Question no.1

Why is Message Authentication also called Data Origin Authentication?

⇨ Message authentication also known as data origin authentication is an assurance that the source of the information is indeed verified. Data origin authentication guarantees data integrity because if a source is corroborated, then the data must not have been altered. Various methods, such as Message Authentication Codes (MACs) and digital signatures are most used.

In a short, it verifies the origin of the data and ensures that it has not been tampered with during transmission.

Question no.2

Please list 4x kinds of authentications

⇨ They are:

1) Message authentication
2) Entity authentication
3) Transaction authentication
4) Key authentication

Question no.3

What is a man-in-the-middle (or more appropriately, person-in-the-middle) attack? How can Authentication resolve this attack?

⇨ A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

Question.no4

Message Authentication is usually associated with which Security Services?

⇨ Message Authentication is usually associated with the security service of Data Integrity, which is one of the fundamental security services provided by cryptographic systems. Data integrity ensures that data has not been modified, altered, or tampered with during transmission, and message authentication provides a way to verify the integrity of the data by verifying its origin and ensuring that it has not been altered by any unauthorized party.

Question.no5

Can you give me an example how to use 2x facts authentication? How about 3x facts authentication?

⇨ examples of 2-factor authentication (2FA) and 3-factor authentication (3FA):

2FA Example:

1. You log in to your bank account with your username and password.
2. The bank sends a unique code to your registered mobile phone number.
3. You enter the code to verify your identity and complete the login process.

In this example, the username and password serve as the first factor, and the unique code sent to your phone serves as the second factor of authentication.

3FA Example:

1. You log in to your company's network with your username and password.
2. The company sends a unique code to your registered mobile phone number.
3. You enter the code to verify your identity.
4. You provide a biometric scan, such as a fingerprint or facial recognition, to complete the login process.

In this example, the username and password serve as the first factor, the unique code sent to your phone

serves as the second factor, and the biometric scan serves as the third factor of authentication.