National University Of Technology

Name:	Ayesha Imran
Id :	F24605019
Date:	23rd october , 2025
Assignment:	02
Lecturer:	Lec Abtiya Ashraf
Course:	Information Security

QUESTION 1: Each time you start a new chat or reinstall WhatsApp, it generates new encryption keys. why ?

- Because new keys make your chat more secure.
- If old keys were re-used, anyone who got those keys could read new messages.
- So whatsapp makes fresh keys each time to keep every chat private and safe from past hacks.
- Simple analogy: New chat = new lock, so old keys can't open it.

QUESTION 2: Can AES use a 512-bit key ? Why or why not?

- No AES cannot use a 512-bit key.
- AES was designed to only support three key sizes: 128, 192 and 256 bits.
- These are part of it's official design standard.
- It is a fixed algorithm
- Simple Analogy: AES works only with the key sizes it was built for - 512 bits is not allowed.

QUESTION 3: Your IoT device has Low power and Little memeory. Would AES still be a good choice?

- Not the best choice.
- AES is strong but can be too heavy for small, low-power devices.
- IOT devices often use lighter algorithms like TinyAES Speck, or Simon that need less power and memory.
- Simple Analogy: Strong but big; IOT devices = small and weak → not a good match.

QUESTION 4: If AES is mathematically secure, why do data breaches still happen?

- Because hackers don't always attack the math, they attack the people or systems using it.
- Breaches happen when:

→ People use weak passwords.

→ Systems are not updated.

→ Keys are stolen, or

→ Data is exposed before encryption.

END