SCSA1602 - NETWORK SECURITY

Assignment – I

**Part – A**

1. \_\_\_\_\_\_\_\_\_\_\_ involve some modification of the data stream or the creation of a false stream
2. The use of mathematical algorithms to transform data into a form that is not readily intelligible is \_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_ refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract.
4. The mechanism of deciphering without knowing the enciphering details is \_\_\_\_\_\_\_
5. In \_\_\_\_\_\_\_\_\_\_\_\_attack, the attacker knows the plaintext for some parts of the ciphertext.

**Part-B**

1. Give short note on the Caser cipher?
2. What is brute force attack?
3. Encrypt the plaintext “balloon” with keyword monarchy. (Use Playfair cipher method)
4. Define Integrity and confidentiality.
5. What is symmetric cryptography.

**Part C**

1. Explain elaborately the Hill cipher with neat example. (Assume keyword and plaintext)

