

**Department of Computer Engineering**

**LMS Assignment 10**

Q. 1 What is a product cipher? Explain its properties confusion and diffusion with an example.

In cryptography, a product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.[1] The product cipher combines a sequence of simple transformations such as substitution (S-box), permutation (P-box), and modular arithmetic. The concept of product ciphers is due to Claude Shannon, who presented the idea in his foundational paper, Communication Theory of Secrecy Systems.

For transformation involving reasonable number of n message symbols, both of the foregoing cipher systems (the S-box and P-box) are by themselves wanting. Shannon suggested using a combination of S-box and P-box transformation—a product cipher. The combination could yield a cipher system more powerful than either one alone. This approach of alternatively applying substitution and permutation transformation has been used by IBM in the Lucifer cipher system, and has become the standard for national data encryption standards such as the Data Encryption Standard and the Advanced Encryption Standard. A product cipher that uses only substitutions and permutations is called a SP-network. Feistel ciphers are an important class of product ciphers.

[10 M]