MSE

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Computer Science and Engineering)

MID SEMESTER EXAMINATION SEMESTER- I SEPTEMBER-2018

INFORMATION SECURITY (3CS401)

Exam Seat Number: _____

Date and Time: Wednesday, 19/09/2018, 03.00pm to 04.30pm Max Marks: **30**

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) Mobile phones and programmable calculators are strictly prohibited.
iv) Except Exam Seat Number writing anything on question paper is not allowed. Exchange/Sharing of stationery, calculator etc. not allowed.

Number on the right of marks indicates course outcomes (only for faculty use).

			Marks	
Q1	A)	Using Chinese Remainder Theorem(CRT) find the least value of an integer X which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.	5	CO1
Q1	B)	Using additive cipher decrypt the cipher text message "**wtaad**". Show your work.	2	CO2
Q1	C)	Calculate $\varphi(\varphi(77))$?	3	CO1
Q2	A)	a. Encrypt the message "**meet me**" using the Hill cipher with the key 9 4 5 7 Show your calculations and the result.(consider a=0, b=1,…,z=25) b. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.	5	CO1
Q2	B)	DES uses 8 S-boxes, each with a 6 bit input and 4-bit output. Use the following S-Box 1 table to answer the following question:	3	CO1

S-Box 1	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

i) The input to DES S-box 1 is $(100011)_2$. What is the output of this stage? Convert the output to decimal. Show your work.

Q2	C)	Bob chooses RSA modulus n = 91. a. He wants an easily-remembered encryption exponent, so he wants to use either e = 10 or e = 26. However, one of these will not work. Which one won't work and why? b. Since Bob didn't study for his crypto mid-term exam, he couldn't answer part (a). To play it safe, he decided to stick to primes, so he choose e = 17. Find the corresponding decryption exponent "d "and show how you derived it.	5	CO2
Q3	A)	Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α= 2. a. Show that 2 is a primitive root of 11. b. If user A has public key $Y_A = 9$, what is A's private key X_A? c. If user B has public key $Y_B = 3$, what is the secret key K shared with A?	5	CO3

(P.T.O.)

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

MSE

Final Year B.Tech. (Information Technology)

MID SEMESTER EXAMINATION SEMESTER- I SEPTEMBER-2018

CRYPTOGRAPHY AND NETWORK SECURITY (3IT401)

Day, Date and Time: Wednesday, 19/09/2018, 03.00pm to 04.30pm

Exam Seat Number: _____

Max Marks: **30**

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) Mobile phones are strictly prohibited.
iv) Except Exam Seat Number writing anything on question paper is not allowed.
Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).

			Marks	
Q1	A)	Using suitable example, explain design principle of: (Any Two) i) Hill Cipher ii) Playfair Cipher iii) Row Transposition Cipher	6	CO1
Q1	B)	Differentiate active and passive attacks with necessary countermeasures.	3	CO1
Q2		Complete following table comparing Output Feedback and Counter modes of data operation w.r.t. given parameters.	9	CO3

Sr. No.	Parameter ↓ Mode →	OFB	CTR
1	Input Mode (Stream/Block)		
2	Use of synchronized IV (Y/N)		
3	Encryption Parallelizable (Y/N)		
4	Decryption Parallelizable (Y/N)		
5	Random Read Access (Y/N)		
6	Error Propagation (Y/N)		
7	Supports Authentication than Confidentiality (Y/N)		
8	Working Design (In the form of En/Decryption component Figure)		

Q3	A)	For RSA algorithm, if primes p= 13, q=19 are used with encryption parameter e= 7; Calculate following: i) Decryption Parameter d (Forming minimum value valid pair with e) ii) Cipher C1 for plaintext M1=100 iii) Plaintext M2 back from Cipher C2= 120	9	CO2
Q3	B)	Fill in the blanks with appropriate integer values. Design criteria of DES algorithm uses:- i) Total _____ rounds of operation. ii) Individual round applies _____ bit key. iii) Block size = ___bits. iv) Total number of S boxes = _____ v) Input to each S box = _____ bits vi) In 3DES/2, the total key bits used are = _____	3	CO2

WALCHAND COLLEGE OF ENGINEERING

(Government Aided Autonomous Institute)

Vishrambag, Sangli - 416415

Final Year B. TECH. (Computer Science and Engineering)

MSE , ODD SEMESTER, AY 2022-23 | **MSE**

Cryptography and Network Security (5CS401)

PRN: _____

Day, Date and Time: Monday, 10/10/2022, 03.00 pm to 04.30 pm

Max Marks: **30**

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions:
a) All questions are compulsory.
b) Writing question number on answer book is compulsory otherwise answers may not be assessed.
c) Assume suitable data wherever necessary.
d) Figures to the right of question text indicate full marks.
e) Mobile phones and programmable calculators are strictly prohibited.
f) Except PRN anything else writing on question paper is not allowed.
g) Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).

		Marks	
Q1 A)	Use a brute force-attack to decipher the following message enciphered using Caesar Cipher/shift cipher. a. Ciphertext: **Tfuv-sivrbzex zj efk fecp wle, slk rcjf r mvip xffu vovitzjv wfi pfli sirze reu tfxezkzmv jbzccj** (3 Marks) b. Ciphertext: **WKH OHWWHU E** (Hint: Riddle: What makes a road broad?) **(1 mark)** c. Ciphertext: **RHNK TZX** (Hint: Riddle: What goes up but not down?) (1 Mark)	5	CO1
Q1 B)	Construct a table for the Playfair Cipher with the keyword **"EFFECTIVENESS"** and Decrypt the sequence: **"PQFVCKFUFBGMUFYSTIKZKAGWWG"**. Show all the steps required to derive the corresponding plaintext.	4	CO1
Q2 A)	What are the differences between DES and AES Encryption algorithms?	4	CO4
Q2 B)	Briefly describe the three different modes of operations in DES and mention the application of each.	4	CO4
Q3 A)	In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user?	4	CO1
Q3 B)	Consider a Diffie-Hellman scheme with a common prime q=13, and a primitive root α = 7, a. Show that 7 is a primitive root of 13. b. If Alice has a public key Ya=5, what is Alice's Private key Xa? c. If Bob has a public key Yb= 12, what is the secret key K shared with Alice?	6	CO2
Q3 C)	Using Chinese Remainder Theorem (CRT) find an integer X that has a reminder of 3 when divided by 7 and 13, but is divisible by 12.	3	CO1

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Computer Science and Engineering)

MID SEMESTER EXAMINATION SEMESTER- I SEPTEMBER-2019

INFORMATION SECURITY (3CS401)

MSE

Exam Seat Number: _____

Day, Date and Time: Wednesday, 18/09/2019, 03.00pm to 04.30pm

Max Marks: **30**

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) **Mobile phones and programmable calculators are strictly prohibited.**
iv) **Except Exam Seat Number writing anything on question paper is not allowed.**
Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).

			Marks	
Q1	A)	Find the value of $\Phi(237)$ by using Euler's totient function?	2	CO1
Q1	B)	Use Fermat's theorem to find the value of 4^{532} mod 11?	2	CO1
Q1	C)	Using Chinese Remainder Theorem (CRT) find an integer X that has a reminder of 3 when divided by 7 and 13, but is divisible by 12.	4	CO2
Q2	A)	Construct a Playfair matrix with the key **"Hello World"** and Encrypt the message **"hide the gold"**.	3	CO3
Q2	B)	Use the hill cipher with the key $\begin{bmatrix} 3 & 2 \\ 1 & 5 \end{bmatrix}$ to encrypt the message "**MATH**" using A=0, B=1,…Z=25, and working in Mod 36. Then verify the encryption.	4	CO1
Q2	C)	1. What is the Shifted Row transformation for the matrix bellow:(2 Marks)	5	CO2

FE	72	2B	D7
6B	77	A4	6B
AD	01	F0	63
30	D7	AF	FE

2. There is an addition of round key before the start of the AES round algorithms.
a) True b) False
3. In AES conversion of the Plaintext MANIPALINSTITUTE to a state matrix leads to

M	A	N	I
P	A	L	I
N	S	T	I
T	U	T	E

a)

M	P	N	T
A	A	S	U
N	L	T	T
I	I	I	E

b)

M	A	I	L
N	P	I	T
A	N	I	U
S	T	T	E

c)

E	U	T	L
T	I	I	L
T	N	P	A
S	A	N	M

d)

4. How many rounds does the AES-192 perform?
a) 10 b) 12 c) 14 d) 16

3	A)	Consider a Diffie-Hellman scheme with a common prime q=13, and a primitive root α = 7, a. Show that 7 is a primitive root of 13. b. If Alice has a public key Ya=5, what is Alice's Private key Xa? c. If Bob has a public key Yb= 12, what is the secret key K shared with Alice?	5	CO3
	B)	In RSA you intercepted the ciphertext C = 8 sent to a user whose public key e = 13, n=33. What is the plaintext M?	5	CO3

WALCHAND COLLEGE OF ENGINEERING

(Government Aided Autonomous Institute)
Vishrambag, Sangli – 416415

Final Year B.Tech. (Computer Science and Engineering)
ESE , ODD SEMESTER, AY 2022-23
Cryptography and Network Security (5CS401)

ESE

PRN: _____

Day & Date: Tuesday, 13/12/2022 Time: 3.00 pm to 5.00 pm

Max Marks: **50**

IMP: Verify that you have received question papers with correct course code, branch etc.

Instructions
a) All questions are compulsory.
b) Writing question number on answer book is compulsory otherwise answers may not be assessed.
c) Assume suitable data wherever necessary.
d) Figures to the right of question text indicate full marks.
e) Mobile phones, smart gadgets and programmable calculators are strictly prohibited.
f) Except PRN anything else writing on question paper is not allowed.
g) Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (Only for faculty use)

			Marks	
Q1	A)	What is Kerberos? Explain how it provides authentication service.	5	CO3
	B)	Illustrate Secure Hash Algorithm in brief.	5	CO3
	C)	State the value of the padding field in SHA-512 if the length of the message is 1919 bits.	3	CO3
Q2	A)	List the different protocols of SSL. Explain in detail Handshake protocol.	5	CO2
	B)	Discuss authentication header and ESP in detail with their packet format.	6	CO2
	C)	How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.	5	CO2
Q3	A)	Explain the various types of Firewalls with neat diagrams.	5	CO4
	B)	What is Intrusion Detection System? Explain the various types of Intrusion Detection Systems.	5	CO4
Q4	A)	In a public-key system using RSA, you intercept the cipher text C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M?	5	CO1
	B)	Use the brute force attack to decipher the following message: "**UVACLYFZLJBYL**" What is the original plaintext and the encryption key used?	3	CO1
	C)	A box contains gold coins. If the coins are equally divided among six friends, four coins are left over. If the coins are equally divided among five friends, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven friends? (Hint: use Chinese Remainder Theorem).	3	CO1

· · · · · End of question paper · · · · ·

1B094BDD3D2FA4D47187EE21A164254A

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

ESE

Final Year B.Tech. (Computer Science and Engineering)

END SEMESTER EXAMINATION: SEMESTER-I NOVEMBER-2018

INFORMATION SECURITY (3CS401)

Exam Seat Number: _____

Day, Date and Time: Tuesday, 20/11/2018, 10.00am to 12.00Noon

Max Marks: 50

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) Mobile phones and programmable calculators are strictly prohibited.
iv) Except Exam Seat Number writing anything on question paper is not allowed. Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).			Marks	
Q1	A)	Construct a table for the Playfair Cipher with the keyword "**EFFECTIVENESS**"? a. Encrypt the phrase: "EXAMFORINFORMATIONSECURITY" b. Decrypt the sequence: "PQFVCKFUFBGMUFYSTIKZKAGWWG"	7	CO1
Q1	B)	Find the result of the following, using Fermat's little theorem. Show your calculations. 4^{532} Mod 11.	3	CO1
Q1	C)	a. Explain how the cipher-block chaining mode of operation works? -OR- b. List the different protocols of SSL. Explain in detail Handshake protocol.	5	CO3
Q2	A)	Draw the IP security authentication header and explain the functions of each field.	5	CO2
Q2	B)	How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams.	5	CO2
Q2	C)	What is a dual signature and what is its purpose?	3	CO2
Q3	A)	In SHA-512, We apply the Conditional function on E, F, and G buffers. If the leftmost hexadecimal digits of these buffers are 0x9, 0xA, and 0xF respectively, what is the leftmost digit of the result?	3	CO3
Q3	B)	For SHA-512, show the equations for the values of W16, W17 and W79.	3	CO3
Q3	C)	State the value of the padding field in SHA-512 if the length of the message is 1919 bits.	3	CO3
Q3	D)	Explain the concept of digital signature.	3	CO2
Q4	A)	List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway?	5	CO2
Q4	B)	What is intrusion detection system? Explain its types in detail.	5	CO2

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

ESE

Final Year B.Tech. (Computer Science and Engineering)

END SEMESTER EXAMINATION SEM.- I NOVEMBER/DECEMBER - 2019

BE - Comp [CSE]

INFORMATION SECURITY (3CS401)

ESE - 2019

Exam Seat Number: _____

Day, Date and Time: Friday, 29/11/2019, 10.00am to 12.00Noon

Max Marks: **50**

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. Assume suitable data wherever necessary.

ii) Figures to the right of question text indicate full marks.

iii) Mobile phones and programmable calculators are strictly prohibited.

iv) Except Exam Seat Number writing anything on question paper is not allowed. Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).

			Marks	
Q1	A)	Use a brute force attack to decrypt the following riddles encrypted using Caeser Cipher. a. Ciphertext: **WKH OHWWHU E** (Hint: Riddle: What makes a road broad?) b. Ciphertext: **CSYV EKI** (Hint: Riddle: What goes up but not down?)	5	CO1
Q1	B)	Encrypt "**thepepsiisintherefrigerator**" using Vignere Cipher System using the keyword "**HUMOR**".	5	CO1
Q1	C)	a. What is the inverse of confidentiality, integrity, and availability (C.I.A.) triad in risk management? A. misuse, exposure, destruction B. authorization, non-repudiation, integrity C. disclosure, alteration, destruction D. confidentiality, integrity, availability b. Under what circumstance might a certification authority (CA) revoke a certificate? A. The certificate owner has not utilized the certificate for an extended period. B. The certificate owner public key has been compromised. C. The certificate owner' private key has been compromised. D. The certificate owner has upgraded his/her web browser. c. Which of the following virus types changes its characteristics as it spreads? A. Boot sector B. Parasitic C. Stealth D. Polymorphic	3	CO1
Q1	D)	1. Which technique (Cryptography or Steganography) is used in each of the following cases for confidentiality? a. A student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts it in a ball-point pain, and passes the pen to another student. b. To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement. **-OR-** 2. Find the multiplicative inverse of 6 in Z_{10}.	2	CO3

(P.T.O.)

Q2	A)	Bob has a public RSA key (n = 91, e = 5). He sends Alice a message "m" and the digital signature "s" of the message. The message and signature that Alice receives is (m = 35, s = 42). Should Alice accept the message as genuine or not? You must give justification for your answer.	5
Q2	B)	Give a neat sketch to explain the concept of Secured Hash Algorithm (SHA).	5

Q3	A)	What are the services provided by SSL record protocol? Describe the operation of this protocol with suitable illustration.	5
Q3	B)	How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams.	5
Q3	C)	Draw the IP security authentication header and explain the functions of each field.	5

Q4	A)	List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway?	5
Q4	B)	What is intrusion detection system? Explain its types in detail.	5

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Information Technology)

END SEMESTER EXAMINATION SEM.- I NOVEMBER/DECEMBER - 2019

CRYPTOGRAPHY AND NETWORK SECURITY (3IT401)

ESE

BE-IT&CSE.
ESE-2019

Exam Seat Number: _____

Day, Date and Time: Friday, 29/11/2019, 10.00am to 12.00Noon

Max Marks: **50**

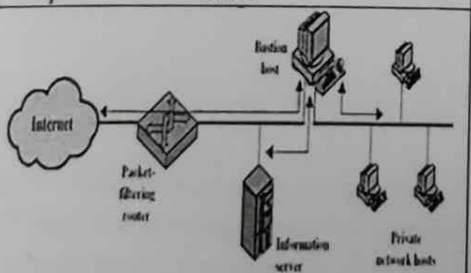
IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) Mobile phones and programmable calculators are strictly prohibited.
iv) Except Exam Seat Number writing anything on question paper is not allowed. Exchange/Sharing of stationery, calculator etc. not allowed.

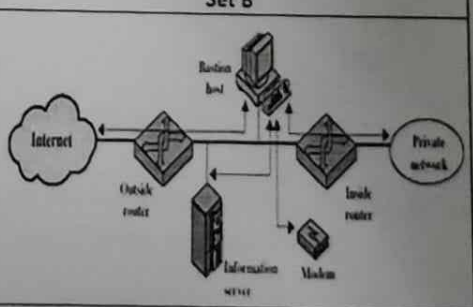
Text on the right of marks indicates course outcomes (only for faculty use).

			Marks	
Q1	A)	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6; i) Find Public key of Alice =YA ii) Find Public key of Bob= YB iii) What is the secret key they exchanged = K?	6	CO2
Q1	B)	Fill in the blanks: i) Euler Totient Function ø(23) = _____ ii) If encrypted text by Caesar cipher is 'PLFURFRPSXWHU' ; its plaintext= _____ iii) Usually, Window passwords are stored in ____ byte hash value. iv) RSA computes private key component d= _____; given public key (e=7, n=17 x 31)	4	CO2
Q2	A)	Compare configuration from Set A to Set B (Note: Configuration figures with standard symbolic representation)	6	CO1
Q2	B)	Explain various approaches for Intrusion-anomaly detection.	4	CO3

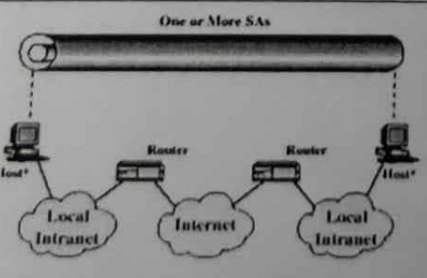
1) Set A



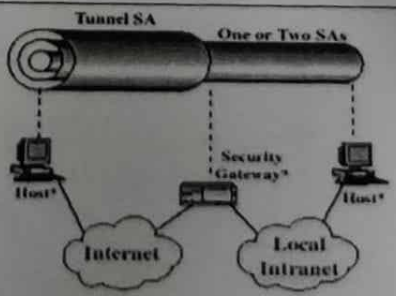
Set B



2) Set A



Set B



(P.T.O.)

Q3	A)	Differentiate following: (Any two) i) Transport and Tunnel mode for IP security ii) Packet filtering router and Application level gateway iii) Tree based and Mesh based PKI architecture	6	CO1
Q3	B)	w.r.t. X.509 certifications; justify the importance of following: i) Certificate Revocation List ii) Certificate Issuer and Subject	4	CO3
Q4	A)	The key provided to Hill cipher is 'GYBNQKURP' and is written in nxn matrix. Encrypt the message 'ACT' and obtain corresponding Cipher-text. Key= $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$	6	CO2
Q4	B)	Justify that, Kerberos V5 is having operational flexiblility than V4.	4	CO
Q5		Write notes on: (Any two) i) Trusted Systems ii) Honeypots iii) Email Security iv) Digital Signature- Generation and Verification	10	CO

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Computer Science and Engineering)

MAKEUP EXAMINATION: SEMESTER I MAY-2019

INFORMATION SECURITY (3CS401)

Exam Seat Number: _____

Day, Date and Time: Thursday, 09/05/2019, 02.00pm to 05.00pm

Max Marks:

IMP: Verify that you have received question paper with correct course, code, branch etc.

Instructions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written. Assume suitable data wherever necessary.
ii) Figures to the right of question text indicate full marks.
iii) Mobile phones and programmable calculators are strictly prohibited.
iv) Except Exam Seat Number writing anything on question paper is not allowed. Exchange/Sharing of stationery, calculator etc. not allowed.

Text on the right of marks indicates course outcomes (only for faculty use).		Mar
Q1 A)	Using Extended Euclidean Algorithm find the multiplicative inverse of 11 in Z_{26} (The integers Mod 26).	6
Q1 B)	Use the Chinese Remainder Theorem (CRT) to solve the following system of linear Congruence's: $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 5$ $x \equiv 2 \pmod 7$	6
Q1 C)	Distinguish active and passive attack with example.	6
Q2 A)	Construct a table for the Playfair Cipher with the keyword "**EFFECTIVENESS**" and Encrypt the phrase: "EXAMFORINFORMATIONSECURITY".	6
Q2 B)	Explain AES encryption process in detail.	6
Q2 C)	Use the Vigenere cipher with the keyword **"Health"** to encipher the message "Life is full of surprises".	6
Q3 A)	Perform encryption and decryption using the RSA algorithm for the following: P=3; q=13; e=5; M=10	6
Q3 B)	Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=11 and a primitive root α=2. a. If Alice has a private key XA=9, what is Alice public key YA? b. If Bob has a private key XB=4, what is Bob's public key YB? c. What the shared secret key?	6
Q3 C)	Explain the ElGamel cryptosystem with example.	6
Q4 A)	List the main features of SHA 512 cryptographic hash function. Draw the block diagram of SHA 512 and state the general step in the process.	7
Q4 B)	Explain the concept of digital signature.	7
Q5 A)	Explain packet format of ESP in transport mode and tunnel mode.	8
Q5 B)	List and give the purpose of four protocols defined in SSL or TLS.	8
Q6 A)	Discuss the different types of firewall systems.	8
Q6 B)	Explain the various types of IDS.	8