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

Question Paper Code : 40404

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2021.

Sixth/Seventh Semester

Computer Science Engineering

CS 8792 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to B.E. Computer and Communication Engineering/B.E. Electronics and Communication Engineering/B.E. Electronics and Telecommunication Engineering/B.Tech. Information Technology)

(Regulations 2017)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is meant by Denial of Service attack? Is it Active Attack or Passive Attack?

2. Let message = “Anna”, and k = 3, find the ciphertext using Caesar.

3. Find Residues of 6 when n = 8.

4. Find gcd(2740, 1760) using Euclidean Algorithm.

5. Using Fermat’s theorem, check whether 19 is prime or not? Consider a is 7.

6. Find atleast two points lies in the elliptic curve $y^2 = x^3 + 2x + 3 (\text{mod}\, 5)$.

7. What is meant by padding? And, why padding is required?

8. Draw functional diagram of RSA based Digital Signature.

9. Explain the process of Radix 64 conversion.

10. Write short notes on Spammers and Key loggers.

PART B — (5 × 13 = 65 marks)

11. (a) (i) Let message = "graduate", Key = "word", find ciphertext using playfair cipher. (8)

(ii) List out any two di-gram, two tri-gram. Shortly describe the application of di-gram and tri-gram in cryptography. (5)

Or

(b) Demonstrate encryption and decryption process in hill cipher. Consider m = "sh" and key = hill". (4 + 9)

12. (a) (i) Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data. (8)

(ii) Explain the bitwise XOR operation which involved in RC4. (5)

Or

(b) (i) Explain with sample data: Four transformations in AES. (10)

(ii) In finite field arithmetic, $\left(x^6 + x^4 + x^2 + x + 1\right) + \left(x^7 + x + 1\right) = ?$. (3)

13. (a) (i) Demonstrate the DH key exchange methodology using following key values : $p = 11$, $g = 2$, $X_A = 9$, $X_B = 4$. (7)

(ii) Diffie–Hellman key agreement is not limited to negotiating a key shared by only two participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate, Write the steps and formulas to be followed for DH key exchange between Alice, Bob, and Carol. (6)

Or

(b) (i) In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M? (7)

(ii) In an RSA system, the public key of a given user is e = 65, n = 2881, What is the private key of this user? (6)

14. (a) Write the steps involved in the Generation of Message Digest. (13)

Or

(b) (i) Discuss the four requirements of Kerberos. (4)

(ii) Shortly describe about the elements of X509 Certificate. (9)

15. (a) Discuss the seven types of MIME content type.

Or

(b) Draw IPSec Authentication Header and write short notes on each element of the Header.

PART C — (1 × 15 = 15 marks)

16. (a) A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint : Use Chinese Remainder Theorem).

Or

(b) (i) Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? (5)

(ii) Prove that Euler's Totient value of any prime number (p) is $p-1$ and the Euler's Totient value of the non-prime number (n) is $(p-1)\times(q-1)$ where $p\times q$ are prime factor of n. (5)

(iii) Mr. Ram chooses RSA for encryption, and he chooses 3 and 7 are two prime numbers. He encrypt the given message (message given in English alphabets) by mapping A = 1, B = 2, C = 3.., Z = 26. Find atleast two problems in his implementation. (5)

———————

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

Question Paper Code : X10328

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020
Seventh Semester
Computer Science and Engineering
CS8792 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Information Technology and Computer and Communication Engineering)
(Regulations 2017)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Compare active and passive attack.
2. Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now.
3. Give the five modes of operation of block cipher.
4. Define field and ring in number theory.
5. Find the GCD of (2740,1760) using Euclid's Algorithm.
6. For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message = 80 and thus find the plain text.
7. What is MAC ? Mention the requirement of MAC.
8. State birthday problem.
9. List out the applications of SSL.
10. What do you mean by IP Security policy ?

PART – B **(5×13=65 Marks)**

11. a) i) What is monoalphabetic cipher ? Examine how it differs from Caesar cipher. **(7)**

ii) Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext. **(6)**

(OR)

b) i) Explain OSI Security Architecture model with neat diagram. **(7)**

ii) Describe the various security mechanisms. **(6)**

12. a) i) Demonstrate that the set of polynomials whose coefficients forms a field is a ring. **(5)**

ii) For each of the following elements of DES, indicate the comparable element in AES if available :

a) XOR of subkey material with the input to the function. **(4)**

b) f function. **(4)**

(OR)

b) What do you mean by AES ? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. **(13)**

13. a) i) With a neat sketch, explain the Elliptic curve cryptography with an example. **(8)**

ii) Alice and Bob use the Diffie – Hellman key exchange technique with a common prime number 11 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the shared secret key. **(5)**

(OR)

b) State Chinese Remainder theorem and find the value of X for the given set of congruent equations using Chinese Remainder theorem. **(13)**

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

$X \equiv 4 \pmod{11}$

14. a) Briefly explain the steps of message digest generation in Whirlpool with a block diagram. **(13)**

(OR)

b) Explain PKI management model and its operations with the help of a diagram. **(13)**

15. a) With the help of a neat diagram, explain wired and wireless TLS architecture. **(13)**

(OR)

b) Assume when an attacker tries to modify the database content by inserting an UPDATE statement. Identify this SQL injection attack method and justify. Detail the methods used to prevent SQL injection attack. **(13)**

PART – C **(1×15=15 Marks)**

16. a) Discuss examples from real life, where the following security objectives are needed :

i) Confidentiality. **(5)**

ii) Integrity. **(5)**

iii) Non-repudiation. **(5)**

Suggest suitable security mechanisms to achieve them.

(OR)

b) Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer amount	Cryptography functions required
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. **(15)**

———————

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

Question Paper Code : 71690

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2017.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering and Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. State Fermat's theorem.
2. Determine the gcd (24140, 16762) using Euclid's algorithm.
3. State the difference between private key and public key algorithm.
4. Give the five modes of operation of block cipher.
5. What is the role of compression function in hash function?
6. Specify the various types of authentication protocol.
7. Define the roles of firewalls.
8. State the difference between threats and attacks.
9. Draw the ESP packet format.
10. Specify the benefits of IPSec.

PART B — (5 × 16 = 80 marks)

11. (a) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT (16)

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

$X \equiv 4 \pmod{11}$

Or

(b) Describe :

(i) Playfair cipher

(ii) Railfence cipher

(iii) Vignere cipher. (16)

12. (a) Explain Diffie-Hellman Key exchange algorithm in detail. (16)

Or

(b) Describe DES algorithm with neat diagram and explain the steps. (16)

13. (a) Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm. (16)

Or

(b) Explain the concepts of Digital signature algorithm with key generation and verification in detail. (16)

14. (a) Discuss the different types of virus in detail. Suggest scenarios for deploying these types in network scenario. (16)

Or

(b) Explain Intrusion Detection System (IDS) in detail with suitable diagram. (16)

15. (a) Explain the architecture of IP security in detail. (16)

Or

(b) Discuss authentication header and ESP in detail with their packet format. (16)

Reg. No. :

Question Paper Code : 40917

22/04/18 AN

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2018
Seventh/Eighth Semester
Computer Science and Engineering
CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Electronics and Communication Engineering/Information Technology)
(Regulations 2013)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Why is asymmetric cryptography bad for huge data ? Specify the reason.
2. State Euler's theorem.
3. List the parameters (block size, key size, and no. of rounds) for the three AES versions.
4. Perform encryption and decryption using RSA Algorithm for the following. P = 7; q = 11; e = 17; M = 8.
5. What is a hash in cryptography ?
6. How digital signatures differs from authentication protocols ?
7. What is the main function of a firewall ?
8. What is a Threat ? List their types.
9. List out the services provided by PGP.
10. What is the difference between TLS and SSL security ?

PART – B **(5×16=80 Marks)**

11. a) Explain classical encryption techniques with symmetric cipher and Hill cipher model.

(OR)

b) State and prove the Chinese remainder theorem. What are the last two digits of 49^{19} ?

12. a) What do you mean by AES ? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.

(OR)

b) With a neat sketch explain the Elliptic curve cryptography with an example.

13. a) How Hash function algorithm is designed ? Explain their features and properties.

(OR)

b) With a neat diagram, explain the MD5 processing of a single 512 bit block.

14. a) Explain briefly about the architecture and certification mechanisms in Kerberos and X.509.

(OR)

b) How does screened host architecture for firewalls differ from screened subnet firewall architecture ? Which offers more security for information assets on trusted network ? Explain with neat sketch.

15. a) Illustrate how PGP encryption is implemented through a suitable diagram.

(OR)

b) Write short notes on the following :

a) Public Key Infrastructure (8)

b) Secure Electronic Transaction (8)

10-4-19
FN

Reg. No. :

Question Paper Code : 52874

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2019.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering/Information Technology)

(Regulation 2013)

(Also common to PTCS 6701 — Cryptography and Network Security for B.E. (Part-Time) — Sixth Semester – Computer Science and Engineering – Regulation 2014))

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate active and passive attacks.
2. Specify the components of encryption algorithm.
3. Give the applications of the public key cryptosystem.
4. What are primitive operations used in RC5?
5. What are the requirements for message authentication?
6. Show how SHA is more secure than MD5.
7. List the design goals of firewalls.
8. List the three classes of intruders.
9. Mention the five header fields defined in MIME.
10. What are the benefits of IP Security?

PART B — (5 × 13 = 65 marks)

11. (a) (i) What is steganography? Describe the various techniques used in steganography. (7)

(ii) What is monoalphabetic cipher? Examine how it differs from Caesar cipher. (6)

Or

(b) Explain the network security model and its important parameters with a neat block diagram.

12. (a) (i) Describe in detail the key generation in AES algorithm and its expansion format. (7)

(ii) Describe triple DES and its applications. (6)

Or

(b) (i) Describe RSA algorithm. (8)

(ii) Perform encryption and decryption using RSA algorithm for the following : $p = 7$, $q = 11$, $e = 7$, $M = 9$. (5)

13. (a) Describe digital signature algorithm and show how signing and verification is done using DSS.

Or

(b) Describe the MD5 message digest algorithm with necessary block diagrams.

14. (a) (i) What is Kerberos? Explain how it provides authenticated service. (7)

(ii) Explain the format of the X.509 certificate. (6)

Or

(b) Explain the various types of firewalls with neat diagrams.

15. (a) Explain PGP cryptographic functions in detail with suitable block diagrams.

Or

(b) Explain the architecture of IPsec in detail with a neat block diagram.

PART C — (1 × 15 = 15 marks)

16. (a) (i) Explain briefly about Diffie Hellman key exchange algorithm with its merits and demerits. (10)

(ii) Explain public key cryptography and when it is preferred? (5)

Or

(b) Solve using playfair cipher method. Encrypt the word "Semester Result" with the keyword "Examination". Discuss the roles to be followed.

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

12/11/2016
FN

Question Paper Code : 80304

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Seventh Semester Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare active and passive attack.
2. Find gcd (1970, 1066) using Euclid's algorithm.
3. Brief the strengths of triple DES.
4. What is an elliptic curve?
5. State any three requirements for authentication.
6. Differentiate MAC and Hash function.
7. List the three classes of intruders.
8. Define Zombie.
9. List the limitations of SMTP/RFC 822.
10. Define Botnets.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain OSI Security Architecture model with neat diagram. (8)

(ii) Describe the various security mechanisms. (8)

Or

(b) (i) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT.

X = 2(mod 3)

X = 3(mod 5)

X = 2(mod 7). (8)

(ii) State and prove Fermat's theorem. (8)

12. (a) Explain AES algorithm with all its round functions in detail. (16)

Or

(b) Explain RSA algorithm, perform encryption and decryption to the system with $p = 7$; $q = 11$; $e = 17$; $M = 8$. (16)

13. (a) Describe MD5 algorithm in detail. Compare its performance with SHA-1. (16)

Or

(b) Explain digital signature standard with necessary diagrams in detail. (16)

14. (a) Discuss Client Server Mutual authentication, with example flow diagram. (16)

Or

(b) Explain the technical details of firewall and describe any three types of firewall with neat diagram. (16)

15. (a) Discuss the working of SET with neat diagram. (16)

Or

(b) Explain the operational description of PGP. (16)

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

Question Paper Code : 80223

12(11) 16 FN

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Civil Engineering

CE 6703 – WATER RESOURCES AND IRRIGATION ENGINEERING

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the two important standards for irrigation water?
2. Define flood walls.
3. Define consumptive use of surface water.
4. What is multipurpose reservoir?
5. What are canal regulators?
6. Define Duty, Delta and Base period.
7. What is the need for water budget?
8. What is the purpose of canal lining?
9. Why drop irrigation is preferred?
10. Define micro irrigation.

PART B — (5 × 16 = 80 marks)

11. (a) Briefly state the various steps needed for planning an irrigation project. List the various objectives of water resources development in the context of the lesser developed countries.

Or

(b) What are the various water sources used for irrigation? How is the storage capacity of a large reservoir fed by a rier for a large irrigation project determined?

12. (a) Outline briefly the concept of ground water budgeting and its importance in the determination of the safe yield from a basin.

Or

(b) What are the quality criteria for irrigation water? Show the relationship between the different parameters. Classify the irrigation water based on various parameters.

13. (a) What is meant by transpiration by plants? Do you consider it an evil as it causes water loss from the soil and plants? What does transpiration coefficient means?

Or

(b) Suggest a method for estimating the consumptive use of crops over a large area. Classify the consumption use of water by crop based on its estimation during specific periods.

14. (a) What are cross drainage work? What is necessity of such a work in a canal project, and how does this necessity is fulfilled by such water?

Or

(b) List the different types of canal lining in common use. Draw a neat sketch of a typical cross section of a canal carrying a discharge of 60 m^3/sec and lined with brick in cement motor. Mark the salient features on the sketch.

15. (a) What is tank irrigation? Differentiate between isolated tanks and Group tanks. How can compute the storage capacity of an irrigation tank?

Or

(b) What is participating irrigation management? Give a case study of the above type of management and explain.

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

Question Paper Code : 80352

12/11/16 FN

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Electronics and Communication Engineering

EC 6701 — RF AND MICROWAVE ENGINEERING

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. List the radio frequency bands available in microwave and radio frequency ranges.
2. Define S-parameters.
3. Define Noise figure.
4. Calculate VSWR of an amplifier, if the amplifier has reflection coefficient 0.2533.
5. Compare PIN and PN diode.
6. What is isolator? And why isolators are called uniline?
7. What is magnetron?
8. What is Tetrodes and Pentodes?
9. What is network analyzer?
10. Classify microwave powers with its range.

PART B — (5 × 16 = 80 marks)

11. (a) (i) What is transmission (T) matrix? Obtain and explain the relationship with [S] and vice versa. (8)

(ii) Compute the intrinsic wave impedance, phase velocity and wavelengths of an electromagnetic wave in free space and a printed circuit board (PCB) material whose dielectric constant is 4.6 for the frequency f = 30 MHz and 3 GHz. (8)

Or

(b) (i) Explain and analyze any reciprocal lossless network with derivation. (10)

(ii) Discuss on the application of RF and microwave area. (6)

12. (a) Derive the equation for power gain, available power gain and transducer power gain. (16)

Or

(b) Investigate the stability regions of a transistor whose S-parameters are recorded as follows :

$S_{12} = 0.2\angle -10^\circ$; $S_{11} = 0.7\angle -70^\circ$; $S_{21} = 5.5\angle 85^\circ$ and $S_{22} = 0.7\angle -45^\circ$ at 750 MHz. (16)

13. (a) Discuss briefly about working principle, operation, characteristics and application of varactor diode. (16)

Or

(b) What is circulator? With neat diagram, explain the working principle, construction, operation of four-port circulator using magic-tee. Verify the circulator theory with necessary S-parameter equations.

14. (a) Explain the working principle and operation of multi-cavity Klystron amplifier and derive the expressions for its output power. (16)

Or

(b) A travelling wave tube (TWT) operates under the following parameters :

Beam Voltage $V_0 = 3$ kV

Beam Current $I_0 = 30$ mA

Characteristic impedance of helix $= Z_0 = 10\ \Omega$

Circuit length $= N = 50$ m

Frequency $f = 10$ GHz

Determine :

(i) Gain parameters C.

(ii) Output power gain A_p in decibels.

(iii) All four propagation constants. (16)

15. (a) Explain the impedance measurement technique using slotted line and reflectometer. (8 + 8)

Or

(b) Explain the measurement of high VSWR with the help of block diagram. (16)

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

Question Paper Code : 80385

12/11/16 FN

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Electrical and Electronics Engineering

EE 6701 — HIGH VOLTAGE ENGINEERING

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is back flashover?
2. Define Isokeraunic level or thunderstorm days.
3. What is ionization by collision?
4. Define Gas law.
5. What is a tesla coil?
6. What is Deltatron circuit?
7. What are the advantages of generating voltmeters?
8. List some advantages of Faraday generator.
9. Define 50% flash over voltage.
10. What are the tests need to be conducted on power transformer?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain the mechanism of lightning stroke. (10)

(ii) Give the mathematical model for lightning discharges and explain them. (6)

Or

(b) Explain the different methods employed for lightning protection of overhead lines. (16)

12. (a) From the fundamental principles, derive Townsend's criteria for the breakdown of gaseous dielectric medium. (16)

Or

(b) Explain the various breakdown theories involved in commercial liquid dielectrics. (16)

13. (a) (i) Mention the necessity of generating high DC voltages. (4)

(ii) Explain with a neat diagram the generation of high DC voltages using Van-de-graff generator. State the factors which limit the voltage developed. (12)

Or

(b) Explain the working principle of Cockroft-Walton voltage multiplier circuit. Derive an expression for total voltage drop and total ripple voltage of n-stage voltage multiplier circuit and hence deduce the condition for optimum number of stages. (16)

14. (a) (i) Enumerate digital peak voltmeter. (8)

(ii) What is CVT? Explain how CVT can be used for high voltage AC measurement. (8)

Or

(b) Explain how a sphere gap can be used to measure the peak value of voltages? Also discuss the parameters and factors that influence such voltage measurement? (16)

15. (a) Discuss the various tests carried out in a circuit breaker at HV labs. (16)

Or

(b) Explain in sequence the various high voltage test being carried out in a power transformer. (16)

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

Question Paper Code : 80133

12/11/16 FN

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Fifth Semester

Biomedical Engineering

BM 6503 — BIO MATERIALS AND ARTIFICIAL ORGANS

(Common to Medical Electronics)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Give the classification of biomaterials. Give one example for each class.

2. What is a viscoelastic material? Give an example.

3. Write any two advantages of Yitrium siabilized zirconia as an implant material over aluminia.

4. What is DCC coating? State its application in medical devices.

5. Silica flour (finely ground SiO_2 densily : 265 kg/m^3)

   is used as a filler for polymethyl siloxane (silastic rubber). Find the weight percent and volume fraction of SiO_2 required to make a silastic rubber with a density of 125 kW/m^3.

6. Draw the stress-stain curve of collagen, elastin and tissue.

7. Write the three types of soft tissue implants. Give examples.

8. State the role of vascular crafts. List any two requirements for that.

9. What is an artificial kidney and what are all function?

10. What is the function of an oxygenator? Name any two types.

PART B — (5 × 16 = 80 marks)

11. (a) Explain the following with an example :

(i) Stress and strain. (4)

(ii) Toughness. (4)

(iii) Fatigue failure and Wear failure. (4)

(iv) Young's Modulus. (4)

Or

(b) (i) Explain the steps involved in a wound healing process. (10)

(ii) Write a note on body response to implants. (6)

12. (a) Explain the types, properties and manufacturing of implants using the following.

(i) Stainless steel. (8)

(ii) Co based alloys. (8)

Or

(b) (i) Explain the types, properties and manufacturing of implants using carbon. (10)

(ii) Explain the creep and stress relaxation in a viscoelastic material. (6)

13. (a) (i) Discuss the structure and biomaterial applications of the following biopolymers

(1) Collagen. (5)

(2) Elastin. (5)

(ii) Write a note on dental filling composites and cements. (6)

Or

(b) Discuss in detail the biomaterials used for ophthalmology. (16)

14. (a) (i) Write a detailed note on the nature. properties and functionality of suture materials. (10)

(ii) A nylon suture was implanted in the abdominal cavity of a dog. The suture was removed after 10 days and a second piece of the same suture was removed after 20 days, and its average tensile strength was found to be decreased by 40% and 50% respectively. How long it will take the strength to decay 60% of its original value? (6)

Or

(b) Discuss in detail the functionality of Hip and knee joint replacements. (16)

15. (a) (i) Explain the functioning of artificial kidney (dialyzer membrane). (12)

(ii) A bioengineer is designing an arterial stent from NiTi alloy and polyester cloth to enlarge an arthroscelerotic artery Calculate the hoop stress in an 8×10^3 m diameter artery with a thickness of 1×10^{-3} m due to a blood pressure of 90 mm of Hg. Assume the artery a uniform cube. (4)

Or

(b) Explain the following with reference to dental implants

(i) Endosseous implant. (4)

(ii) Re implantation of natural teeth. (4)

(iii) Mandibular reconstruction. (4)

(iv) Testing and evaluation of dental implant. (4)

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

Exam Cell
30/10/17
FN

Question Paper Code : 50399

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2017
Seventh/Eighth Semester
Computer Science and Engineering
CS 6701 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Electronics and Communication Engineering/Information Technology)
(Regulations 2013)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions.

PART – A **(10×2=20 Marks)**

1. Categorize Passive and Active attack.
2. State Fermat's Theorem.
3. Perform encryption for the plain text M = 88 using the RSA Algorithm p = 17, q = 11 and the public component e = 7.
4. Give the significance of hierarchical key control.
5. How is the security of a MAC function expressed ?
6. Mention the significance of signature function in Digital Signature Standard (DSS) approach.
7. Write a simple authentication dialogue used in Kerberos.
8. List any 2 applications of X.509 Certificates.
9. Specify the purpose of ID Payload in Phase I and Phase II inherent in ISAKMP/ IKE encoding.
10. Justify the following statement :

"With a Network Address Translation (NAT) box, the computers on your internal network do not need global IPV4 addresses in order to connect to the Internet".

PART – B (5×16=80 Marks)

11. a) Encrypt the following using play fair cipher using the keyword MONARCHY.

"SWARAJ IS MY BIRTH RIGHT". Use X for blank spaces.

(OR)

b) Discuss the properties that are to be satisfied by Groups, Rings and Fields.

12. a) Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 83 and a primitive root $\alpha = 5$.

i) If Alice has a private key $X_A = 6$, what is Alice's public key Y_A ? (6)

ii) If Bob has a private key $X_B = 10$, what is Bob's public key Y_B ? (6)

iii) What is the shared secret key ? (4)

(OR)

b) For each of the following elements of DES, indicate the comparable element in AES if available.

i) XOR of subkey material with the input to the function. (4)

ii) f function. (4)

iii) Permutation p. (4)

iv) Swapping of halves of the block. (4)

13. a) Write down the steps involved in

i) Elgamal Digital Signature Scheme. (8)

ii) Schnorr Digital Signature Scheme.
used for authenticating a person. (8)

(OR)

b) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest.

14. a) Explain how secure electronic transaction (SET) protocol enables e-transactions in details. Explain the components involved.

(OR)

b) Discuss how firewalls help in the establishing a security framework for an organization.

15. a) i) Discuss the different methods involved in authentication of the source. (8)

ii) Write about how the integrity of message is ensured without source authentication. (8)

(OR)

b) i) Write the steps involved in the simplified form of the SSL/TLS protocol. (8)

ii) Write the methodology involved in computing the keys in SSL/TLS protocol. (8)

14/12/18

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

Question Paper Code : 20375

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2018.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGPAPHY AND NETWORK SECURITY

(Regulations 2013)

(Common to Electronics and Communication Engineering, Information Technology)

(Also common to PTCS 6701 – Cryptography and Network Security for B.E. (Part-Time) – Sixth Semester – Computer Science and Engineering – Regulations 2014)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Distinguish between attack and threat.
2. Calculate the cipher text for the following using one time pad cipher.
   Plain Text: ROCK & Keyword: BOTS
3. Compare DES and AES.
4. Why is trap door one way function used?
5. Define the term message digest.
6. Contrast various SHA algorithms.
7. List various types of firewall.
8. Discriminate statistical anomaly detection and rule based detection.
9. What are the services provided by PGP?
10. Differentiate transport and tunnel mode in IPSec.

PART B — (5 × 13 = 65 marks)

11. (a) Solve gcd (98, 56) using Extended Euclidean algorithm. Write the algorithm also.

Or

(b) Perform Encryption and decryption using Hill Cipher for the following.
Message PEN and Key: ACTIVATED.

12. (a) Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 88.

Or

(b) Find the secret key shared between user A and user B using Diffie Hellman algorithm for the following.

q = 353; α (primitive root) = 3, X_A = 45 and X_B = 50

13. (a) Illustrate SHA2 in detail.

Or

(b) Explain Elgamal digital signature scheme.

14. (a) Analyze various types of virus and its counter measures.

Or

(b) Illustrate the working principle of SET. Relate SET for E-commerce applications.

15. (a) Explain in detail about S/MIME.

Or

(b) Describe in detail about SSL/TLS.

PART C — (1 × 15 = 15 marks)

16. (a) Why ECC is better than RSA? However, why is it not widely used? Defend it.

Or

(b) Evaluate the performance of PGP. Compare it with S/MIME.

———————

Reg. No. :

Question Paper Code : 91409

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2019

Seventh/Eighth Semester

Computer Science and Engineering

CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering/Information Technology)

(Regulations 2013)

(Also common to PTCS6701 – Cryptography and Network Security for B.E. Part-time – Sixth Semester – Computer Science and Engineering – Regulations 2014)

Time : Three Hours

Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Define Field and Ring in number theory.
2. Consider the RSA encryption method with p = 11 and q = 17 as the two primes. Find n and ϕ (n).
3. Does the set of residue classes (Mod3) form a group
   a) With respect to modular addition ?
   b) With respect to modular multiplication ?
4. List the entities that are to be kept secret in conventional encryption techniques.
5. State the requirements of a digital signature.

6. Compare direct and arbitrated digital signature.

7. What is realm in Kerberos ?

8. List the five principal services provided by PGP.

9. In SSL and TLS, why is there a separate change_cipher_spec protocol rather than including a change_cipher_spec message in the Handshake Protocol ?

10. What entities constitute a full service in Kerberos environment ?

PART – B **(5×13=65 Marks)**

11. a) i) Explain in detail about the entities in the symmetric cipher model with their requirements for secure usage of the model. **(6)**

ii) Demonstrate that the set of polynomials whose coefficients form a field is a ring. **(7)**

(OR)

b) Write a note on different types of security attacks and services in detail. **(13)**

12. a) Explain Diffie Hellman Key exchange algorithm in detail. **(13)**

(OR)

b) Explain the working of RSA and choose an application of your choice for RSA and show how encryption and decryption is carried out. **(13)**

13. a) i) Compare the uses of MAC and Hash function. Represent them using appropriate diagrams. **(8)**

ii) List down the advantages of MD5 and SHA algorithms. **(5)**

(OR)

b) List the design objectives of HMAC and explain the algorithm in detail. **(13)**

14. a) Discuss about the components involved in e-transactions using secure electronic transaction protocol. Specify how it ensures the security during transactions. **(13)**

(OR)

b) Explain in detail about the types of firewalls and mention the design criteria of a firewall to protect the host machines in an educational institution. **(13)**

15. a) Using the PGP cryptographic functions, explain the security features offered for e-mails in detail. **(13)**

(OR)

b) Discuss in detail about IP security architecture and the services offered by IPSec. **(13)**

PART – C **(1×15=15 Marks)**

16. a) Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer amount	Cryptography functions required
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. **(15)**

(OR)

b) Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption. **(15)**

———————