Cryptography and Network Security: Principles and Practice, Sixth Edition - Author: William Stallings

- **Chapter-1**

□ a Challenge of Computer Security
□ CIA Confidentiality Integrity Availability
□ Definition and Types of Threat and Attack
□ Figure-1.1, 1.2

- **Chapter-2**

□ Caesar Cipher
□ Playfair Cipher
□ One Time Pad

- **Chapter-3**

□ Fiestal Structure
□ DES Encryption
□ DES Alternatives-3DES

- **Chapter-5**

□ AES-
i Byte Substitution
ii Diffusion Layer
iii What is affine mapping?