09/4/21

To install Oracle DBSAT tool.

- Extract dbsat.zip on the target server

(1) Create a directory, where you will extract dbsat file.

```
mkdir -p /home/oracle/dbsat
```

(2) Extract DBSAT file in the directory

```
unzip dbsat.zip -d /home/oracle/dbsat.
```

(3) Navigate to the directory

```
cd /home/oracle/dbsat.
```

0801CS171077

Shikhar Mahajan Shikhar Rajshree PAGE NO DATE 9/4/21

Question - 5

(a) largest prime factor

(1) 100 = 5 $[2^2 \times 5^2]$

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

(3) 10,000 = 5 $[2^4 \times 5^4]$

(4) 1,00,000 = 5 $[2^5 \times 5^5]$

(5) 10,00,000 = 5 $[2^6 \times 5^6]$

(6) 101 = prime itself

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

(8) 10,001 = 137 $[73 \times 137)$

(9) 1,00,001 = 9091 $\{11 \times 9091\}$

(10) 10,00,001 = 9901 $[101 \times 9901]$

(b) (1) $\phi(29) = 29 - 1 = \underline{\underline{28}}$ [as 29 is prime

(2) $\phi(32) = \phi(2^5) = 2^5 - 2^4 = \underline{\underline{16}}$ [as 32 is direct power of prime

(3) $\phi(80) = \phi(2^4 \times 5) = \phi(2^4) \times \phi(5)$

$= (2^4 - 2^3) \times (5-1)$

$= 8 \times 4 = \underline{\underline{32}}$

0801CS171077

Shikhar Mahajan Shikhar

9/4/21

(4) $\phi(100) = \phi(2^2 \times 5^2)$

$= \phi(2^2) \times \phi(5^2)$

$= (2^2 - 2^1) \times (5^2 - 5^1)$

$= 2 \times 20 = \underline{\underline{40}}$

(5) $\phi(101) = 101 - 1$ [as 101 is prime

$= 100$

Q5

(c) Given, $P = 13$

$G = 7$

Alice $= 7^9 \bmod 13 = \underline{\underline{8 = x}}$

$\boxed{b=3}$ $\therefore$ $\underline{\underline{a = 9}}$

Bob $= 7^3 \bmod 13 = \underline{\underline{5 = y}}$

Private key $\Rightarrow y^9 \bmod 13$

$= 5^9 \bmod 13$

$= \boxed{5}$

$\Rightarrow x^b \bmod 13$

$= 8^3 \bmod 13$

$= \boxed{5}$

$\underline{\underline{\text{Ans} = 5}}$

0801CS171077

Shikhar Mahajan Shikhar

9/4/21

Q5 (d) Ciphertext $C=10$

Public key	Private key
$e = 5$	
$n = 35$	$d = e^{-1} \bmod \phi(n)$

~~Private~~

$d = 5^{-1} \bmod (35)$

$\phi(35) = (5-1)(7-1)$
$= 4 \times 6$
$= \underline{\underline{24}}$

$d = 5^{-1} \bmod 24$
$= 5 \times d \pmod{24} = 1$

$\underline{\underline{d = 5}}$

Private key $d=5$
$n=35$

$m = c^d \bmod n$
$= (10)^5 \bmod 35$
$= 100000 \bmod 35$

Ans $\boxed{M = 5}$ plaintext

(e) ① MD5 : MD5 stands for Message digest algo. is a widely used hash function producing a 128-bit hash value. MD5 can be used to send a message of "infinite" size but also suffers from extensive vulnerabilities which renders its unsuitable for cryptographic purpose.

0801CS171077
Shikhar Mahajan
Shikhar

(2) SHA - 1 : stands for secure hash algo. is a cryptographic hash function which produces a 160-bit hash value. It was designed by US national security Agency. Similarly to MD5, SHA-1 is also descended from MD4 & SHA-1 is also not considered secure anymore due to failing computation infeasibility

(3) HMAC : It stands for Hash based Message Authentication Code. It is a specific type of message Authentication Code (MAC) involving a hash function & a secret cryptographic key. It can be used simultaneously to verify both data integrity & authenticity of a message. It uses asymmetric crypotography using a shared secret to trade off the need for a complex public-key infrastructure.

(4) PKI : stands for public key ~~interface~~ infrastructure. PKI is a set of roles, policies hardware, software & procedures needed to create, distribute, use, store & revoke digital certificates & manage public key encryption. Its purpose is to fasciliate the secure electronic transfer of information for a range of network activities such as e-commerce, & confidential email.