SASTRA UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

B.Tech Degree Examinations

May 2011

Sixth Semester

Course Code: **BCSCCS 601R01**

Course: **CRYPTOGRAPHY & NETWORK SECURITY**

Question Paper No. : **B0198** Duration: **3** hours

Max. Marks: **100**

PART – A

Answer all the questions **20 x 2 = 40 Marks**

1. What is meant by security attack?

2. What are the objectives of security services?

3. What is meant by release of message contents?

4. What is meant by data integrity?

5. What is substitution technique? Which is the best substitution technique?

6. What is meant by double encryption?

7. What is encrypt-decrypt-encrypt?

8. How to choose the cryptographic algorithms?

9. What is DES?

10. Write a short note on Knapsack algorithm.

11. What is meant by Elliptic Curve Logarithm problem?

12. Write a short note on Computational Advantage of ECC.

13. What is Encrypted Key Exchange Protocol?

14. Write a short note on Conference Key Distribution.

15. Why do we need Message Authentication Code?

16. Write a short note on PGP.

17. What is the difference between SMTP and MIME?

18. What is meant by Trusted Systems?

19. Write a short note on SSL.

20. Write a short note on Screened Host Firewall System for Single-homes Bastian Host.

PART – B

Answer all the questions **4 x 15 = 60 Marks**

21. Why does Protocol Layer need Security Services? Demonstrate various Security Services with suitable example.

(OR)

22. What is meant by Padding and Error Propagation? With suitable example, demonstrate the Encryption and Decryption Procedures of Cipher Block Chaining Mode.

23. With neat diagram, describe the architecture of Blowfish with its 16 rounds Feistel network and its Function F.

(OR)

24. What is meant by Asymmetric Key Cryptography Protocol? Explain the RSA algorithm with your own suitable example.

25. With suitable example, explain the Diffie-Hellman public key cryptography key exchange algorithm.

(OR)

26. What is meant by Digital Signature? Describe Digital Signature Algorithm with its various parameters and procedures.

27. Why do we need IPSec at the Network Layer? Describe in detail about IPSec Architecture and its various services.

(OR)

28. What are the various types of Firewalls? With suitable diagrams, demonstrate all of them.

* * *

SASTRA UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

B.Tech. Degree Examinations

May 2012

Sixth Semester

Course Code: **BCSCCS 601R01**

Course: **CRYPTOGRAPHY & NETWORK SECURITY**

Question Paper No. : **B0194** Duration: **3** hours

Max. Marks: **100**

PART – A

Answer all the questions **20 x 2 = 40 Marks**

1. What is stegnography?

2. State link encryption approach.

3. Define Threat and Attack.

4. Mention the features of polyalphabetic ciphers.

5. What are the characteristics of asymmetric algorithms?

6. State Man-in-the-middle attack.

7. Define Blow fish.

8. What is Triple encryption?

9. What is an Elliptic curve?

10. State the properties of Hash function.

11. What are the two approaches of digital signatures? Explain them.

12. List the applications of IP sec.

13. What are the services provided by PGP?

14. List and briefly define the three class of intruders.

15. What are the techniques used to protect a password file?

16. What is a honey pot?

17. Define reactive password checking.

18. What is kerboros? Write its function.

19. What is Avalanche effect in DES?

20. List the design goals for a firewall.

PART – B

Answer all the questions **4 x 15 = 60 Marks**

21. What are the techniques involved in distribution of public keys?

(OR)

22. With a suitable example, explain about RSA algorithm.

23. (a) Explain in detail about Diffie-hellman key exchange. (8)
    (b) Describe briefly about elliptic curves over real numbers. (7)

(OR)

24. (a) Discuss the features of SHA algorithm. (8)

(b) Write about Secure Socket Layer (SSL) architecture. (7)

25. Describe about trusted systems.

(OR)

26. Discuss in detail about the different approaches of DSA and its algorithm.

27. Write short notes on Brute force attack and cryptanalysis.

(OR)

28. Explain triple encryption with two keys.

* * * * *

SASTRA UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

B.Tech. Degree Examinations

May 2014

Sixth Semester

Course Code: **BCSCCS 601R02 / BITCIT 601R02 / BICCIC 601R02**

Course: **CRYPTOGRAPHY & NETWORK SECURITY**

Question Paper No. : **B0140** Duration: **3** hours

Max. Marks: **100**

PART – A

Answer all the questions **20 x 2 = 40 Marks**

1. Mention the aspects of information security.

2. Differentiate between Active and Passive attacks.

3. Define one time pad.

4. What is mono alphabetic substitution cipher?

5. What is covert channel?

6. What is meet-in-the middle attack?

7. In what way AES differs from DES?

8. Write some features of blow fish algorithm.

9. What are the ingredients for public-key encryption?

10. Write Davies-Price double encryption method.

11. What is hash function?

12. What is message authentication code?

13. Write the equation for user A key generation in ECC-Key-Exchange.

14. What are the web security threats?

15. What are the three parameters by which, security association is uniquely identified?

16. What is meant by birthday attack?

17. What are the requirements of hash functions?

18. Define PGP.

19. What is meant by alert protocol?

20. List out some of the benefits of IP security.

PART – B

Answer all the questions **4 x 15 = 60 Marks**

21. Explain the OSI security architecture in detail.

(OR)

22. Draw neatly the diagram of Fiestal cipher structure and explain it in detail.

23. Explain AES algorithm.

(OR)

24. Discuss the counter mode encryption and decryption.

25. Describe the RSA public key encryption and discuss its variants.

(OR)

26. Discuss the intellectual property rights in network security.

27. Illustrate the elagamal digital signature scheme.

(OR)

28. Describe the MAC and internet key exchange.

* *

SASTRA UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

B.Tech. Degree Examinations

May 2015

Sixth Semester

Course Code: **BCSCCS 601R02 / BITCIT 601R02 / BICCIC 601R02**

Course: **CRYPTOGRAPHY & NETWORK SECURITY**

Question Paper No. : **B0138** Duration: 3 hours

Max. Marks: 100

PART – A

Answer all the questions **20 x 2 = 40 Marks**

1. What is the difference between diffusion and confusion?
2. When is an encryption scheme unconditionally secure?
3. Distinguish between threat and attack.
4. What is nonrepudiation?
5. What is avalanche effect?
6. Determine the factors of $x^3 + 1$ over GF (2).
7. What is meant by cipher-text stealing?
8. For the group S_n of all permutations of distinct symbols, show that S_n is not abelian for $n > 2$.
9. What is the smallest positive integer that has exactly k divisors for $1 \leq k \leq 6$?

10. What is a meet-in-the-middle attack?

11. Perform encryption using the RSA algorithm for $p = 7; q = 11, e = 17; M = 8$.

12. What are the four phases of virus life cycle?

13. What is the zero point of an elliptic curve?

14. Generate a public key using Elagammal Cryptographic system for $q = 19; \alpha = 10; X_A = 5$.

15. What rights does a copyright confer?

16. Define a cryptographic hash function.

17. Why is R64 conversion useful for an e-mail application?

18. What is the difference between transport mode and tunnel mode?

19. What is MIME?

20. What properties should the digital signature have?

PART – B

Answer all the questions **4 x 15 = 60 Marks**

21. (a) Using this playfair matrix:

T	M	P	Q	S
Z	V	W	X	Y
E	O	C	U	R
F	N	A	B	D
L	G	H	I/J	K

Encrypt this message: "The enemy must be stopped at all costs. Do whatever is necessary". (8)

(b) What is differential cryptanalysis and explain its working principle with respect to DES. (7)

(OR)

22. (a) Explain Vigenere cipher with its vulnerability to cryptanalysis and encrypt the following plaintext using the key *deceptive*: (11)

"wearediscoveredsaveyourself"

(b) Explain the various parameters and design choices that determine the actual algorithm of a Feistel cipher. (4)

23. (a) Construct GF(2^4) multiplication table using Generator for the polynomial m(x) = $x^4 + x + 1$ and determine the multiplicative inverse of $x^3 + x + 1$. (10)

(b) Does the set of residue classes (mod3) form a group with respect to modular addition and modular multiplication? (5)

(OR)

24. (a) Discuss the CBC and CFB block cipher operations. (12)

(b) Show that an integer is congruent modulo 9 to the sum of its decimal digits. (3)

25. Explain the following:

(a) Diffie-Hellman Key Exchange Protocol and its vulnerability to Man-in-the-Middle Attack. (8)

(b) Key exchange algorithm using elliptic curves. (7)

(OR)

26. Give a detailed account on firewall wall characteristics and its types.

27. Discuss steps of SHA-512 with a neat diagram.

(OR)

28. Explain SSL Architecture and its protocols.

* *

SASTRA DEEMED UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

B.Tech. Degree Examinations

May 2018

End Semester

Course Code: **BCSCCS 601R03 / BITCIT 601R03 / BICCIC 601R03**

Course: **CRYPTOGRAPHY AND NETWORK SECURITY**

Question Paper No. : **B0162** Duration: 3 hours

Max. Marks: **100**

PART – A

Answer all the questions **10 x 2 = 20 Marks**

1. Define integrity and nonrepudiation.

2. What are the known parameters for cryptanalyst in known plaintext attack?

3. How effective are Avalanche effect?

34 4. Determine the gcd (24140, 16762) using Euclid's algorithm.

5. State advantages of counter mode.

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

7. Define virus. Specify the types of viruses.

8. State the security function of trapdoor one-way function.

9. What is the difference between weak and strong collision resistance?

10. How to express HMAC with secret key?

PART – B

Answer all the questions **4 x 15 = 60 Marks**

11. (a) Let M be the plain text message, M = "ABCDEF", where M is in hexadecimal (base 16) format. Find L0, R0 and L1 and R1. Whether F function used in each round of DES is invertible or not? Evaluate the consequence of F function, S Box and E Box in DES encryption. (10)

(b) Find the cipher-text of the corresponding plaintext "C O M P U T", using Hill cipher where key $K = \begin{bmatrix} 5 & 3 & 6 \\ 2 & 4 & 7 \\ 8 & 1 & 9 \end{bmatrix}$, show your calculation and results.

(OR)

12. (a) Does a confusion and diffusion achieves perfect secrecy? Why? Examine the significance of confusion and diffusion in DES with its structure. (10)

(b) Find the cipher-text of the corresponding plaintext "INNOVATE", using columnar transposition cipher. (5)

13. (a) Let $a(x) = x^6 + x^4 + x^2 + x + 1$, $b(x) = x^5 + x + 1$. Find b(x) mod a(x) using extended Euclidean algorithm. (8)

$1+x^2$

(b) Derive an expression for encryption and decryption in CFB mode. Describe with neat diagram. (7)

(OR)

14. (a) Let polynomial arithmetic modulo $m(x) = x^3 + x + 1$. Find $(x^2 + x) X (x^2 + x)$, $(x^2 + x + 1) X (x^2 + x)$ over $Gf(2^3)$. (7)

x^2 $x,$

(b) How to encrypt and decrypt a single block in XTS AES mode? Elaborate. (8)

15. (a) Let P = 29 and Q = 19. Interpret public key and private key using RSA algorithm. Encrypt the message M = 2242 using RSA algorithm. What are the possible approaches for attacking the RSA algorithm? (10)

(b) Illustrate the issues in ethical hacking. (5)

(OR)

16. (a) Illustrate the secret key exchange among two users using Diffie Hellman key exchange protocol. Find the shared secret key, where g = 14, p = 17, a = 21 and y = 41. Describe Man in middle attack in Diffie Hellman key exchange. (10)

(b) Categorize the significance of software piracy. (5)

17. (a) Define one round process in SHA. How to derive 64 bit word from 512 bit input block using SHA – 512? Elaborate. (10)

(b) Identify the components involved in the verification of documents in DSS. (5)

(OR)

18. (a) Net Banking is an example of an application that uses SSH. The client indicates himself to the bank server through a password. Does the password communicate through packet exchange format? If yes, justify your answer with its SSH structure. (10)

(b) List the design objectives of HMAC. Derive the expressions of GHASH. (5)

PART – C

Answer the following **1 x 20 = 20 Marks**

19. (a) Determine the gcd of $(x^5 + x^4 + x^3 + x^2 + x + 1)$ and $x^3 + x^2 + x + 1$ over GF(5). (5)

(b) Let a0 = B4, a1 = 2F, a2 = 12 and a3 = 10, using AES Mix column procedure. Construct the new column value. Elaborate the calculations. (10)

(c) Determine points on elliptic curve cryptography over $E_{23}(1, 1)$. (5)

* * * * *

$-4x^2$ ~~+4~~ x^2

$x^3 + x^2 + x + 1$ | $x^5 + x^4 + x^3 + x^2 + x + 1$

~~$x^5 + x^4 + x^3 + x^2$~~

$-4x^5 - 4x^4 - 4x^3 - 4x^2$

$+ \quad + \quad + \quad +$

~~$x +$~~

$5\cancel{x^5} + 5\cancel{x^4} + 5\cancel{x^3} + 5\cancel{x^2}$

$x + 1$