Reg.No. | | | | | | |

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination: ESE

Year: BTech **Branch:** Computer Engineering

Subject: Networks Security **Subject Code: CS4017**

Max. Marks: 100 **Total Pages of Question Paper:** 2

Day & Date: Wednesday 12/12/2018 **Time: 2.30 PM To 5.30 PM**

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

Q1a Suppose that you are using facebook and you got Priyanka Chopra's photo asking to click on it to get dinner with her. Now you have clicked on it and you lost all your valuable data. What type of attack it is and how this work? **9**

OR

Q1b Suppose you had inserted a html code on web server without any permissions and approvals. When this code is executed on client machine if fetched the pages by client then it performs attack on client. Which type of attack it is? How this will happen? Justify with example **9**

Q1c For the given key K= 0010010111, if the generated keys are K1=0010 1111, and K2=1110 1010, what is the cipher text of plaintext P=10110110. Given that P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxes are **5**

$$S0 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix} \text{ and } S1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

Q1d Evaluate the modular multiplicative inverse of 550 mod 1769? **4**

Q2a Convert the given plain text =1000 0111 0010 1000 into Ciphertext, if the key is 0101 1010 1011 0101. The mix column matrix $M_e = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$ and S-Box is **8**

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

OR

Q2b Let P(3,10) and Q(9,7) in $E_{23}(1,1)$ then find the third point R=P+Q on the curve **8**

Q2c Users A and B use the Diffie Hellman key exchange technique with a common prime 71 and a primitive root 7.if Private keys are X_A=5 and X_B = 12 then what is shared secret? **5**

Q2d Perform the encryption using RSA algorithm for p=11, q=13, e=11 and M=7 **3**

Q3a How various attacks are happened in preliminary versions of Needham Schroeder protocol and by what process these are resolved? What is the final solution for these attacks which will avoid all attacks. 8

OR

Q3b Illustrate in detail the working of the SHA-512 algorithm with the help of neat diagrams. 8

Q3c Suppose your data is stored in a dictionary and hacker will perform a attack on this data. How this dictionary attack will be performed by hacker and how you defeat this dictionary attack? 5

Q3d What is Discretionary Access Control? How it is functioning in the Windows system? 3

Q4a The IPSec protocol uses its two protocol mode to provide security. In each mode security associations are created. Illustrate these two modes security association for IPV4 and IPV6. 8

OR

Q4b Give the design architecture of SSL protocol stack and justify its use for security using various protocols used in it. 8

Q4c Consider that you are communicating to your friend and sharing some audio/video contents over email. You want to secure your audio/video data at the time of transfer. Which protocol you will recommend for the security. Elaborate the same in detail. 5

Q4d If we want to use web service using port number 80 and need of security for any transaction over this communication. What protocol we have to use? How this protocol works? 3

Q5a Define the following terms: Cyber attack, Cyber warfare, Cyber terrorism. State three factors which contribute to the reason why cyber attacks are launched against a group of people. State the difference between a professional hacker and a cyberterrorist. 8

OR

Q5b What are the different investigation stages in digital forensic? Give details at each stage.
Compare digital forensic with cyber forensic and give details about how cyber forensic differs with digital forensic? 8

Q5c What is facebook forensic? Give detail description of the facebook protocol format. 5

Q5d Give details of Mobile forensic in terms of Data Obtainable, Network Call Data Records, Cell Site Analysis. 3

Q6a A protocol is used at network layer to provide a security which is having functionality of authentication, confidentiality, and key management. Give the design of this protocols architecture with detail description and specify security association created with its parameters. 9

Q6b What is asymmetric key based authentication? What are the flaws in the protocol? How these are overcome using the corrected protocol? 5

Q6c What is SSL handshake protocol? Give its working in detail with neat diagram. 4

A

Reg.No.

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination: ESE

Year: BTech Final	**Branch:** Computer Engineering
Subject: Network Security	**Subject Code: CS4017**
Max. Marks: 100	**Total Pages of Question Paper:**
Day & Date: ~~Monday 29/04/19~~ 10/05/19	**Time: 10.00 AM To 1.00 PM**

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

Q. 1. **Attempt the following**

A
```
#pragma check_stack(off)
#include <string.h>
#include <stdio.h>
#include <stdio.h>
#include <string.h>

void doit(void)
{
    char buf[8];

    gets(buf);
    printf("%s\n", buf);
}

int main(void)
{
    printf("So... The End...\n");
    doit();
    printf("or... maybe not?\n");

    return 0;
}
```
9

Specify the attack possible on the given code? How that attack is performed. Describe in detail.

B Describe IP spoofing by specifying how one hacker can do this spoofing with neat diagram. 8

OR

C What is session hijacking? How it will be performed? Session hijacking leads to which attack. 8

Q. 2. A Using extended Euclidean algorithm, find the multiplicative inverse of 1234 mod 4321. 7

B For the given plaintext P =0100 0001 calculate the cipher text, if the key used is K=1010000010, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxex are 10

$$S0 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix} \text{ and } S1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

OR

C Convert the given Ciphertext= 0010 0100 1110 1100 into Plaintext, if the key is 0100 1010 1111 0101. The inverse of mix column matrix $M_c = \begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix}$ and S-Box is 10

1010	0101	1001	1011
0001	0111	1000	1111
0110	0000	0010	0011
1100	0100	1101	1110

Q. 3. A Perform the encryption using RSA algorithm for the p=11, q=13,e=11,M=7 9

B For an elliptic curve $E_{11}(1,6)$, consider the point G=(2,7). Compute 5G. 9

OR

C User A and B use the Diffie Hellman key exchange technique with a common prime p=71 and a primitive root a=7. If user A and B has Public key X_A=5 and X_B=12 respectively then find their shared secret key and public key of A and B. 9

Q. 4. A Illustrate the Needham-Schroeder Protocol with neat diagrams. 8

B Is the password based authentication is one-way or mutual? Describe how it works in detail. 8

OR

C Correlate the system in which one centralized trusted third party is divided into two parts. And specify it in detail with AS and TGS. 8

Q. 5. A Evaluate IPSec authentication header with its transport mode and tunnel mode with neat diagrams for the use of security. 8

B How a secure hash value is created using SHA algorithm? 8

OR

C Create a procedure to transfer the data using SSL with specification of headers. 8

Q. 6. **Attempt the following**

A What are the different investigation stages in digital forensic? Give details at each stage. 8
Compare digital forensic with cyber forensic and give details about how cyber forensic differs with digital forensic?

OR

B Define the following terms: Cyber attack, Cyber warfare, Cyber terrorism. State 8
three factors which contribute to the reason why cyber attacks are launched against a group of people. State the difference between a professional hacker and a cyber terrorist.

C What is facebook forensic? Give detail description of the facebook protocol format. 5

D Give details of Mobile forensic in terms of Data Obtainable, Network Call Data Records, Cell Site Analysis. 3

Vishwakarma Institute of Technology Issue 01 : Rev No. 0 : Dt. 16/03/16

Title : Question Paper FF No. 868

Reg.No. | | | | | | | |

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination : ESE

Year: B.Tech Final	**Branch :** Computer Engineering
Subject : Network Security	**Subject Code :CS402THL**
Max. Marks :100	**Total Pages of Question Paper :2**
Day & Date : Monday, 10th Dec 2018	**Time :** 2.30 pm to 5.30pm

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

			Marks
Q 1		**Attempt the Following**	
	A	Cross site scripting is the attack on web server or client? Describe it properly.	8
		OR	
	B	What is ARP spoofing? How it leads to synchronize the communication with third party.	8
	C	What is Phishing? How to avoid phishing?	8
	D	How DoS attack works?	4
Q2		**Attempt the Following**	
	A	For the given plain text P=00110110 calculate the Cipher text, if the key used is K=0010010111, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxex are $S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix}$ and $S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}$	9
		OR	
	B	Convert the given plaintext=1101 0101 1010 1100 into cipher text, if the key is 0100 1010 1111 0101. The mix column matrix $M_e=\begin{bmatrix}1&4\\4&1\end{bmatrix}$ and S-Box is 1001 0100 1010 1011 1101 0001 1000 0101 0110 0010 0000 0011 1100 1110 1111 0111	9
	C	What is the modular multiplicative inverse of 550 mod 1769	4
	D	What is group, ring, and fields	3
Q3		**Attempt the Following**	
	A	For E_{11} (1,6), consider the point G(2,7). Compute the multiples of G as 2G, 3G and 4G.	8
		OR	
	B	Consider a point Q= (1, 12) and P=(7, 3) ∈ E_{23}(1, 4) and try to	8

determine k such that kP = Q. where k is the solution to the discrete logarithm problem.

C If a Diffie-Hellman key exchange is based on prime number 353 and its primitive root is 3. And the two users **A & B** using this prime number for key exchange is having secret keys 97 and 233 respectively. What is the common secret key of A and B. 4

D Perform the encryption using RSA algorithm for p=7, q=11, e=17, if M=9. 4

Q4 **Attempt the Following**

A How Kerberos are used for authentication? 8

B How Needham Schroeder Protocol was evolved to be more secure authentication protocol 8

C Design a role based access control system for the education Institute. 4

D What is shared secrete based authentication? How to avoid parallel session attack in it? 4

Q5 **Attempt the Following**

A How Authentication Header provides support for data integrity and authentication of IP packets? Support your answer with the IPSec AH with the help of transport and tunnel mode. 8

OR

B How ESP provides confidentiality to IP packet? Is ESP better than AH? Justify your answer. 8

C How to secure MIME? What functions MIME provides? 4

D What are the various operations performed by SSL record protocol? How to prepend header in SSL record protocol? 4

Q6 **Attempt the Following**

A What are the principles of cyber forensics? How the process of cyber forensic investigation works? 8

OR

B Illustrate the phases of digital forensic and give details about how a crime is detected? 8

C Is mobile forensic different than computer forensic? How? 4

D What is facebook protocol format? How it helps in the facebook forensic? 4

Title : Question Paper FF No. 868

Reg.No.							

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination : MSE

Year: B.Tech Final **Branch :** Computer Engineering

Subject : Network Security **Subject Code :**CS402THL

Max. Marks :100 **Total Pages of Question Paper :**2

Day & Date : 6/10/17 **Time :** 10.00 am

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

			Marks
Q 1		**Attempt the any three of the Following**	
	A	What is DoS attack? How does this attack happen on any machine? Describe your answer with neat diagrams.	6
	B	What is ransomware attack? Describe it in detail.	6
	C	What are the different vulnerabilities? How will they be resolved?	6
	D	What is phishing? How one can avoid phishing?	6
Q2		**Attempt the two of the Following**	
	A	What is ARP spoofing? How does it lead to synchronization of communication with the third party?	8
	B	What is buffer overflow attack? How to avoid it?	8
	C	Cross site scripting is the attack on web server or client? Describe it in detail.	8
Q3		**Attempt the any three of the Following**	
	A	What is the modular multiplicative inverse of 550 mod 1769?	6
	B	Describe groups, rings, Fields with their properties.	6
	C	State the Chinese Remainder theorem. Formulate a suitable problem and solve it using the Chinese Remainder theorem.	6
	D	What is block cipher? Describe various methods of block cipher and give example of one.	6
Q4		**Attempt the Following**	
	A	For the given plain text P=00110110 calculate the Cipher text, if the key used is K=0010010111, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxes are $S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix}$ and $S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}$ 0101 1010	8
	B	Convert the given cipher text =1101 0111 0010 1000 into plaintext, if the key is 0100 1010 1111 0101. The mix column matrix $M_e=\begin{bmatrix}9&2\\2&9\end{bmatrix}$ and S-Box is 0000 1000 0111 1101	8

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

the decryption S-box is

1010	0101	1001	1011
0001	0111	1000	1111
0110	0000	0010	0011
1100	0100	1101	1110

or

C Convert the given plaintext=1101 0111 0010 1000 into cipher text, if the key is 0100 1010 1111 0101. The mix column matrix $M_e = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$ and S-Box is 8

00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

0010 0100 1110 1100

Q5 **Attempt the two of the Following**

A Depict how the Elliptic curve is implemented over the set of real numbers. Illustrate how the Elliptic curve is implemented over the set of prime numbers. 8

B In RSA given p=19, q=23 and e=3, find n, Φ(n), and d. 8

C Outline the rules of addition over an elliptic curve. For E_{11} (1,6) consider the point G = (2,7). Compute the value of 2G and 3G. 8

Q6 **Attempt the two of the Following**

A In a public key system using RSA, you intercept the cipher text C=10 sent to a user whose public key is e=5, n=35. What is the plain text M? 8

d=5 M=5

B User A and B use the Diffie-Hellman key exchange technique with a common prime p=71 and primitive root a=7. 8

a. If user A has private key Xa=5, what is A's public key Ya?

b. What is shared secret key K?

C Let P(3,10) and Q(9,7) be the points on the elliptic curve $E_{23}(1,1)$. There exists third point R=P+Q on the curve. What are the co-ordinates of R? 8

Title : Question Paper **FF No. 868**

Reg.No.							

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination : Summer Term

Year: B.Tech Final **Branch :** Computer Engineering

Subject : Network Security **Subject Code :CS402THL**

Max. Marks :100 **Total Pages of Question Paper :2+1**

Day & Date : Tuesday, 5th July 2018 **Time :** 2.30 pm to 5.30pm

---

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

		Marks
Q 1	**Attempt the Following**	
A	Mahesh has MAC address x.y.z.t and Dinesh who is a hacker used this MAC address to communicate with Priya. Can you find out how this hacking has happened? Elaborate with neat diagram.	8
	OR	
B	*#pragma check_stack(off)* *#include <string.h>* *#include <stdio.h>* *void foo(const char* input)* *{* *char buf[10];* *printf("My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");* *strcpy(buf, input);* *printf("%s\n", buf);* *printf("Now the stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");* *}* *void bar(void)* *{* *printf("Augh! I've been hacked!\n");* *}* *int main(int argc, char* argv[])* *{* *printf("Address of foo = %p\n", foo);* *printf("Address of bar = %p\n", bar);* *if (argc != 2)* *{* *printf("Please supply a string as an argument!\n");* *return -1;* *}* *foo(argv[1]);* *return 0;* *}* What kind of attack is possible on the given code? How that attack is performed? Illustrate in detail.	8
C	How to defend SQL injection attack? Justify your answer by giving example of SQL injection and defending that.	4
D	Design a block chain for Crypto currency.	4

E What is ransomware attack? Describe it in detail. 4

Q2 **Attempt the Following**

A For the given plain text P=10110110 calculate the Cipher text, if the key used is K=0010010111, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxes are 8

$$S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix} \text{ and } S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}$$

OR

B Convert the given plain text =1000 0111 0010 1000 into Ciphertext, if the key is 0101 1010 1011 0101. The mix column matrix $M_e=\begin{bmatrix}1&4\\4&1\end{bmatrix}$ and S-Box is 8

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

C How the algebraic structure of Groups, Rings, and Fields used in the security? Give the properties of each by specifying the relation between them. 4

D What is the modular multiplicative inverse of 1234 mod 4321? 4

Q3 **Attempt the Following**

A What is Needham-Schroeder protocol? How the problems of each version are resolved in next of Needham-Schroeder protocol? 8

OR

B Consider that you are a client and communicate with a server. This server allows you to communicate if you are authenticated by the authentication server and grants a ticket for communication with server. Now justify how this authentication works. Also mention the protocol which is secure for this communication. 8

C Justify use of SHA-512 for the security of any one system. 4

D In an educational system when access rights are given then what are the mandatory access controls. 4

Q4 **Attempt the Following**

A For E_{11} (1,7), consider the point R (2,5). Compute the multiples of G as 2G,4G, 6G. 8

OR

B Consider a elliptic curve $y^2=x^3+4$; and a point on the curve G(2,2). If n_A=121 what is A's public key? 8

C Perform the encryption using RSA algorithm for p=7, q=11, e=17, if M=21. 4

D Consider a Diffie-Hellman scheme with common prime 11 and primitive root 2. If user A has public key Y_A=9 what is the A's private key? 4

Q5 **Attempt the Following**

A How ESP provides confidentiality to IP packet? How ESP header will help to protect data from third party illegal access. 8

OR

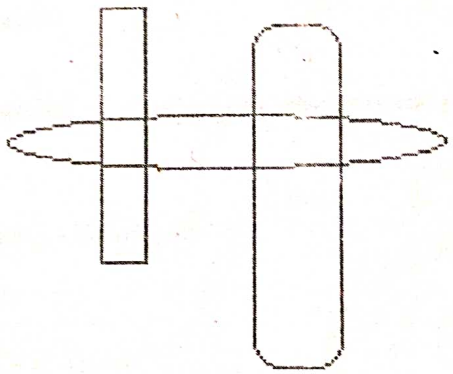
B How Authentication Header provides support for data integrity and authentication of IP packets? Support your answer with the IPSec AH with the help of transport and tunnel mode. 8

C Give the detail architecture of IPSec. 4

D What are the various operations performed by SSL record protocol? How to prepend header in SSL record protocol? 4

Q6 **Attempt the Following**

A	What are the principles of cyber forensics? How the process of cyber forensic investigation works?	8
	OR	
B	What are the methods of data hiding? Which are the methods for detecting/ recovering data? How these methods help to recover the data?	8
C	You are requested to provide security to IoT using MQTT. How this security will be provided?	4
D	What is facebook protocol format? How it helps in the facebook forensic?	4



Title : Question Paper **FF No. 868**

Reg.No.						

Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 411037.
(An Autonomous Institute Affiliated to University of Pune)

Examination : MSE

Year: M.Tech Final **Branch :** CSE[IT]

Subject : Network Security **Subject Code :CS505THP**

Max. Marks :100 **Total Pages of Question Paper :3**

Day & Date : TUE, 13/03/2018 **Time :** 10 am to 1 PM

Instructions to Candidate

1. All questions are compulsory.
2. Neat diagrams must be drawn wherever necessary.
3. Figures to the right indicate full marks.
4. Use of nonprogrammable electronic pocket calculator, mollier charts, steam tables and statistical table are allowed.

Q 1	**Attempt the Following**	Marks
A	How IP spoofing is possible on a machine? Can you perform this spoofing with some example? Elaborate with neat diagram.	8
	OR	
B	Mahesh has MAC address x.y.z.t and Dinesh who is a hacker used this MAC address to communicate with Priya. Can you find out how this hacking has happened? Elaborate with neat diagram.	8
C	How dictionary attack is performed? And how to defend it.	4
D	What is ransomware attack? Describe it in detail.	4
E		4

```
#pragma check_stack(off)
#include <string.h>
#include <stdio.h>
void foo(const char* input)
{
  char buf[10];
  printf("My stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");
  strcpy(buf, input);
  printf("%s\n", buf);
  printf("Now the stack looks like:\n%p\n%p\n%p\n%p\n%p\n%p\n\n");
}
void bar(void)
{
  printf("Augh! I've been hacked!\n");
}
int main(int argc, char* argv[])
{
  printf("Address of foo = %p\n", foo);
  printf("Address of bar = %p\n", bar);
  if (argc != 2)
  {
    printf("Please supply a string as an argument!\n");
    return -1;
    }
foo(argv[1]);
  return 0;
}
```

What kind of attack is possible on the given code? How that attack is performed? Illustrate in detail.

Q2 **Attempt the Following**

A Suppose that you are using facebook and you got Priyanka Chopra's photo asking to click on it to get dinner with her. Now you have clicked on it and you lost all your valuable data. What type of attack it is and how this work? 8

OR

B Suppose you had inserted a html code on web server without any permissions and approvals. When this code is executed on client machine if fetched the pages by client then it performs attack on client. Which type of attack it is? How this will happen? Justify with example 8

C How to defend SQL injection attack? Justify your answer by giving example of SQL injection and defending that. 4

D A company has its database stored on distributed servers and you want to perform denial of service attack. How to defend it? 4

Q3 **Attempt the Following**

A For the given Cipher text C=10110101 calculate the plain text, if the key used is K=0011010111, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxes are 8

$$S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix} \text{ and } S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}$$

OR

B For the given plain text P=10110110 calculate the Cipher text, if the key used is K=0010010111, and P10=3 5 2 7 4 10 1 9 8 6, P8=6 3 7 4 8 5 10 9, IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, and S-Boxes are 8

$$S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix} \text{ and } S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}$$

C If N=30 and n1=3 and n2=5 find f(i) using Chinese remainder theorem. 4

D What is the modular multiplicative inverse of 550 mod 1769? 4

Q4 **Attempt the Following**

A Convert the given cipher text =1001 1001 0010 1001 into plaintext, if the key is 0101 1010 1101 0101. The mix column matrix $M_e=\begin{bmatrix}9&2\\2&9\end{bmatrix}$ and S-Box is 8

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

the decryption S-box is

1010	0101	1001	1011
0001	0111	1000	1111
0110	0000	0010	0011
1100	0100	1101	1110

OR

B Convert the given plain text =1000 0111 0010 1000 into Ciphertext, if the key is 0101 1010 1011 0101. The mix column matrix 8

$M_e = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$ and S-Box is

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

C How the algebraic structure of Groups, Rings, and Fields used in the security? Give the properties of each by specifying the relation between them. 4

D Encrypt the message P=1, 2, 5, 7 if K= 1, 2, 3, 6, 4, 5,1,0 using RC4 method. 4

Q5 **Attempt the Following**

A How Kerberos used for authentication? How tickets are generated? Illustrated with neat diagram 8

OR

B In Needham-Schroeder protocol how KDC will help to authenticate client to the server. How the problems in each version will get resolved by other version and what are these problems? 8

C In Discretionary access control method what are the various access controls. 4

D Justify use of SHA-512 for the security of any one system. 4

Q6 **Attempt the Following**

A How SSL provide security to various communications? Illustrate with its architecture. 8

OR

B How IPSec provide security to upper layer packets using IPV4 and IPV6. 8

C In an educational system when access rights are given then what are the mandatory access controls. 4

D Give details of S/MIME to provide security to audio and video data transfer. 4