*Total No. of Questions: 6* *Total No. of Printed Pages:3*

**Enrollment No......................................**

# Faculty of Engineering
## End Sem Examination Dec-2023
## CB3EL05 / CB3EL13 Cryptology

Programme: B.Tech. Branch/Specialisation: CSBS

**Duration: 3 Hrs.** **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. What is the main limitation of pseudorandom bit generation? **1**
(a) The generated bit sequence is too slow to generate
(b) The generated bit sequence is too large to store
(c) The generated bit sequence is not truly random
(d) The generated bit sequence is too difficult to encrypt

ii. What are some examples of elementary cryptosystems? **1**
(a) Caesar cipher, Vigenere cipher, and Playfair cipher
(b) RSA, AES, and DES
(c) Quantum key distribution and BB84 protocol
(d) Digital signatures and hash functions

iii. Which of the following is an example of asymmetric ciphers? **1**
(a) Block cipher (b) RSA encryption
(c) AES encryption (d) Advanced cryptology

iv. What operations does ChaCha use to generate a keystream? **1**
(a) 32-bit addition, bitwise addition (XOR), and rotation operations
(b) Modular arithmetic and exponentiation
(c) Substitution and permutation
(d) Bitwise AND, OR, and NOT operations

v. How many similar rounds are there in the AES-128 algorithm? **1**
(a) 2 pairs of 5 similar rounds; every alternate
(b) 9 the last
(c) 8 the first and last
(d) 10 no

vi. What is the security of RSA based on? **1**

(a) The difficulty of factoring large composite numbers
(b) The difficulty of computing discrete logarithms
(c) The difficulty of finding prime numbers
(d) The difficulty of computing modular arithmetic

vii. What is the purpose of a hash function? **1**

(a) To encrypt data
(b) To compress data
(c) To generate random numbers
(d) To create a unique digital fingerprint of data

viii. What is the purpose of non-repudiation in digital signatures? **1**

(a) To ensure that the digital document is not tampered with
(b) To ensure that the digital document is encrypted
(c) To ensure that the digital document is compressed
(d) To ensure that the digital document is legally binding

ix. What are some applications of zero knowledge protocols? **1**

(a) Privacy and blockchain scaling
(b) Data compression and storage
(c) Encryption and decryption
(d) Digital signatures and authentication

x. What is the role of entanglement in quantum cryptography? **1**

(a) To compress the message to save storage space
(b) To encrypt the message using a secret key
(c) To generate a shared secret key between the sender and receiver
(d) To generate a digital signature for the message

Q.2 i. In the context of security services, what is the difference between an authentication and a confidentiality? **2**

ii. Generate Pseudo Random number by using MID square method while seed is given as 2315. **3**

iii. Elaborate a cryptosystem. How does it work? **5**

OR iv. Define the CIA triad. Why it is important? **5**

Q.3 i. Summarize the ZUC algorithm. **2**

ii. What are the key properties of the A5/1 encryption algorithm? **8**

OR iii. Explain Grain family and RC4 cipher. **8**

Q.4 i. What is meant by Padding? **3**

ii. What do you understand by AES? How does AES work? **7**

OR iii. Which encryption algorithm is more secure, ECC or RSA? **7**

Q.5 i. Write a note on Whirlpool. **4**

ii. Compare message digest and hash function. **6**

OR iii. State the difference between digital signature and electronic signature. **6**

Q.6 Write a short note on any two:

i. Security application **5**

ii. Key management **5**

iii. Post quantum cryptography **5**

******

# Marking Scheme

## Cryptology-CB3EL05-CB3EL13(T)

| | | | | |
|---|---|---|---|---|
| Q.1 | i) | c)The generated bit sequence is not truly random | | **1** |
| | ii) | a)Caesar cipher, Vigenere cipher, and Playfair cipher | | **1** |
| | iii) | b)RSA encryption | | **1** |
| | iv) | a) 32-bit addition, bitwise addition (XOR), and rotation operations | | **1** |
| | v) | b)9 the last | | **1** |
| | vi) | a) The difficulty of factoring large composite numbers | | **1** |
| | vii) | d) To create a unique digital fingerprint of data | | **1** |
| | viii) | d) To ensure that the digital document is legally binding | | **1** |
| | ix) | a) Privacy and blockchain scaling | | **1** |
| | x) | c) To generate a shared secret key between the sender and receiver | | **1** |
| Q.2 | i. | Authentication | 1 Mark | **2** |
| | | Confidentiality | 1 Mark | |
| | ii. | MID square formula | 1.5 Mark | **3** |
| | | Method | 1.5 Marks | |
| | iii. | Cryptosystem | 2 Marks | **5** |
| | | Working | 3 Marks | |
| OR | iv. | Define the CIA triad Why it is important | (As per explanation) | **5** |
| Q.3 | i. | ZUC algorithm | 1 Mark | **2** |
| | | definition | 1 Mark | |
| | ii. | A5/1 definition | 2 Marks | **8** |
| | | Diagram | 2 Marks | |
| | | key properties of the A5/1 | 2 Marks | |
| | | encryption decryption algorithm | 2 Marks | |
| OR | iii. | Explain Grain family and RC4 cipher | (As per explanation) | **8** |
| Q.4 | i. | Padding | (As per explanation) | **3** |
| | ii. | AES | (As per explanation) | **7** |
| OR | iii. | Algorithm | 5 Marks | **7** |
| | | Diagram | 2 Marks | |
| Q.5 | i. | Write a note on Whirlpool | 4 Marks | **4** |
| | ii. | Message Digest | 3 Marks | **6** |
| | | Hash Function | 3 Marks | |
| OR | iii. | Digital Signature | 3 Marks | **6** |
| | | Electronic Signature | 3 Marks | |
| Q.6 | | Attempt any two: | | |
| | i. | Security Application | (As per explanation) | **5** |
| | ii. | Key Management | (As per explanation) | **5** |
| | iii. | Post quantum Cryptography | (As per explanation) | **5** |

******

P.T.O.