**DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING AND TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**Seventh Semester**

**CS6701-CRYPTOGRAPHY AND NETWORK SECURITY**

**UNIT-I**

**INTRODUCTION AND NUMBER THEORY**

**PART-A**

**MOST IMPORTANT QUESTIONS**

1. **What** is Digital Signature?[APR/MAY 2015]
2. **Point** out the types of cryptanalytic attacks. [NOV/DEC 2014]
3. **Compare** Block and Stream cipher. [APR/MAY 2015][NOV/DEC 2014]
4. **Show** how to convert the given text “Anna University” into cipher text using Rail fence Technique. [MAY/JUNE 2013]
5. **Differentiate** between Active attacks and Passive Attacks [APR/MAY 2015] [MAY/JUN2014]
6. **Solve** 117 mod 13. [APR/MAY 2015]
7. **Find** GCD (21,300) using Euclidean Algorithm. [MAY/JUNE 2013]
8. **Define** primitive root. [APR/MAY 2015]

**IMPORTANT QUESTIONS**

1. **Define** Steganography. [MAY/JUNE 2013]
2. **Quote** Euler’s theorem and find the values of i) Φ (35) ii) Φ (27).[MAY/JUN2016] [MAY/JUN2014]
3. **Classify** the basic functions used in encryption algorithms. [NOV/DEC 2014]
4. **Assess** the following cipher Text using brute force attack:

CMTMROOEOORW (Hint: Algorithm-Rail fence) [NOV/DEC 2014]

**STANDARD QUESTIONS**

1. **Compare** Substitution and Transposition techniques.
2. **List** the properties of Congruences.
3. **Define** cryptography

**PART-B**

**MOST IMPORTANT QUESTIONS**

1. Explain the substitution Encryption Techniques in detail.[APR/MAY 2015] [NOV/DEC 2015] [MAY/JUNE 2013]
2. State and Describe

(i) Fermat’s theorem (8) [APR/MAY 2015] [NOV/DEC 2014] [MAY/JUNE 2013]

(ii) Eular’s theorem (8)

1. (i) **Tabulate** the substitution Techniques in detail (8)

(ii) **Describe** the Transposition Techniques in detail (8)

1. i) Explain different security mechanisms focused by OSI security Architecture.(12) [MAY/JUN 2016]

ii) **Evalute** 321 mod 11 using Fermat’s theorem. (4)

1. (i) Encrypt the message “PAY” using hill cipher with the following key matrix And show the decryption to **formulate** original plain text

 |17 17 5|

K= |21 18 21| [NOV/DEC 2014]

 |2 2 19|

1. (i) ApplyCaesar cipher and k=5 decrypt the given Cipher text

“YMJTYMJWXNIJTKXNQJSHJ”. (8)

 (ii)Apply Vigenere cipher, encrypt the word “explanation” using the key “leg”. (8)

**IMPORTANT QUESTIONS**

1. (i) **Discuss** the following
	* 1. Message Integrity (2)
		2. Denial of Service (2)
		3. Availability (2)
		4. Authentication (2)
	1. **Estimate** 1113 mod 53 using modular exponentiation. (8)
2. **(i) Solve** using playfair cipher. Encrypt the word “Semester Result” with the

Keyword “Examination”. List the rules used. (8)

(ii) Find GCD of 1070 and 1066 using Euclid algorithm. (6)

**STANDARD QUESTIONS**

1. (i) **Discuss** briefly the Discrete Algorithms. (8)

(ii) **Discuss** about the Groups, Rings and Field (8)

1. (i) **Explain** how to solve x2≡1 (mod 35) using Chinese remainder theorem. (8)

 (ii)**Explain** in detail the Euclid’s Algorithm. (8)

**UNIT-II**

**BLOCK CIPHER AND PUBLIC KEY CRYPTOGRAPHY**

**PART-A**

**MOST IMPORTANT QUESTIONS**

1. **Define** RC5.
2. **List** the five modes of operation of block cipher?
3. **Formulate** few applications of RC5 algorithm. [APR/MAY 2015]
4. **What** is the need of AES? [NOV/DEC 2015]
5. **Define** avalanche effect?
6. **Write** short notes on triple DES**.** [NOV/DEC 2015]

**IMPORTANT QUESTIONS**

1. **Give** the applications of the public key crypto systems.
2. **Explain** any one attacking technique in RSA.
3. **Discover** the Difference between public key and conventional encryption.
4. **Summarize** the purpose of Diffie Hellman key exchange.

**STANDARD QUESTIONS**

1. **Evaluate** encryption and decryption using RSA algorithm for the following P=7, q=11; e=17; m=8
2. **How** is the S-box constructed?

**PART-B**

**MOST IMPORTANT QUESTIONS**

1. Explain Data Encryption standard (DES) in detail. [APR/MAY 2015] [NOV/DEC 2015] [NOV/DEC 2014] [MAY/JUNE 2013] [MAY/JUN2014]
2. **Explain** the following modes of operation in block cipher.
3. Electronic code book and Cipher block chaining. (8)
4. Cipher feedback mode and output feedback mode. (8)
5. (i) **Formulate** the single round of DES algorithm. (10)

(ii)**Design** the key discarding process of DES. (6)

1. **(i) Evaluate** using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7.

If user A has private key XA=3.What is A’s public key YA?

(ii)If user B has private key XB=6. What is B’s public key YB?

What is the shared secret key? Also write the algorithm.

1. **Describe** RSA Algorithm in detail and for the given values trace the sequence of calculation in RSA algorithm P=7, Q=13, E=5,M=10. [APR/MAY 2015] [MAY/JUNE 2013] [MAY/JUN2014]

**IMPORTANT QUESTIONS**

1. **Apply** the mathematical foundations of RSA algorithm. Perform encryption

decryption for the following data.P=17, q=7, e=5, n=119, message=”6”. Use

Extended Euclid’s algorithm to find the private key. [NOV/DEC 2014]

1. (i) **Explain** briefly about Diffie-Hellman key exchange algorithm with its pros and cons.(8)

ii) User A and B use Diffie-Hellman key exchange a common prime q=71 and a primitive root a=7.**Calculate** the following.

If user A has private key XA=5, what is A’s public key YA. [NOV/DEC 2014]

If user A has private key XB=12, what is B’s public key YB and what is shared secret key? (8)