OR	iii.	Describe the role of a hash function in verifying the integrity of a message or file.	**6**	02	01,02 03,04 05	04	01,02 03,04
Q.6		Attempt any two:					
	i.	Why is key management essential in cryptographic systems?	**5**	03	01,02 03,04 05	05	01,02 03,04
	ii.	What are the key properties of zero-knowledge proofs?	**5**	03	01,02 03,04 05	05	01,02 03,04
	iii.	What is the role of Bluetooth in contact tracing apps like those used during the COVID-19 pandemic?	**5**	03	01,02 03,04 05	05	01,02 03,04

******

Total No. of Questions: 6 *Total No. of Printed Pages:4*

Enrollment No......................................

Faculty of Engineering
End Sem Examination Dec 2024
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.

			Marks	**BL**	**PO**	**CO**	**PSO**
Q.1	i.	Integrity in the context of security means: (a) Ensuring that the data is available at all times (b) Preventing unauthorized access to the data (c) Ensuring that data has not been altered in an unauthorized way (d) Ensuring that the data is always encrypted	**1**	01	01,02 03,04 05	01	01,02 03,04
	ii.	In cryptography, what does the term "pseudo-random" refer to? (a) A truly random sequence of bits (b) A deterministic sequence that appears random (c) A sequence generated by physical noise (d) A sequence that cannot be predicted	**1**	01	01,02 03,04 05	01	01,02 03,04
	iii.	Stream ciphers are often preferred in hardware implementations due to: (a) High throughput and low complexity (b) Strong resistance against quantum attacks (c) Built-in support for public key infrastructure (PKI) (d) Ability to encrypt large data blocks	**1**	01	01,02 03,04 05	02	01,02 03,04

iv.	Which of the following stream ciphers is most commonly associated with mobile communication systems (GSM networks)? (a) Salsa (b) RC4 (c) A5/1 (d) ZUC	**1**	01	01,02 03,04 05	02	01,02 03,04
v.	Elliptic Curve Cryptography (ECC) is preferred over RSA because: (a) It offers higher security with smaller key sizes (b) It is easier to implement (c) It provides unbreakable encryption (d) It uses simpler mathematical principles	**1**	01	01,02 03,04 05	03	01,02 03,04
vi.	The Data Encryption Standard (DES) uses a key size of: (a) 128 bits (b) 64 bits (c) 56 bits (d) 192 bits	**1**	01	01,02 03,04 05	03	01,02 03,04
vii.	In the context of hash functions, what is a collision? (a) Two different hash functions producing the same output (b) Two identical inputs producing the same hash output (c) Two different inputs producing the same hash output (d) When the hash value becomes too large for storage	**1**	01	01,02 03,04 05	04	01,02 03,04
viii.	In which scenario is a digital signature particularly useful? (a) Encrypting large amounts of data (b) Providing proof of identity and ensuring message integrity (c) Compressing files for transmission (d) Storing passwords securely	**1**	01	01,02 03,04 05	04	01,02 03,04
ix.	In a public key infrastructure (PKI), which key is used to encrypt data sent to a recipient? (a) Public key (b) Private key (c) Session key (d) Symmetric key	**1**	01	01,02 03,04 05	05	01,02 03,04

	x.	In a contact tracing application, cryptographic techniques are primarily used to: (a) Track individuals' locations (b) Ensure data integrity and privacy (c) Store medical records (d) Speed up infection diagnosis	**1**	01	01,02 03,04 05	05	01,02 03,04
Q.2	i.	What is non-repudiation in security?	**2**	01	01,02 03,04 05	01	01,02 03,04
	ii.	What does availability mean in the context of security services?	**3**	03	01,02 03,04 05	01	01,02 03,04
	iii.	Why is asymmetric cryptography slower than symmetric cryptography?	**5**	02	01,02 03,04 05	01	01,02 03,04
OR	iv.	What are elementary cryptosystems?	**5**	01	01,02 03,04 05	01	01,02 03,04
Q.3	i.	What is the main difference between a stream cipher and a block cipher?	**2**	02	01,02 03,04 05	02	01,02 03,04
	ii.	What is the grain family of stream ciphers designed for?	**8**	03	01,02 03,04 05	02	01,02 03,04
OR	iii.	What is a major flaw in the RC4 algorithm?	**8**	02	01,02 03,04 05	02	01,02 03,04
Q.4	i.	What are the advantages of AES over DES?	**3**	01	01,02 03,04 05	03	01,02 03,04
	ii.	What makes ECC (Elliptic Curve Cryptography) more efficient than RSA?	**7**	03	01,02 03,04 05	03	01,02 03,04
OR	iii.	How does the DES encryption algorithm work? What are the main components of its structure?	**7**	02	01,02 03,04 05	03	01,02 03,04
Q.5	i.	Explain the role of a message digest in ensuring the integrity of data during transmission.	**4**	01	01,02 03,04 05	04	01,02 03,04
	ii.	What is a digital signature? Why is it used?	**6**	01	01,02 03,04 05	04	01,02 03,04

P.T.O.

Marking Scheme

CB3EL13 Cryptology

Q.1	i)	c. Ensuring that data has not been altered in an unauthorized way	**1**
	ii)	b. A deterministic sequence that appears random	**1**
	iii)	a. High throughput and low complexity	**1**
	iv)	c. A5/1	**1**
	v)	a. It offers higher security with smaller key sizes	**1**
	vi)	c. 56 bits	**1**
	vii)	c. Two different inputs producing the same hash output.	**1**
	viii)	b. Providing proof of identity and ensuring message integrity	**1**
	ix)	a. Public key	**1**
	x)	b. Ensure data integrity and privacy	**1**
Q.2	i.	Definition-2 marks	**2**
	ii.	Availability-1 mark, services-2 marks	**3**
	iii.	Asymmetric cryptography-2 Marks Symmetric cryptography- 2 Marks, Difference -1 Mark	**5**
OR	iv.	Elementary cryptosystems- explanation- 5 marks	**5**
Q.3	i.	Stream cipher - 1mark block cipher- 1 mark	**2**
	ii.	Grain family algorithm- 4 Marks, diagram- 2marks, description- 2 marks	**8**
OR	iii.	RC4 algorithm- 5 marks, diagram-2 marks, description -1 mark	**8**
Q.4	i.	AES -1.5 marks, DES- 1.5 marks	**3**
	ii.	ECC algorithm explanation-4 marks RSA- 3 marks	**7**
OR	iii.	DES encryption algorithm work- 4marks main components- 3 marks	**7**
Q.5	i.	Message digest description – 4 marks	**4**
	ii.	Digital signature- 3 marks, uses- 3 marks	**6**
OR	iii.	Hash function explanation- 6 marks	**6**
Q.6			
	i.	key management description - 5 marks	**5**
	ii.	key properties of zero-knowledge proofs- 5 marks	**5**
	iii.	role of Bluetooth in contact tracing app description- 5 marks	**5**

******

P.T.O.