Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

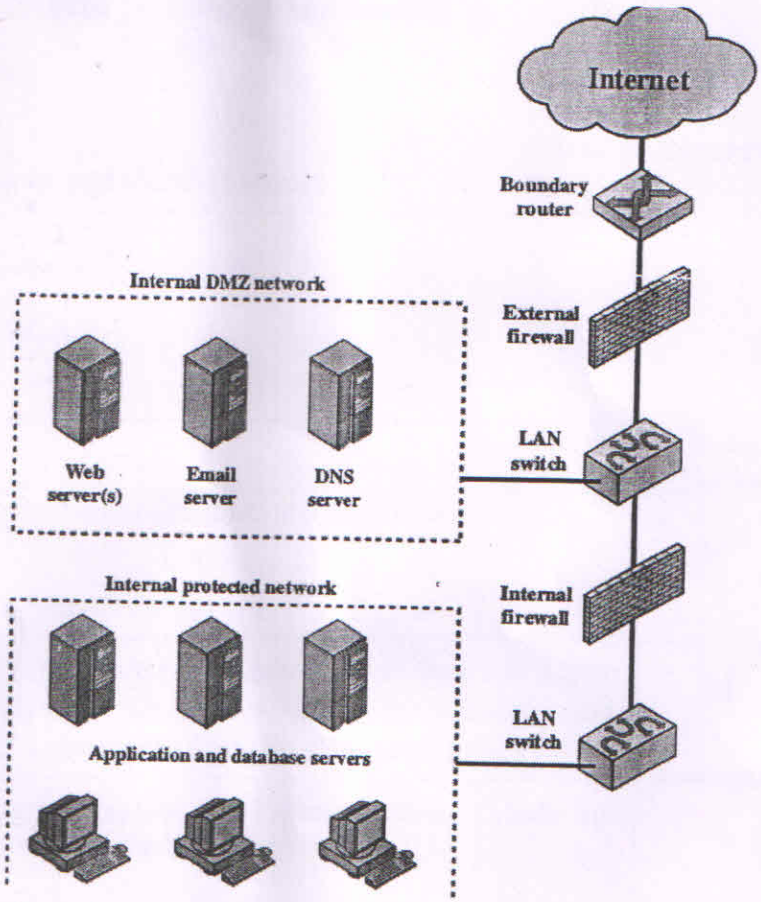
Synoptic
March 2019

Max. Marks: 20 | **Duration: 1 hr**
Class: T.E. | **Semester: VI**
Course Code: CE62 | **Branch: Computer**
Name of the Course: Cryptography and System Security

Instructions:
(1) All Questions are Compulsory
(2) Draw neat diagrams
(3) Assume suitable data if necessary

Q. No.		Mks
Q1	Types of Computer Criminals: 1. Amateurs 2. Crackers 3. Career Criminals **Marks Distribution:** State the types ---------- **01mks** Explained all three types---------- **03mks** **Diffusion:** **OR** In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by be many plaintext digits. In a binary block cipher, diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation; the effect is that bits from different positions in the original plaintext contribute to a single bit of ciphertext. ***The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.*** ***Confusion:*** **Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key.** Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex	**04**

	substitution algorithm. In contrast, a simple linear substitution function would add little confusion. **Marks Distribution:** Explained diffusion properly using the technical term ---------- **2mks** Explained confusion properly using the technical term ---------- **2mks**	
Q2	**The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique:** • Plaintext is encrypted two letters at a time. • If a pair is a repeated letter, insert filler like 'X'. • If both letters fall in the same row, replace each with the letter to its right (circularly). • If both letters fall in the same column, replace each with the the letter below it (circularly). • Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair. **Marks Distribution:** The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique------- **02mks** Problem solved correctly---------- **02mks**	**04**
Q3	**Marks Distribution:** Explained properly the Cipher Feedback Mode and Electronic Code Book modes of block ciphers with the help of diagrams---- **03mks for each mode** Explained properly the Cipher Feedback Mode and Electronic Code Book modes of block ciphers without the help of diagrams---- **02mks for each mode** **OR** **Marks Distribution:** Explained Blowfish Algorithm properly without diagram ---------- **04mks** Explained Blowfish Algorithm properly with diagram ---------- **06mks**	**06**
Q4	**DMZ Networks:** An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.	**06**



In this type of configuration, internal firewalls serve three purposes:

1. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

2. The internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Second, an internal firewall can protect the DMZ systems from attack from the internal protected network.

3. Multiple internal firewalls can be used to protect portions of the internal network from each other.

Marks Distribution:

Explained DMZ with diagram---------- **06mks**

Explained DMZ without diagram ------ **04mks**