CBCS SCHEME

USN | | | | | | | | | | |

BIS703

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.2026
Information and Network Security

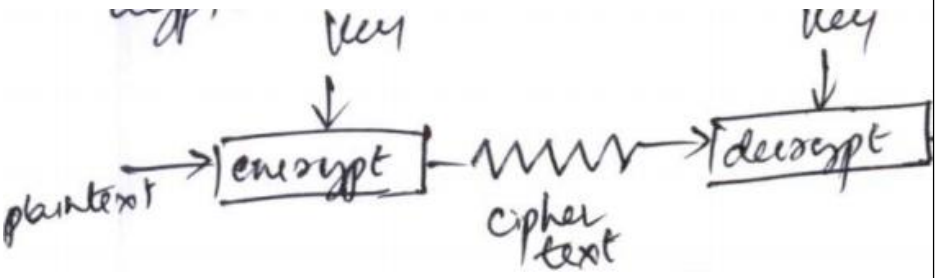
Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	M	L	C
Q.1	a.	Explain the basic terminology of crypto along with its black box.	4	L2	CO1
	b.	Explain simple substitution cipher with an example.	8	L3	CO1
	c.	Discuss double transposition cipher with an example.	8	L3	CO1
		OR			
Q.2	a.	Explain modern crypto history.	6	L2	CO1
	b.	Describe the Taxonomy of cryptography.	7	L2	CO1
	c.	Describe the Taxonomy of cryptanalysis.	7	L2	CO1
		Module – 2			
Q.3	a.	Discuss the requirements of a cryptographic hash function.	6	L2	CO2
	b.	Explain Cryptographic Tiger Hash Algorithm.	10	L3	CO2
	c.	Explain the uses of a hash function.	4	L2	CO2
		OR			
Q.4	a.	Define secret sharing. Explain the concept of secret sharing using key escrow.	10	L3	CO2
	b.	Discuss the usage of random numbers with unpredictability.	6	L2	CO2
	c.	Explain the categorization of water marks.	4	L2	CO2
		Module – 3			
Q.5	a.	Define Randomness. Differentiate between deterministic and non-deterministic generators.	10	L2	CO3
	b.	Explain the freshness mechanism in detail.	10	L2	CO3
		OR			
Q.6	a.	Explain the problems related to passwords.	4	L2	CO3
	b.	Describe the dynamic password schemes based on challenge - response.	8	L2	CO3
	c.	Explain the Diffie-Hellman key agreement protocol.	8	L2	CO3

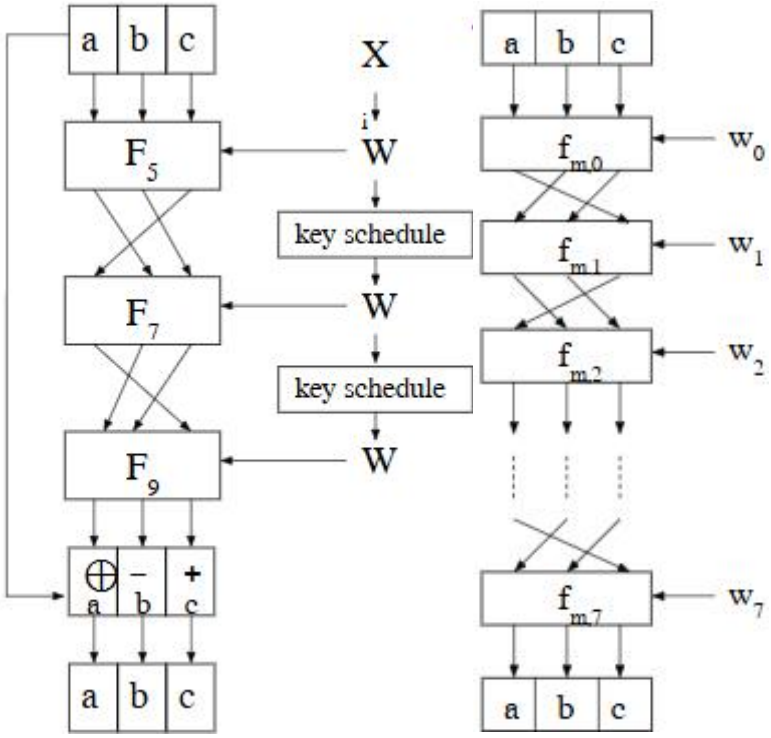
		Module – 4			
Q.7	a.	Explain the key life cycle with a neat diagram.	4	L2	CO4
	b.	Discuss key distribution approaches to acquiring shared keys from a KC.	10	L2	CO4
	c.	Explain the key storage risk factor.	6	L2	CO4
		OR			
Q.8	a.	Explain the fields of X.509 version 3 public-key certificate.	8	L2	CO4
	b.	Explain the public-key certificate management models.	12	L2	CO4
		Module – 5			
Q.9	a.	Explain simple SSL hand shake protocol.	10	L2	CO5
	b.	Discuss the SSL key management in detail.	10	L2	CO5
		OR			
Q.10	a.	Discuss WLAN design issues.	5	L2	CO5
	b.	Explain GSM and UMTS key management.	10	L2	CO5
	c.	Discuss the usage of cryptography in video broadcasting.	5	L2	CO5

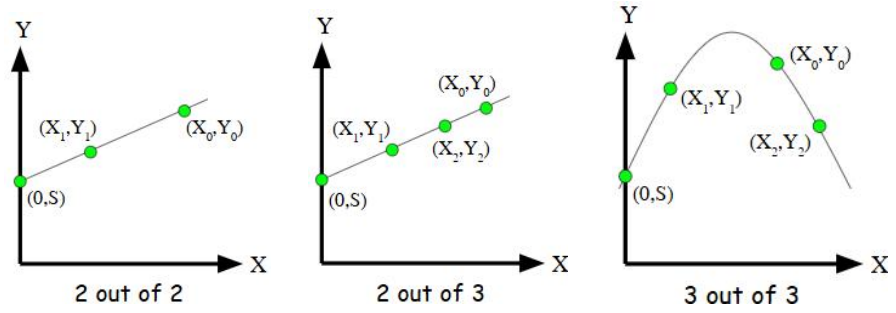
* * * * *

Sub:	**INFORMATION AND NETWORK SECURITY**	**BIS703**		
Answer any FIVE FULL Questions Choosing one full Question from each module				
Q.N	**QUESTION**	**M**	**L**	**C**
1.a	**Explain the basic terminology of crypto along with its black box.** Basic terminology : Cryptology, Cryptography, Cryptanalysis… (2m) Black box(2m):  	4m	L2	**CO 1**
b	**Explain simple Substitution Cipher with an example.** The message is encrypted by substituting the letter of the alphabet n places ahead of the current letter. For example, with n = 3, plaintext: abcdefghijklmnopqrstuvwxyz ciphertext: DEFGHIJKLMNOPQRSTUVWXYZABC **Convention:** The plaintext is lowercase, and The ciphertext is uppercase. Using the key 3, we can encrypt the plaintext message **fourscoreandsevenyearsago** The possible keys are n ∈ {0,1,2,..., 25}	8	L3	**CO 1**
c	**Discuss Double Transposition Cipher with an example.** **Encryption Procedure:** First write the plaintext into an array of a given size Then permute the rows and columns according to specified permutations Ex: **Step 1.**Write the plaintext attackatdawn into a 3 x 4 array $\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix}$ **Step 2.** Transpose (or permute) the rows according to (1,2,3) —>	8	L3	**CO 1**

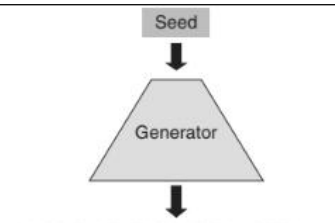
	(3,2,1) Then transpose the columns according to (1,2,3,4) —» (4,2,1,3) $\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix} \longrightarrow \begin{bmatrix} d & a & w & n \\ c & k & a & t \\ a & t & t & a \end{bmatrix} \longrightarrow \begin{bmatrix} n & a & d & w \\ t & k & c & a \\ a & t & a & t \end{bmatrix}$ The ciphertext is then read from the final array: **NADWTKCAATAT** **Decryption Procedure:** **Step 1:**The ciphertext is first put into a 3 x 4 array. **Step 2:**Then the columns are numbered as (4,2,1,3) and rearranged to (1,2,3,4) The rows are numbered (3,2,1) and rearranged into (1,2,3) $\begin{bmatrix} N & A & D & W \\ T & K & C & A \\ A & T & A & T \end{bmatrix} \longrightarrow \begin{bmatrix} D & A & W & N \\ C & K & A & T \\ A & T & T & A \end{bmatrix} \longrightarrow \begin{bmatrix} A & T & T & A \\ C & K & A & T \\ D & A & W & N \end{bmatrix}$ The double transposition does nothing to disguise the letters that appear in the message. It appears to thwart an attack that relies on statistical information contained in plaintext.			
2.a	**Explain Modern Crypto History.** Throughout the 20th century, cryptography played an important role in major world events. So-called Purple cipher was used for high level Japanese government communication. The Japanese Imperial Navy used a cipher known as JN-25. In Europe, the German Enigma cipher (code named ULTRA) was used. In the post-World War II era, Shannon offered 2 fundamental cipher design principles.  **Enigma cipher**	6	L2	**CO 1**

	Confusion: Obscurs relationship between plaintext and ciphertext: Simple Substitution *Diffusion*: It spreads plaintext statistics through ciphertext: Double Transportation In 1970's DES became an official U.S. government standard			
b	**Discuss the taxonomy of Cryptography.** Modern symmetric ciphers can be subdivided into stream ciphers and block ciphers. Generally speaking: Block ciphers are easier to optimize for software implementations Stream ciphers are usually most efficient in hardware. Why not use public key crypto for everything? *symmetric key crypto is orders of magnitude faster than public key*	7	L2	**CO 1**
c	**Describe the taxonomy of Cryptanalysis.** Includes attacks on Symmetric and Public key ciphers. A Taxonomy of Cryptanalysis **1. Cipher-only attack:** intruder has cipher text **2. Known- plaintext attack:** intruder has cipher & plain text. **3. Chosen- plaintext attack:** intruder has access to chosen cipher & plain text. Cryptanalyst can choose specific plaintext blocks to encrypt, which yield more info regarding key **4. Adaptively-chosen-plaintext attack:** special case of chosen plain text attack. Cryptanalyst can choose one large block of plaintext to be encrypted or A small block and then choose another, Based on the result of the first and so forth. **5. Chosen- cipher text attack:** analyst choose different cipher-texts to be decrypted.Analyst has access to decrypted plain text. His job is to deduce the key **6. Chosen- key attack:** Cryptanalyst has some knowledge about the relationships between keys.Its not very practical **7.Rubber-hose cryptanalysis:** Cryptanalyst threatens, blackmails or tortures someone until they give KEY. **8.Purchase-key attack: or Bribery:** These are powerful and best way to break an attack.	7	L2	**CO 1**
3.a	**Discuss the requirements of a Cryptographic Hash function.**	6	L2	**C02**

	Cryptographic Hash function h(x) must provide: **Compression** – output length is small **Efficiency** – h(x) easy to compute for any x **One-way** – given a value y it is infeasible to find an x such that h(x) = y **Weak collision resistance** – given x and h(x), infeasible to find y ≠ x such that h(y) = h(x) **Strong collision resistance** – ***infeasible*** to find ***any*** x and y, with x ≠ y such that h(x) = h(y)			
b	**Explain Cryptographic Tiger Hash function.** ✓ Hash and intermediate values are 192 bits, 24 (inner) rounds. ✓ **S-boxes:** Claimed that each input bit affects a, b and c after 3 rounds ✓ **Key schedule:** Small change in message affects many bits of intermediate hash values.  **Outer and Inner Rounds** ✓ **Multiply:** Designed to ensure that input to S-box in one round mixed into many S-boxes in next. ✓ S-boxes, key schedule and multiply together designed to ensure strong **avalanche** effect. Uses lots of ideas from block ciphers , S-	10	L3	**CO 2**

	boxes, Multiple rounds, Mixed mode arithmetic. ✓ At a higher level, Tiger employs: Confusion & Diffusion			
c	**Explain the uses of Hash function.** ✧ Authentication (HMAC) ✧ Message integrity (HMAC) ✧ Message fingerprint ✧ Data corruption detection ✧ Digital signature efficiency ✧ Anything you can do with symmetric crypto ✧ Also, many, many clever/surprising uses	4	L2	**C02**
4. a	**Describe secret sharing. Explain the concept of secret sharing using key escrow.** Shamir's Secret Sharing ➢ Two points determine a line Give (X_0,Y_0) to Alice Give (X_1,Y_1) to Bob ➢ Then Alice and Bob must cooperate to find secret S ➢ Also works in discrete case ➢ Easy to make "m out of n" scheme for any $m \leq n$  Give (X0,Y0) to Alice Give (X1,Y1) to Bob Give (X2,Y2) to Charlie ➢ Then any two can cooperate to find secret S ➢ But one can't find secret S ➢ A "2 out of 3" scheme Give (X0,Y0) to Alice Give (X1,Y1) to Bob Give (X2,Y2) to Charlie ➢ 3 pts determine parabola ➢ Alice, Bob, and Charlie must cooperate to find S ➢ A "3 out of 3" scheme	10	L3	**CO 2**

b	**Discuss the usage of random numbers with unpredictibility.** In cryptography, random numbers are needed to generate symmetric keys, RSA key pairs (i.e., randomly selected large primes), and Diffie-Hellman secret exponents. Random numbers have an important role to play in security protocols as well. Random numbers are, of course, used in many non-security applicationssuch as simulations and various statistical applications. In such cases, the random numbers usually only need to be statistically random, that is, they must be, in some statistical sense, indistinguishable from random. cryptographic random numbers must be statistically random and they must also satisfy a much more stringent requirement—they must be unpredictable.	6	L2	**CO 3**
c	**Explain the caterization of water marks.** ➢ Visible ➢ Invisible ➢ Robust ➢ Fragile	4	L2	**CO 2**
5. a	**Define Randomness. Differentiate between deterministic and non-deterministic generators.** The relationship between cryptography and randomness is extremely important.Many cryptographic primitives cannot function securely without randomness.'randomness', by its very nature, defies classification rules. A **non-deterministic** generator is based on the randomness produced by physical phenomena and therefore provides a source of 'true randomness' in the sense that the source is very hard to control and replicate. Non-deterministic generators can be based on hardware or software. Non-deterministic generators work by measuring the physical phenomena and then converting the measurements into a string of bits. A deterministic generator is an algorithm that outputs a pseudorandom bit String has no apparent structure. Anyone who knows the information that is input to the deterministic generator can completely predict the output.	10	L2	**C03**



Basic model of a deterministic generator

The two components of this model are:

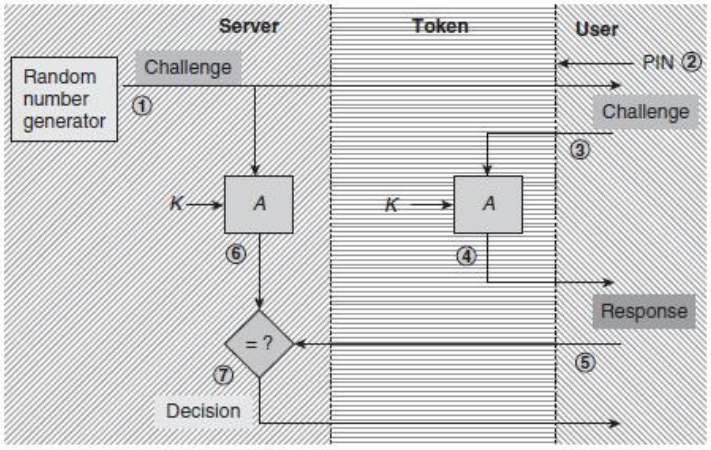
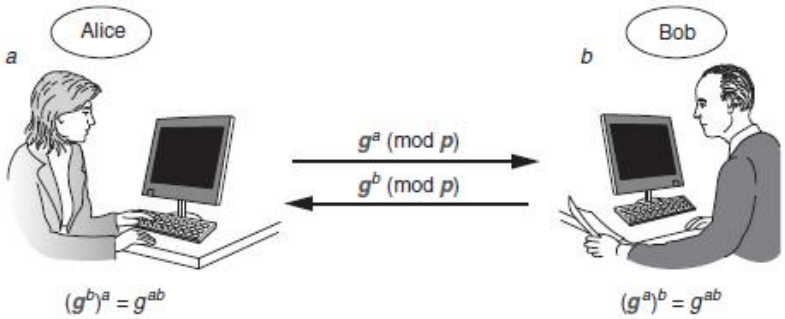
A seed. The secret information that is input into the deterministic generator is
often referred to as a seed. This is essentially a cryptographic key. The seed is
the only piece of information that is definitely not known to an attacker.

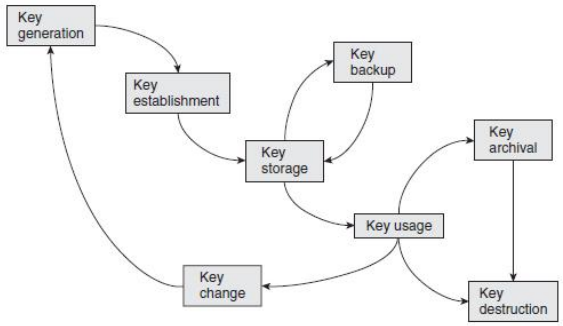
The generator. This is the cryptographic algorithm that produces the pseudo random output from the seed.

Non-deterministic generators	Deterministic generat
Close to truly randomly generated output	Pseudorandom outpu
Randomness from physical source	Randomness from a (short) ran
Random source hard to replicate	Random source easy to rep
Security depends on protection of source	Security depends on protectio
Relatively expensive	Relatively cheap

5b	**Explain the freshness mechanism in detail.** A **clock-based freshness mechanism** is a process that relies on the generation of some data that identifies the time that the data was created. This is sometimes referred to as a timestamp.Clock-based freshness mechanisms seem a natural solution, however, they come with four potential implementation problems: Existence of clocks., Synchronisation., Communication delays., Integrity of clock-based data. In applications where clock-based mechanisms are not appropriate, an alternative mechanism is to use logical time. Logical time maintains a notion of the order in which messages or sessions occur and is normally instantiated by a **counter or** **sequence numbe**r. Integrity of sequence numbers. Just as for clock-based time, an attacker who can freely manipulate sequence numbers can cause various problems in any protocol that relies on them. Thus	10	L2	**CO 3**

	sequence numbers should have some level of cryptographic integrity protection when they are sent. One problem that is shared by both clock-based mechanisms and sequence numbers is the need for some integrated infrastructure. **Nonce-based mechanisms** do not have this need. Their only requirement is the ability to generate nonces (literally, 'numbers used only once'), which are randomly generated numbers for one-off use. **Clock-based** | **Sequence numbers** | **Nonce-ba** Synchronisation needed? | Yes | Yes | No Communication delays | Window needed | Window needed | Window ne Integrity required? | Yes | Yes | No Minimum passes needed | 1 | 1 | 2 Special requirements | Clock | Sequence database | Random ger			
6	Q.6 a) Explain the problems related to passwords. Passwords are widely used for authentication, but they suffer from several problems: ● Length limitations: Humans' memory limits restrict password length, which constrains the total password space and makes exhaustive attacks more feasible. ● Complexity vs. memorability: Users prefer simpler, memorable passwords, restricting the usable password space and enabling dictionary attacks. Attempts to boost complexity often backfire usability-wise, leading to insecure practices (e.g., writing passwords down). ● Usability–security tradeoff: When users are pushed to create complex passwords, they may resort to insecure behaviors that undermine security rather than improve it. ● Repeatability: A password remains identical each use during its lifetime, so if compromised, the attacker can reuse it for as long as needed. Regular forced changes attempt to mitigate this but worsen usability and can promote poor storage habits. ● Vulnerabilities at entry and beyond: Passwords are exposed at entry (shoulder surfing), via social engineering (phishing), or through data breaches and interception (network traffic or compromised databases).	4	L2	CO3
	Q.6 b) Describe the dynamic sessions based on challenge–response. (8 marks)	8	L2	

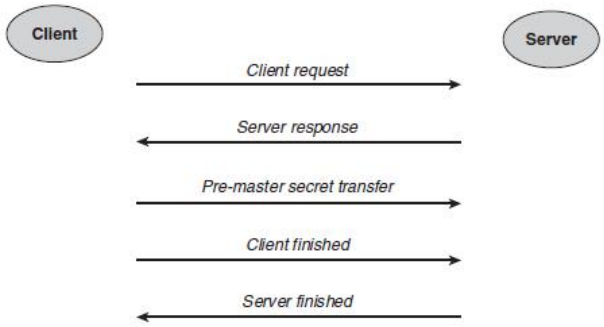
	8.5 DYNAMIC PASSWORD SCHEMES  Figure 8.3. Example of a dynamic password scheme based on challenge–response Dynamic session-based challenge–response authentication avoids sending passwords directly over the network. Working: User Identification-User sends ID to the server. Challenge Generation-Server generates a random number (challenge). Response Creation-User computes response using secret key/password and challenge. Response Transmission-Response sent to server. Verification-Server independently computes expected response. Session Key Generation-If valid, a temporary session key is created. Session Establishment-Secure session is established. Session Termination-Session expires after logout or timeout. Advantages: Prevents replay attacks Password is never transmitted			
	Q.6 c) Explain the Diffie–Hellman key agreement protocol. (8 marks)  Figure 9.10. Diffie–Hellman protocol The Diffie–Hellman key agreement protocol allows two parties to securely establish a shared secret key over an insecure channel. Steps: Publicly agree on a large prime number (p) and primitive root (g). User A selects a private key *a* and computes A=gamod pA = g^a \mod pA=gamodp.	8	L2	

	User B selects a private key *b* and computes B=gbmod pB = g^b \mod pB=gbmodp. Users exchange values A and B. User A computes shared key K=Bamod pK = B^a \mod pK=Bamodp. User B computes shared key K=Abmod pK = A^b \mod pK=Abmodp. Features: Shared key is identical for both users. Private keys are never transmitted. Provides secure key exchange over public networks.			
7	Q.7 a) Explain the key life cycle with a neat diagram. (4 marks)  Figure 10.1. The key lifecycle The key life cycle describes the stages through which a cryptographic key passes from creation to destruction. Stages of Key Life Cycle: Key Generation – Keys are created using secure algorithms and sufficient randomness. Key Distribution – Keys are securely distributed to authorized entities. Key Storage – Keys are stored securely to prevent unauthorized access. Key Usage – Keys are used for encryption, decryption, signing, or verification. Key Rotation/Update – Keys are periodically changed to reduce exposure. Key Revocation – Compromised or expired keys are revoked. Key Destruction – Keys are securely deleted when no longer required. Diagram (textual): Key Generation → Distribution → Storage → Usage → Rotation → Revocation → Destruction	4	L2	CO4
	Q.7 b) Discuss key distribution approaches to acquiring shared keys from a Key Center (KC). (10 marks) A Key Center (KC) is a trusted third party responsible for distributing secret keys securely. Key Distribution Approaches: Manual Distribution-Keys are physically delivered.Suitable for small systems.Not scalable. Key Distribution Center (KDC)-KC shares a master key with each user.Session keys are generated on request.Used in Kerberos. Online Trusted Server-Server actively participates in key exchange.Ensures	10	L2	

	freshness of keys. Public-Key Based Distribution-KC distributes session keys encrypted using public keys.Improves scalability. Hybrid Approach-Combines symmetric and asymmetric techniques.Common in SSL/TLS. Advantages: Secure, centralized control Disadvantages: Single point of failure, trust dependency			
	Q.7 c) Explain the key storage risk factor. (6 marks) Key storage risk factors refer to threats associated with improper storage of cryptographic keys. Key Risks:Unauthorized Access – Attackers gaining access to stored keys.Insufficient Protection – Storing keys in plaintext.Insider Threats – Misuse by authorized personnel.Hardware Failure – Loss of keys due to device damage.Malware Attacks – Key extraction via malicious software.Poor Backup Practices – Permanent key loss or duplication.Mitigation: Hardware Security Modules (HSMs), encryption, access control.	6	L2	
8	Q.8 a) Explain the fields of X.509 version 3 public-key certificate. (8 marks) An X.509 v3 certificate binds a public key to an entity. Fields: Version – Indicates certificate version (v3). Serial Number – Unique identifier. Signature Algorithm – Algorithm used by CA. Issuer – Certificate Authority name. Validity Period – Start and expiry dates. Subject – Entity to whom certificate is issued. Subject Public Key Info – Public key and algorithm. Extensions (v3) – Usage constraints, policies, etc. Digital Signature – CA's signature.	8	L2	CO4

Table 11.1: Fields of an X.509 Version 3 public-key certificate

Field	Description
Version	Specifies the X.509 version being used (in this case V3)
Serial Number	Unique identifier for the certificate
Signature	Digital signature algorithm used to sign the certificate
Issuer	Name of the creator of the certificate
Validity	Dates and times between which the certificate is valid
Subject	Name of the owner of the certificate
Public-Key Info.	Public-key value; Identifier of public-key algorithm
Issuer ID	Optional identifier for certificate creator
Subject ID	Optional identifier for certificate owner
Extensions	A range of optional fields that include: *Key identifier* (in case owner owns several public keys); *Key usage* (specifies usage restrictions); *Location of revocation information*; *Identifier of policy relating to certificate*; *Alternative names for owner*.

	Q.8 b) Explain the public-key certificate management models. (6 marks) Certificate Management Models: Hierarchical Model-Root CA issues certificates to subordinate CAs.Widely used (e.g., SSL/TLS). Mesh (Web of Trust) Model-Users certify each other.Used in PGP. Bridge CA Model-Connects multiple PKI hierarchies.Enables interoperability. Hybrid Model-Combination of hierarchical and mesh.	6	L2	
9	Explain simple SSL hand shake protocol. • Client request: o Sends a session ID (unique identifier for the session). o Sends a pseudorandom number rC for freshness. o Sends a list of cipher suites it supports. • Server response: o Echoes the session ID. o Provides its own pseudorandom number rS for freshness. o Chooses and returns the selected cipher suite from the client's list. o Sends the server's public-key certificate (and any certificate chain) for authentication.  Figure 12.1. Simple SSL Handshake Protocol message flow	10	L2	CO5
	Q.9 b) Discuss the SSL key management in detail. (10 marks) SSL Key Management: Authentication Keys-Server certificates verify identity. Key Exchange-RSA or Diffie–Hellman used. Session Key Generation-Symmetric keys derived from shared secret. Key Separation-Different keys for encryption and MAC. Session Resumption-Reduces overhead using session IDs. Key Expiry-Short-lived session keys for security.	10	L2	
10	Q.10 a) Discuss WLAN design issues. (5 marks) WLAN Design Issues: Main design choices: Symmetric cryptography: Used for speed (bulk traffic). Key establishment is straightforward for small setups; larger enterprise deployments may use public-key mechanisms for initial authentication, but CCMP in WPA2 relies on symmetric cryptography. Use of recognized cryptographic mechanisms: WEP relied on ad hoc designs; WPA2 adopts established, vetted algorithms. Flexibility, but constrained: Cryptographic mechanisms are largely locked	5	L2	CO5

	down for confidentiality and data origin authentication; some flexibility remains in the initial device authentication method to suit different environments. Migration considerations: WEP flaws spurred a rapid, backward-compatible fix. WPA (and WPA2) were designed to be deployed as an incremental improvement rather than a complete rewrite, enabling a smoother upgrade path.			
	Q.10 b) Explain GSM and UMTS key management. (5 marks) GSM Key Management: Uses secret key Ki stored in SIM. Authentication via challenge–response. Session key Kc used for encryption. UMTS Key Management: Mutual authentication. Stronger encryption algorithms. Multiple keys for integrity and confidentiality.	5	L2	
	Q.10 c) Discuss the usage of cryptography in video broadcasting. (5 marks) Usage of Cryptography: Content Encryption – Prevents unauthorized viewing. Access Control – Conditional access systems. Digital Rights Management (DRM) – Protects copyrights. Key Distribution – Secure delivery of decryption keys. Authentication – Verifies legitimate receivers.	5	L2	

-