MOUNT ZION COLLEGE OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

CS8792 – CRPTOGRAPHY AND NETWORK SECURITY – COACHING PLAN

UNIT I - INTRODUCTION

UNIT 1 – PRIORITY I:

- Substitution encryption techniques - Caesar cipher, Play fair cipher, Hill cipher, Vigenere cipher, vernam cipher – one time pad (Additive cipher)
- Transposition encryption techniques - Rail Fence, Row – column Transposition

PART A:

1. Define cryptography.
2. Differentiate symmetric and asymmetric encryption.
3. What are the aspects of security?
4. Compare Block and Stream cipher.
5. Decipher the following cipher Text using brute force attack: CMTMROOEOORW using Rail fence algorithm.
6. List out the components of encryption algorithm.
7. What is brute-force attack?
8. Why is asymmetric cryptography bad for huge data? Specify the reason.
9. Define cryptanalysis.
10. Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now.

PART B:

1. Given Cipher text “YMJTYMJWXNIJTKXNQJSHJ”, the message is encrypted by Caesar cipher and k=5. Try to decrypt the message.
2. Using Vigenere cipher, encrypt the word “explanation” using the Key “leg”.
3. Encrypt the following using play fair cipher using the keyword MONARCHY. Use X for blank spaces “SWARAJ IS MY BIRTH RIGHT”.
4. Solve the following using playfair cipher method. Encrypt the word “SEMESTER RESULT” with the keyword “Examination”. Discuss the rules to be followed.(APR/MAY 19)
5. Perform encryption and decryption using Hill Cipher for the following. Message: PEN and Key: ACTIVATED.
6. What is monoalphabetic cipher? Examine how it differs from Caesar cipher. NOV/DEC 20, APR/MAY 19.

7. 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. (NOV/DEC 20)
8. Encrypt the message “PAY” using rail fence with the following key matrix and show the decryption to get original plain text.

PART C:

1. Explain the rules to perform encryption using play fair cipher and encrypt ‘snowshooos’ using ‘monarchy’ I and J count as one letter and x is the filler letter
2. Encrypt the word “Semester Result” with the keyword “Examination” using playfair cipher. APR/MAY 2019.
3. Compare transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the “treat diagrams as single units” using the keyword “sequence”.

UNIT 1 – PRIORITY II:

- OSI security architecture - Security attacks, services and mechanisms
- Model of network security
- Need for Security at Multiple levels, Security Policies

PART A:

1. Define security policies.
2. Differentiate active and passive attacks.
3. List out the types of attack.
4. Define security mechanisms.
5. List four categories of security threats.
6. Define Model of network security.
7. What is the need for security at multiple levels.

PART B & C:

1. Explain OSI Security Architecture model with neat diagram.(NOV/DEC 20)
2. Explain the network security model and its important parameters with a neat block diagram. (APR/MAY 19).
3. Describe the various security mechanism.(NOV/DEC 20)
4. Describe the following.(NOV/DEC 20)
   a) Message Integrity
   b) Denial of Service
   c) Availability
   d) Authentication

UNIT 1 – PRIORITY III:

- Security trends - Legal, Ethical and Professional Aspects of Security
- Foundations of modern cryptography: perfect security – information theory, cryptanalysis

PART A:

1. State legal aspects of security.
2. Define steganography.
3. Define ethical aspects of security.
4. State professional aspects of security.
5. Define cryptanalysis.
6. What is called perfect security?

PART B & C:

1. Discuss the security trends in detail with suitable example.
2. Discuss modern cryptography in detail with necessary block diagram.

UNIT II - SYMMETRIC CRYPTOGRAPHY

UNIT II – Priority I

- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES
- AES – Advanced Encryption Standard
- Block cipher mode of operation
- Groups, Rings, Fields

PART A:

1. Define finite group.
2. Define field and ring in number theory.
3. What is the difference between a block cipher and a stream cipher?
4. State the five modes of operation of block cipher.
5. What is triple encryption? How many keys are used in triple encryption?
6. Compare DES and AES.
7. Define ring in number theory.
8. Why set of all Integers is not a field?
9. Draw the general design of S-AES encryption cipher.
10. List out the data units used in AES.

11. Define ECB.
12. List out the evaluation criteria of AES Algorithm.
13. What are the properties of ring?

PART B & C:

1. Describe AES algorithm with all its round functions in detail.(APR/MAY 19)
2. Discuss the properties that are to be satisfied by Groups, Rings and Fields.
3. What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.(NOV/DEC 20)(APR/MAY 18)
4. For each of the following elements of DES, indicate the comparable element in AES if available:(NOV/DEC 20)
   a) XOR of sub key material with the input to the function.
   b) f function

UNIT II – Priority 2

- Euclid's algorithm
- Congruence and matrices
- RC4 – Key distribution

PART A:

1. Write the Euclidean Algorithm.
2. Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm we have learned in arithmetic. Calculate q and r for a= -255 and n=11
3. Find gcd (1970, 1066) using Euclid's algorithm.
4. Define RC4 stream cipher.
5. State the need of Key-Distribution Center.

PART B & C:

1. Solve gcd(30, 65) using Extended Euclidean algorithm. Write the algorithm also.
2. How Man in the middle attack is performed on double Data encryption Standard?
3. Discuss about Public Key distribution and Symmetric-Key Distribution.

UNIT II – Priority 3

- Algebraic structures

- Modular arithmetic

PART A:

1. List the fundamental elements of abstract algebra or modern algebra.
2. Define algebraic structure.
3. State the types of algebraic structure.
4. What is called cyclic group?
5. Define subgroups.

PART B & C:

1. Describe Modulo Arithmetic operations and properties in detail.

UNIT III – PUBLIC KEY CRYPTOGRAPHY

UNIT III – Priority 1

- Chinese Remainder Theorem
- RSA cryptosystem
- Diffie Hellman key exchange

PART A:

1. Compare public key and private key.
2. State whether symmetric and asymmetric cryptographic algorithm need key exchange.
3. Give the applications of the public key cryptosystem
4. State the purpose of Diffie Hellman key exchange.
5. List out the different attacks of RSA cryptosystem.
6. Perform encryption and decryption using RSA algorithm for the following. p=7, q=11; e=17; m=8.
7. Are strong primes necessary in RSA?
8. State any one technique attacking in RSA.
9. Differentiate conventional Encryption and Public-Key Encryption.

PART B & C:

1. Describe RSA Algorithm. Perform encryption and decryption using RSA algorithm for the following: p=7 q=11, e=7, M=9.(APR/MAY 19)
2. Prove the following
   (i).If n and a are coprime, then aϕ(n) ≡ 1 (mod n).
   (ii) Use Euler's Theorem to find a number a between 0 and 9 such that a is congruent to7^1000 modulo 10. (Note that this is the same as the last digit of the decimal expansion of 7^1000.)
3. 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. (NOV/DEC 20)
4. Explain Diffie Hellman key exchange algorithm in detail.(APR/MAY 2018)
5. State Chinese Remainder theorem and find the value of X for the given set of congruent equations using Chinese Remainder theorem. (13) X ≡ l(mod 5) X ≡ 2(mod 7) X ≡ 3(mod 9) X ≡ 4(mod 11). (NOV/DEC 20)(APR/MAY 17)

UNIT III – Priority 2

- ElGamal cryptosystem
- Elliptic curve arithmetic – Cryptography
- Euler‘s totient function

PART A:

1. Define Euler’s theorem.
2. State fundamental theorem of arithmetic.
3. Define Euler’s totient function.
4. Define elliptic curve.
5. Using the properties of discrete logarithms, show how to solve the following congruence: x 2 ≡ 36 (mod 77).

PART B & C:

1. With a neat sketch explain the Elliptic curve cryptography with an example.(NOV/DEC 20)
2. Explain the Key generation, encryption, and decryption in ElGamal.
3. If p is a prime and a is a positive integer relatively prime to p, then a^p-1≡ 1(mod p)

UNIT III – Priority 3

- Primes – Primality Testing – Factorization
- Fermat‘s and Euler‘s Theorem

PART A:

1. Define the term coprime.
2. What is a primitive root of a number
3. Define Euler's totient function.
4. State Fermat's little theorem.
5. List out the properties of factorization.

PART B & C:

1. Explain public key cryptography and when it is preferred.

UNIT IV – MESSAGE AUTHENTICATION AND INTEGRITY

UNIT IV – Priority 1:

- SHA
- Digital signature and authentication protocols – Scheme
- Authentication applications - Kerberos, X.509

PART A:

1. List out the properties a digital signature.
2. Define the term message digest.
3. Give two approaches of digital signature.
4. How digital signatures differ from authentication protocols?
5. List out the security services provided by digital signature.
6. What is Kerberos? Point out its uses.
7. Assume a client C wants to communicate with a server S using Kerberos protocol. How can it be achieved?
8. State the purpose of X.509 standard.
9. List any four requirements defined by Kerberos.
10. What is the input and output range in SHA?
11. Differentiate MD4 and MD5.

PART B & C:

1. Explain SHA-1 algorithm with necessary block diagram. (APR/MAY 2017)
2. Describe digital signature algorithm and show how signing and verification is done using DSS.(APR/MAY 19)(APR/MAY 2017)
3. What is Kerberos? Explain how it provides authentication service. (APR/MAY 19)(APR/MAY 2018)

4. Briefly explain the steps of message digest generation in Whirlpool with a block diagram.(NOV/DEC 20)(APR/MAY 19)
5. Explain the format of X.509 certificate.(APR/MAY 19)
6. With a neat diagram, explain the MD5 processing of a single 512 bit blocks.(APR/MAY 18)

UNIT IV – Priority II:

- Authentication requirement
- Authentication function
- MAC – Hash function

PART A:

1. State any three requirements for authentication.
2. What is the role of compression function in hash function?
3. Define the classes of message authentication function.
4. What is called MAC?
5. How is the security of a MAC function expressed?
6. How do you specify various types of authentication protocol?

PART B & C:

1. Where hash functions are used? What characteristics are needed in secure hash function? Write about the security of hash functions and MACs.
2. Discuss the classification of authentication function in detail.
3. How Hash function algorithm is designed? Explain their features and properties.(APR/MAY 18)
4. Explain in detail message authentication code and its requirements.

UNIT IV – Priority III:

- Entity Authentication: Biometrics, Passwords
- Challenge Response protocols

PART A:

1. What is the need of entity authentication?
2. List out the cryptographic mechanisms to protect the messages in a protocol.
3. Give an example for physiological biometrics system.

PART B & C:

1. Describe Challenge-Response protocols in detail.
2. Explain the entity authentication in detail with an example.

UNIT V – SECURITY PRACTICE AND SYSTEM SECURITY

UNIT V – Priority 1:

- Electronic Mail security – PGP, S/MIME
- IP security
- Web Security

PART A:

1. Define S/MIME.
2. Define PGP.
3. List out the steps involved in SET Transactions.
4. Define SET? What are the features of SET?
5. What are the five header fields defined in MIME?
6. Differentiate transport and tunnel mode in IPsec.
7. What are the services provided by PGP?
8. What are the protocols used to provide IP security?
9. Define the term SPI.
10. List out the applications of SSL.
11. What are called IP security services?

PART B & C:

1. Describe the working of SET with neat diagram.(APR/MAY 2018)
2. With the help of a neat diagram, explain wired and wireless TLS architecture. (NOV/DEC 20)
3. Explain the architecture of IPsec in detail with a neat block diagram.(APR/MAY 19)(APR/MAY 2017)
4. Describe PGP cryptographic functions in detail with suitable block diagrams.(APR/MAY 19)(APR/MAY 2018)
5. Evaluate the performance of PGP. Compare it with S/MIME.

UNIT V – Priority 2:

- Intruders
- Firewall

PART A:

1. What is an intruder?
2. What are the three classes of intruders?
3. List out the design goals of firewall.
4. What is Threat? List their types.

5. Give the advantages of intrusion detection system over firewall.
6. Does the firewall ensure 100% security to the system? Justify.

PART B & C:

1. Discuss the role of intrusion detection system? Point out the three benefits that can be provided by the intrusion detection system? What are the three classes of intruders?
2. Explain intrusion detection system (IDS) in detail with suitable diagrams.
3. Illustrate the various types of firewalls with neat diagrams.(APR/MAY 19)
4. How does screened host architecture for firewalls differ from screened subnet firewall? Which offers more security for information assets on trusted network? Explain with a neat sketch. (APR/MAY 18)

UNIT V – Priority 3:

- Malicious software
- virus

PART A:

1. What is a virus in a computer?
2. What are the types of viruses?
3. Differentiate spyware and virus.
4. List out the malicious programs.
5. Define logic bombs.
6. What are the different phases of virus?

PART B & C:

1. Explain the different types of virus in detail. Suggest scenarios for deploying these types in network scenario.