**PROGRAM MASTER OF COMPUTER APPLICATION (MCA)**

**SEMESTER III**

**COURSE CODE &amp; NAME DCA8143 – CRYPTOGRAPHY AND NETWORK SECURITY**

**Assignment Set – 1**

**1. Discuss the five X.800 security services.**

**Ans:** X.800 divides security services into five categories. They are:

1. Authentication

2. Access control

3. Data confidentiality

4. Data Integrity

5. Non-repudiationIts Half solved only

Buy Complete from our online store

<https://smuassignment.in/online-store/>

MUJ Fully solved assignment available for**session Feb/March 2022,**

Lowest price guarantee with quality.

Charges**INR 200 only per assignment.**For more information you can get via mail or Whats app also

Mail id is aapkieducation@gmail.com

Our website www.smuassignment.in

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

**2. What is Symmetric-key cryptography? Explain the following substitution techniques:**

**(a) Caesar cipher**

**(b) Playfair**

**(c) Polyalphabetic ciphers**

**Ans:** The sender and receiver share the same key in the symmetric-key cryptography encryption method. A single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends this ciphertext to the receiver. The receiver uses the same key (or group of rules

**3. Discuss the Data Encryption Standard (DES) algorithm and its strength in detail along with avalanche effect.**

**Ans:** Data Encryption Standard (DES) was the main encryption scheme that was used until recently. The National Bureau of Standards, now called the National Institute of Standards and Technology (NIST), adopted this standard. Since DES is now considered to be insecure for many applications, it has been replaced

**Assignment Set – 2**

**4. Discuss the RSA algorithm by taking a suitable example**

**Ans:** RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. The letters RSA are the initials of their surnames. RSA is one of the first practicable public-key cryptosystems and is widely used for securing data transmission. In this type of cryptosystem, the

**5. What do you mean by digital signature? What is the difference between a digital certificate and a digital signature? Explain.**

Another important application is the digital signature. Here the hash value of a message is encrypted with a user’s private key. Anyone who knows the user’s public key can verify the integrity of the message that is associated with

**6. Write detailed notes on:**

**a) Internet Protocol Security (IPsec)**

[IP](https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol)sec (Internet Protocol Security) is a suite of protocols and algorithms for securing data transmitted over the internet or any public network. The Internet Engineering Task Force, or IETF, developed the IPsec protocols in the mid-1990s to provide security at the IP layer through authentication and encryption of IP