WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

ESE

Final Year B.Tech. (Information Technology)

END SEMESTER EXAMINATION SEM. I NOVEMBER-2017

CRYPTOGRAPHY AND NETWORK SECURITY (3IT401)

Exam Seat Number: ____________________

Day, Date and Time: Monday, 20/11/2017, 03.00pm to 05.00pm

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.

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

iii) Assume suitable data wherever necessary, Write the answers with neat handwriting.

iv) Only FX82 series non programmable Calculator is allowed.

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

			Marks	
Q1	A)	w.r.t Perimeter Security; identify the importance of the following: (Any two) i) Bastion Host ii) Trusted System iii) Network Address Translation	6	CO2
Q1	B)	Focus on Firewall design configurations in terms of implementation.	6	CO3
Q2	A)	How Statistical and Rule based approaches help to examine intrusion in the system?	6	CO2
Q2	B)	Discuss various cases for combining Security Association bundles providing IPSec.	8	CO3
Q3	A)	Alice and Bob use D-H key exchange technique with a common prime q=353 and primitive root α =3 i) If user A has public key YA = 40 and shared secret key between Alice and Bob K= 160 ; calculate A's private key XA. ii) If user B has private key XB = 233, calculate B's public key YB.	6	CO1
Q3	B)	Decipher the plaintext message= 'CAT' by applying Hill cipher with key matrix:	4	CO1

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

*Refer Table – Letters and Their Corresponding Positions; Key * Plaintext = Cipher*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Q4		Compare Following: (Any two) i) Kerberos V4 and V5 ii) Transport and Tunnel mode in IP security iii) Firewall and IDS iv) Cryptography and Hash Functions	6	CO2
Q5		Discover the working of following composing security mechanism: (Any Two) i) Secure Electronic Transactions (SET) ii) Elliptic Key Cryptography iii) Digital Signature Algorithm iv) PGP, S/MIME	8	CO3

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Information Technology)

MAKEUP EXAMINATION APRIL/MAY-2018

CRYPTOGRAPHY AND NETWORK SECURITY (3IT401)

MakeUp

Exam Seat Number: ____________________

Day, Date and Time: Wednesday, 02/05/2018, 02.00pm to 05.00pm

Max Marks: **100**

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)	Compare following: i) CBC and CFB modes of data transfer ii) Active and Passive attacks iii) Packet Filtering Router and Application Level Gateway	12	CO3
Q1	B)	How Digital Signature is generated using DSS algorithm.	6	CO2
Q2	A)	In a publickey system using RSA, you intercept the ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?	8	CO1
Q2	B)	Users A and B use the D-H key exchange technique with a common prime q=71 and primitive root α =7 i) IF user A has private key XA = 5, what is A's public key YA ? ii) IF user B has private key XB = 12, what is B's public key YB ? iii) What is the shared secret key	8	CO2
Q3	A)	What is Kerberos system? How TGS issues TGT for invoking services.	8	CO2
Q3	B)	What are Transport and Tunnel mode for IP security? Demonstrate various cases of Security Associations for IP services.	8	CO3
Q4	A)	Using suitable example; exhibit the working of following: i) Hill Cipher ii) Rotar Machine	8	CO1
Q4	B)	Compare firewall design configurations w.r.t. Single and Dual homed Bastion host.	8	CO2
Q5	A)	Discuss Statistical and Rule based Intrusion Detection approaches.	8	CO1
Q5	B)	Focus on Feistel cipher design structure and principles.	8	CO1
Q6		Write short notes on: i) Electronic Mail Security ii) Secure Electronic Transaction iii) X.509 Digital Certificate	18	CO3

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

MakeUp

Final Year B.Tech. (Information Technology)

MAKEUP EXAMINATION: SEMESTER I MAY-2019

CRYPTOGRAPHY AND NETWORK SECURITY (3IT401)

Exam Seat Number: ____________________

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

Max Marks: **100**

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)	Using suitable block diagram explain design principles of: i) Output Feedback Mode (OFB) of Data Transfer ii) DES algorithm round iii) Kerberos	18	CO2
Q1	B)	i) GCD(60, -12) = ____________ ii) 7^5 mod 119 = ____________	6	CO1
Q2	A)	Differentiate following: i) Private and Public key cryptography ii) Cryptography and Hash functions iii) Transport & Tunnel IP mode	18	CO3
Q2	B)	If plaintext is, 'helloworld', find ciphertext using: i) Caeser Cipher (key = 3) ii) Rail Fence Cipher (key = 2)	6	CO1
Q3	A)	In RSA public cryptosystem, if primes are p=5 and q=11, encryption parameter e=3 and plaintext M=9; Calculate lowest decryption parameter d and cipher C	9	CO2
Q3	B)	Draw structure of X.509 certificate showing various components.	8	CO3
Q4	A)	Using appropriate mathematical function, explain design and key exchange criteria of Diffie-Hellman algorithm. How a common key is calculated from both end users?	9	CO2
Q4	B)	How firewall is useful in system security? Enlist its various types.	8	CO3
Q5		Write Notes on: i) IP Security Architecture ii) Intrusion Detection Systems iii) Email Security	18	CO1

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

Final Year B.Tech. (Information Technology)

MAKEUP EXAMINATION SEM. I APRIL/MAY-2017

CRYPTOGRAPHY AND NETWORK SECURITY (2IT401)

MakeUp

Day, Date and Time: Thursday, 04/05/2017, 02.00pm to 05.00pm

Exam Seat Number: ____________________

Max Marks: **100**

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.
ii) Figures to the right of question text indicate full marks.
iii) Assume suitable data wherever necessary.
iv) Write the answers with neat handwriting.

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

			Marks	
Q1	A)	Differentiate following: (Any 3) i) Symmetric and Asymmetric Cryptography ii) Kerberos V4 and V5 iii) Transport and Tunnel Mode in IP security iv) Steganography and Cryptography	9	CO3
Q1	B)	Write an algorithm for RSA public key cryptography. If two primes p=3, q=11 are used to encrypt plaintext M=5 with public key component e=7; What is its lowest integer private key component d ? Find corresponding cipher C and verify that decryption results into same plaintext M.	9	CO1
Q2	A)	w.r.t. DES algorithm explain following terms: (Any Two) i) S Boxes ii) DES Key Expansion iii)Differential cryptanalysis iv) Round function of DES Algorithm	8	CO1
Q2	B)	What are various design issues in firewall types? Discuss its advantages and disadvantages.	8	CO2
Q3	A)	Using suitable example demonstrate working of: (Any two) i) Hill Cipher ii) Playfair Cipher iii) Rotar m/c iv) Rail Fence Cryptography	8	CO1
Q3	B)	How X.509 certificates assure authentication services?	8	CO2
Q4	A)	How Diffie-Hellman key exchange algorithm helps to design a common key between communicating parties? If users A and B share common prime q=71 and primitive root α= 7; i) IF user A has private key XA = 5, what is A's public key YA ? ii) IF user B has private key XB = 12, what is B's public key YB ? iii) What is the shared secret key K?	9	CO2
Q4	B)	What are various cases for combining security associations in IP security?	9	CO3
Q5	A)	How hash functions are used in Digital Signature Algorithm?	8	CO2
Q5	B)	Explain various types of viruses and its countermeasures?	8	CO3
Q6		Write short notes on: (Any four) i) Intrusion Detection Techniques ii) CBC Mode of Data Transfer iii) Trusted Systems iv) Secure Electronic Transaction v) PGP and S/MIME	16	CO3

(~~P.T.O.~~)

WALCHAND COLLEGE OF ENGINEERING, SANGLI.

(An Autonomous Institute)

ESE

Final Year B.Tech. (Information Technology)

END SEMESTER EXAMINATION NOV./DEC.-2016

CRYPTOGRAPHY AND NETWORK SECURITY (2IT401)

Exam Seat Number: ____________________

Day, Date and Time: Tuesday, 29/11/2016, 03.00pm to 05.00pm

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.

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

iii) Assume suitable data wherever necessary.

iv) Write the answers with neat handwriting.

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

			Marks	
Q1	A)	**Compare the following: (Any 3)** i. Unconditional secure cipher & Computationally secure cipher. ii. Steganography & Cryptography. iii. Active security threat & Passive security threat. iv. Diffusion & Confusion.	6	CO1
Q1	B)	Consider a Deffie-Hellman scheme with a common prime $q=11$ and a primitive root $g=2$. i. Show that 2 is a primitive root of 11. ii. If user A has public key $Ya = 9$, what is A's private key Xa. iii. If user B has public key $Yb = 3$, what is the shared secret key K, shared with A?	6	CO2

Q2	A)	How cross-realm authentication is done in Kerberos?	3	CO3
Q2	B)	Justify the significance of generating digital signature before compression in PGP.	3	CO1
Q2	C)	Characterize the functionalities provided by S/MIME?	4	CO1
Q2	D)	Design flow chart for transmission and reception of PGP message.	4	CO3
Q2	E)	Illustrate the reasons that encourages the development of MIME extension?	4	CO3

Q3	A)	In IPSec, if ESP provides both encryption and decryption, why is AH required?	2	CO3
Q3	B)	How confidentiality and message integrity are provided in SSL record protocol. Draw a neat diagram.	4	CO2
Q3	C)	Differentiate Transport and Tunnel modes in IPSec with neat diagrams.	4	CO2

Q4	A)	List and describe three classes of intruders.	3	CO3
Q4	B)	With respect to the system security, explain the following: i. Honeypot [2M] ii. Worms [2M] iii. Packet-filtering router & circuit-level gateway [3M]	7	CO3

...Autonomous Institute) ...NEERING, SANGLI.

Final Year B.Tech. (Information Technology)

MID SEMESTER EXAMINATION SEPTEMBER / OCTOBER-2016

CRYPTOGRAPHY AND NETWORK SECURITY (2IT401)

MSE

Exam Seat Number: ____________________

y, Date and Time: Wednesday, 28/09/2016, 03.00pm to 04.30pm

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

Max Marks: 30

structions: i) All questions are compulsory. Writing question number is compulsory. The answers may not be assessed if question number is not written.
ii) Figures to the right of question text indicate full marks.
iii) Assume suitable data wherever necessary.
iv) Write the answers with neat handwriting.

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

		Marks	
Q1 A)	What security services are defined by X.800?	6	CO1
Q1 B)	Compare stream cipher with block cipher with example.	2	CO1
Q1 C)	Compare Substitution and Transposition techniques.	2	CO1
Q2 A)	Show that, DES decryption is, in fact, the inverse of DES encryption.	5	CO1
Q2 B)	List atleast five design principles of block cipher.	5	CO3
Q3 A)	What is public key certificate? Draw a neat diagram.	4	CO2
Q3 B)	In a public key system using RSA, you intercept the ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?	4	CO2
Q3 C)	What is a trapdoor one-way function?	2	CO2

(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)

Exam Seat Number: ____________________

Day, 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 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) — 6 — CO1
i) Hill Cipher ii) Playfair Cipher iii) Row Transposition Cipher

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.	Mode → Parameter ↓	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: — 9 — CO2
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

Q3 B) Fill in the blanks with appropriate integer values. — 3 — CO2
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 = ______