|  |  |
| --- | --- |
| **SESSION** | **APR 2025** |
| **PROGRAM** | **MASTER OF COMPUTER APPLICATIONS (MCA)** |
| **SEMESTER** | **III** |
| **COURSE CODE & NAME** | **DCA8143** [**CRYPTOGRAPHY AND NETWORK SECURITY**](https://learning.onlinemanipal.com/d2l/home/14210) |
|  |  |
|  |  |

**SET-I**

**Q1. Define Cryptography. Explain the fundamental goals of Cryptography. How is it different from Network Security? 3+3+4**

**Ans 1.**

**Cryptography**

Cryptography is the science and art of securing information by transforming it into an unreadable format, known as ciphertext, which can only be reverted back into readable form (plaintext) by someone who possesses the correct cryptographic key. It is primarily used to protect sensitive data from unauthorized access, particularly in communication and data storage.

Cryptography uses mathematical algorithms and encryption techniques to safeguard data. The discipline has evolved over time from simple pen-and-paper ciphers to highly complex digital

Its Half solved only

Buy Complete assignment from us

**Price – 190/ assignment**

**MUJ Manipal University Complete SolvedAssignments MARCH 2025**

buy cheap assignment help online from us easily

we are here to help you with the best and cheap help

**Contact No – 8791514139 (WhatsApp)**

**OR**

**Mail us-** bestassignment247@gmail.com

**Our website -** [www.assignmentsupport.in](http://www.assignmentsupport.in)

**Q2. Describe the working of the Caesar Cipher and Playfair Cipher with suitable examples. 10**

**Caesar Cipher**

The Caesar Cipher is one of the earliest and simplest forms of encryption. It is a substitution cipher where each letter in the plaintext is shifted a certain number of places down the alphabet. Named after Julius Caesar, who used it for military communications, the cipher works best with small-scale communication.

**How It Works**: To encrypt a message using the Caesar Cipher, each letter is replaced by another

**Q3. Discuss the principles of Public Key Cryptography. How does RSA Algorithm work? 5+ 5**

**Ans 3.**

**Principles of Public Key Cryptography**

**Public Key Cryptography**

Public Key Cryptography, also known as asymmetric cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt information. Unlike symmetric cryptography where the same key is used for both operations, public key cryptography ensures that even if the public key is widely distributed, only the corresponding private key can decrypt the message.

**Key Principles**

**1. Key Pair Generation**: Each user generates a pair of mathematically related keys – one public

**SET-II**

**Q4. Differentiate between Symmetric Key and Asymmetric Key Cryptography with examples. Also, explain the need for Key Exchange Protocols. 5+ 5**

**Ans 4.**

**Symmetric vs Asymmetric Key Cryptography and Key Exchange Protocols**

**Difference Between Symmetric and Asymmetric Cryptography**

**Symmetric Key Cryptography**: In symmetric key cryptography, the same key is used for both encryption and decryption of messages. It is a faster and simpler method, best suited for encrypting large amounts of data. However, the main drawback is the need to securely share the secret key between the sender and receiver.

**Example:**

AES (Advanced Encryption Standard) is a popular symmetric algorithm. If user A wants to send a message to user B, both must share a secret key. A encrypts the data using the key, and B

**Q5. Explain the concept and working of Digital Signatures. Why are they important in modern communication systems? 5+ 5**

**Ans 5.**

**Concept of Digital Signatures**

**Digital Signatures:** A digital signature is a cryptographic technique used to validate the authenticity and integrity of a message, software, or digital document. It works as a virtual fingerprint that uniquely identifies the sender and ensures that the content has not been altered during transmission.

Digital signatures are based on asymmetric cryptography, where a key pair (public and private

**Q6. What is a Firewall? Explain different types of Firewalls and their working. 5+ 5**

**Ans 6.**

**6. Firewalls and Their Types**

**Firewall**

**Definition and Purpose**

A firewall is a security system, either hardware-based, software-based, or a combination of both, designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

Firewalls are essential in protecting systems from unauthorized access, malware, cyber-attacks, and data breaches. They are a fundamental component of network security infrastructure and are