**Al- Mustaqbal University**

**College of Sciences**

**Department of Cybersecurity**

**Principles of Cyber Security**

**Components of encryption system**

**encryption algorithms**

**First stage**

**Lecture 7**

 **2025-2024 Lectuer : Muntather AL-Mousawi**

OB.6.3: The various ways in which cryptography is used:

* + 1. Key Ways in Which Cryptography is Used
			- Secure Communication:
				* Encryption of Messages: Cryptography is used to encrypt messages, ensuring that only authorized parties can decipher

and understand the content.

* + - * Data Integrity:
				+ Hash Functions: Cryptographic hash functions are employed to verify the integrity of data. Any change in the data will result in a different hash value, alerting users to potential tampering.
			* User Authentication:
				+ Password Protection: Cryptography helps secure user

passwords through techniques like hashing and salting, preventing unauthorized access to accounts.

* + - * Digital Signatures:
				+ Authentication of Documents: Cryptographic digital signatures provide a way to verify the authenticity and origin of digital documents, assuring that they have not been altered.
			* Virtual Private Networks (VPNs):
				+ Tunneling and Encryption: Cryptography secures data transmitted over VPNs, ensuring the confidentiality and integrity of information transferred between connected devices.
			* Secure File Storage:
				+ File Encryption: Cryptography is used to encrypt files or entire storage systems, protecting sensitive information from unauthorized access.
			* Email Security:
				+ Pretty Good Privacy (PGP): PGP employs cryptographic techniques to secure email communications, providing confidentiality, authentication, and integrity for messages.
			* Mobile Device Security:
				+ Device Encryption: Cryptography is used to encrypt data stored on mobile devices, protecting it from unauthorized access in case of loss or theft.
			* Cloud Security:
				+ Data Encryption in Transit and at Rest: Cryptography secures data both in transit to and from the cloud and when stored on cloud servers.
			* IoT Security:
				+ Device Authentication and Communication Security: Cryptography is used to secure communication and authenticate devices in the Internet of Things (IoT) ecosystem.

Class Discussion Topics

1. Discuss the core concepts of cryptography, such as encryption, decryption, and key management.
2. Discuss the limitations inherent in cryptographic algorithms, including vulnerabilities that may be exploited by advancements in mathematics or computing power.