Threats are attacks carried out. **False**

Security mechanisms typically do not involve more that one particular algorithm or protocol. **False**

Contingency planning is a functional area that primarily requires computer security technical measures. **False**

The first step in devising security services and mechanisms is to develop a security policy. **True**

Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits. **False**

Like the MAC, a hash function also takes a secret key as input. **False**

Public-key algorithms are based on simple operations on bit patterns. **False**

AES uses a Feistel structure. **False**

One desirable property of a stream cipher is that the ciphertext be of the same length as the plaintext. **True**

Key distribution can be achieved for 2 parties A and B by third party selecting the key and physically delivering it to A and B. **True**

**System integrity** assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy is a **vulnerability.**

A **passive attack** is an attempt to learn or make sue of information from the system that doesn’t affect system resources.

**Ciphertext** is the scrambled message produced as output.

On average, **¾** of all possible keys must be tried in order to achieve success with a brute-force attack.

**Message authentication** is a procedure that allows communicating parties to verify that received or stored messages are authentic.

Digital signatures and key management are the 2 most important application of **public-key** encryption.

The exact substitutions and transformations performed by the algorithm depend on the **secret key**.

The most widely used encryption scheme is based on the **DES** adopted in 1977 by the National Bureau of Standards.

**CTR** mode is typically used for general-purpose block-oriented transmission and is useful for high-speed requirements.