USN | | | | | | | | | |

Internal Assessment Test 2 – Nov 2025 (Set 1)

Sub:	INFORMATION AND NETWORK SECURITY				Sub Code:	BIS703	Branch :	ISE
Date:	28/11/2025	Duration:	90 min's	Max Marks:	50	Sem/Sec:	VII/ A, B, C	OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1	Explain the concept of a cryptographic protocol. Discuss its purpose, operational and enviromental motivation, and components cryptographic protocol.	10M	CO3	L2

1. Definition

A **cryptographic protocol** is a structured sequence of message exchanges and cryptographic operations between entities to achieve specific security goals such as confidentiality, authentication, integrity and key establishment.

2. **Why Cryptographic Protocols Are Needed**

(a) Operational Reasons

- Real systems need **multiple security services** (e.g., confidentiality + authentication).
- Applications involve **different types of data** with different security requirements.
- Multiple entities usually participate (e.g., client, merchant, banks).
- Actions must occur in a **specific sequence** (e.g., authenticate before transmitting sensitive data).

(b) Environmental Reasons

- Devices differ in OS, hardware, software, and communication languages.
- Protocols ensure **interoperability** (similar to TCP/IP).
- Cryptographic protocols give a **standard process** for achieving security goals across diverse systems.

3. Components of a Cryptographic Protocol

1. Protocol Assumptions

- Pre-requirements before running the protocol.
- Includes key possession, trust model, strength of primitives.

2. Protocol Flow

- Order and direction of message exchanges (steps/passes).

3. Protocol Messages

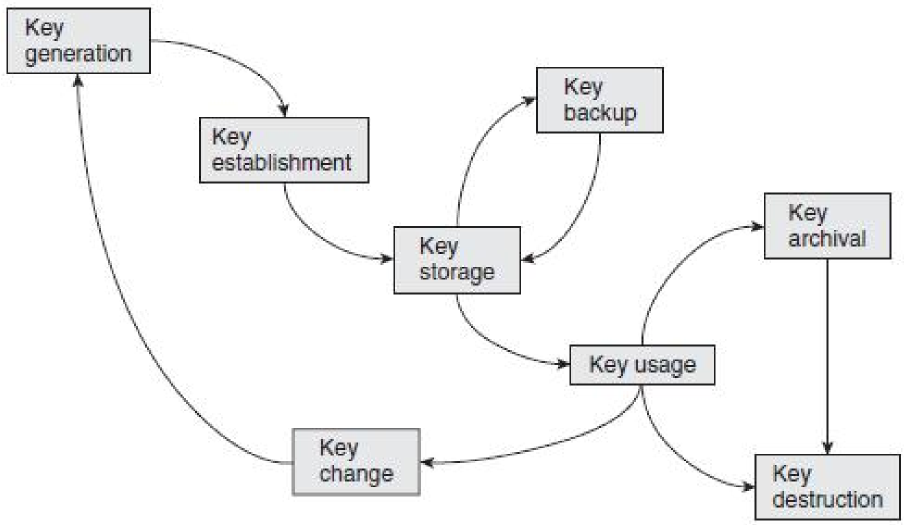
- Contents of each message: nonces, keys, IDs, timestamps, signatures, etc.

4. Protocol Actions

- Cryptographic operations performed by entities: encryption, decryption, verification, key generation, checks.

Importance of Protocol Correctness

- All messages must be well-formed and received in order.
- If any check fails → **protocol failure** → restart protocol.
- Most real security weaknesses arise from **poorly designed protocols**, not from cryptographic primitives.

2	What is key management?.Explain the key lifecycle in cryptographic systems. The scope of key management is perhaps best described as the secure administration of cryptographic keys. This is a deliberately broad definition, because key management involves a wide range of quite disparate processes, all of which must come together coherently if cryptographic keys are to be securely managed. The important thing to remember is that cryptographic keys are just special pieces of data. Key management thus involves most of the diverse processes associated with information security. These include: Technical controls. Process controls. Environmental controls. Human factors.  Figure 10.1. The key lifecycle	10M	CO4	L2
3	Discuss the importance of key separation and describe the processes of key change, key activation, and key destruction The principle of key separation is that cryptographic keys must only be used for their intended purpose. In this section we consider why key separation is a good idea and discuss options for enforcing it. THE NEED FOR KEY SEPARATION The problems that can arise if key separation is not enforced can be serious. In many applications the need for key separation may be quite obvious. For example, it may be the case that encryption and entity authentication are conducted by distinct processes, each with their own particular requirements regarding key lengths. We will see an example of when we look at WLAN security, where the process for encryption is 'locked down' across all applications, but the entity authentication process can be tailored to a specific application environment.	10M	CO4	L3

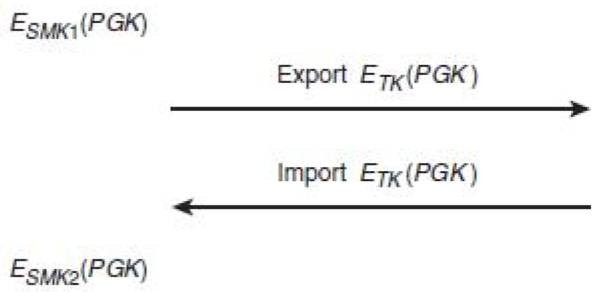


Figure 10.7. Key masquerade attack

Example 1. Like passwords, PINs should not be stored anywhere in the clear. Hence PINs are often stored in encrypted form using a symmetric PIN encrypting key. This key should only ever be used to encrypt PINs. It should never be used to decrypt an encrypted PIN. In contrast, a normal symmetric data key is used both for encryption and decryption. If these two keys are somehow interchanged within an HSM then we have two serious problems. Firstly, it may become possible to decrypt and reveal a PIN. Secondly, it may not be possible to recover any normal data encrypted with the PIN encrypting key.

Example 2. Suppose we have an HSM with the following two security functions:

Function 1. This generates a four-digit PIN for a payment card by:

1. encrypting the card's 16-digit account number using a PIN generation key, and outputting the resulting ciphertext in hex form;
2. scanning the hex output for the first four digits in the range 0 to 9, but ignoring any in the range A to F, which are then used to form the PIN (additional measures need to be taken in the unlikely event that there are insufficient digits generated using this process to form a PIN);
3. outputting the resulting PIN in encrypted form.

Function 2. This generates a MAC on some input data by:

1. computing a simple CBC-MAC (using the version of CBC-MAC depicted in Figure 6.7, which is not recommended in practice) on the input data using a MAC key;
2. outputting the MAC in hex form.

4	With a neat diagram, explain the BB84 quantum key distribution protocol. How does it detect eavesdropping during key establishment? THE BASIC IDEA Quantum key establishment takes place over a *quantum channel*. This is typically instantiated by an optical fibre network or free space. Alice and Bob must have devices capable of sending and receiving information that is encoded as quantum states, often termed *qubits*, which are the quantum equivalent of bits on a conventional communication channel. These qubits are represented by *photons*. In a conventional communication channel, one simple way of establishing a symmetric key is for Alice to generate a key and then send it to Bob. The problem with this approach is that an attacker could be listening in on the communication and thus learn the key. Even worse, neither Alice nor Bob would be aware that this has happened. The basic idea behind quantum key establishment is to take advantage of the fact that in a quantum channel such an attacker cannot 'listen in' without changing the information in the channel. This is a very useful property, which Alice and Bob can exploit to test whether an attacker has been listening to their communication. The most well known quantum key establishment protocol is the *BB84 protocol*. While the following conceptual overview of this protocol is simplified and omits important background information, it should provide a flavour of the basic idea. The BB84 protocol involves the following steps: 1. Alice randomly generates a stream of qubits, and sends these as a stream of polarised photons to Bob. 2. Bob measures them using a *polarisation detector*, which will return either a 0 or a 1 for each photon. 3. Bob contacts Alice over a conventional authenticated channel (perhaps a secure email, a telephone call, or a cryptographically authenticated channel), and Alice then provides him with information that probably results in Bob discarding approximately 50% of the measurements that he has just taken. This is because there are two different types of polarisation detector that Bob can use to measure each photon, and if he chooses the wrong one then the resulting measurement has only a 50% chance of being correct. Alice advises him over the authenticated channel which polarisation detector she used to encode each qubit, and Bob throws away the returns of all the wrongly measured photons. 4. Alice and Bob now conduct a check over the authenticated channel on the stream of bits that they think they have just agreed upon. They do this by randomly choosing some positions and then check to see if they both agree on the bits in these positions. If they find no discrepancies then they throw away the bits that were used to conduct the check, and form a key from the bits that they have not yet checked.	10M		CO4	L3

<table>
<tr>
<td>5</td>
<td>
Describe the cryptographic techniques used in securing wireless LANs such as WPA2 and WPA3. Explain how encryption and authentication protect against common wireless attacks.

A WLAN is a wireless network commonly used in offices and homes. Its operation is defined by IEEE through the 802.11 standards, first released in 1997 and updated many times since. Devices following these standards often carry the Wi-Fi trademark, indicating interoperability and compliance with IEEE 802.11.The security model for WLANs assumes that wireless networks must offer security equivalent to wired networks, except for denial-of-service resistance. Based on this, WLANs require:

Confidentiality – encryption to prevent eavesdropping.

Mutual entity authentication – both client and access point verify each other.

Data origin authentication – ensuring each frame is from the legitimate source and has not been modified.

The original 802.11 standard included WEP for protecting wireless communication at the data link layer, but WEP suffered from serious cryptographic weaknesses. In 2002, WPA was introduced as a temporary fix that improved security while remaining compatible with old hardware. Meanwhile, a complete redesign of the cryptographic components led to WPA2 in 2004 (IEEE 802.11i), which introduced strong AES-based protection and became the long-term security solution for WLANs.

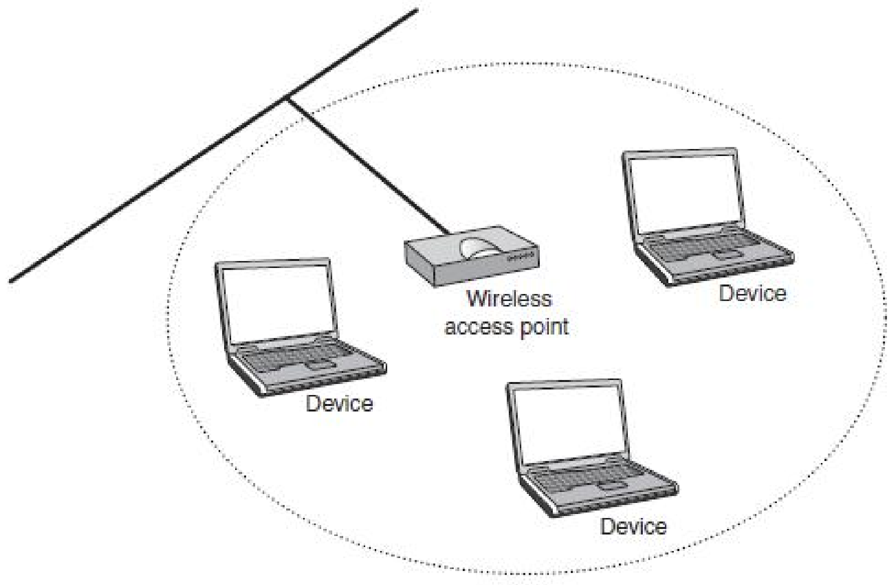
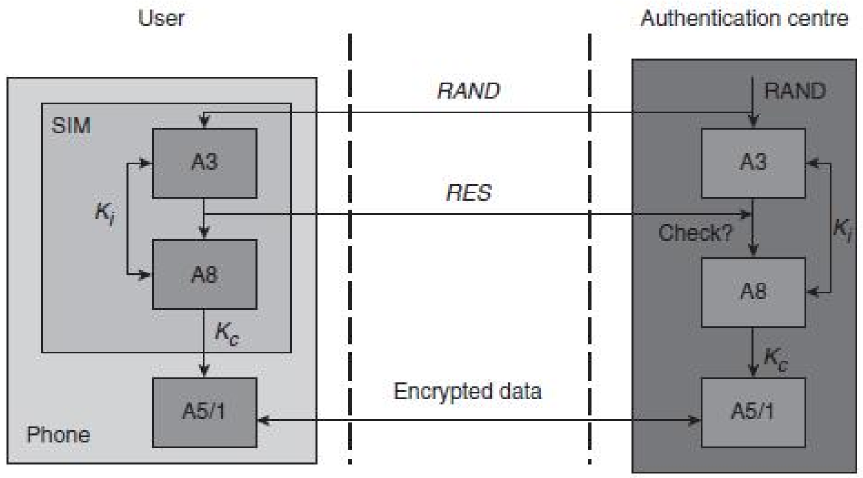


Figure 12.2. Simple WLAN architecture
</td>
<td>10M</td>
<td>CO5</td>
<td>L2</td>
</tr>
</table>

6	Explain the GSM authentication and encryption process.  Figure 12.7. GSM authentication and encryption 1. Alice sends an authentication request to Bob. 2. Bob generates a 128-bit randomly generated challenge number RAND and sends it to Alice. 3. Alice’s SIM card uses Ki and RAND to compute a response RES using algorithm A3: RES = A3Ki (RAND). The response RES is sent back to Bob. 4. Bob, who maintains a database of all the user keys, selects the appropriate key Ki for Alice and then computes the expected response in the same way. If the result matches the received RES then Alice is authenticated. 5. Alice and Bob both use Ki and RAND to compute an encryption key Kc using algorithm A8: Kc = A8Ki (RAND).	10M	C05	L2