Cryptography

Submission Date: Baisakh 21

Assignment 1

1. What is cryptography, cryptology and cryptanalysis?
2. What are different features/services/objectives provided by cryptography?
3. What is CIA traid? Explain.
4. Differentiate between active and passive attack with explanations of each category.
5. Explain message authentication and entity authentication.
6. What is Repudiation? Explain types of repudiation and counter measures of it.
7. What are security services and mechanisms
8. Differentiate conventional **)**symmetric**(** from public key **)**asymmetric**(**
9. Define the term keyspace. Justify the statement “Larger the keyspace , higher the security”.
10. Name any 6 block cipher schemes with their key sizes.
11. What should be considered while selecting a size of a block?
12. Encrypt the massage ‘attack from south east’ with key 'point' using vigenere cipher.
13. Encrypt the message 'hide money' with key 'tutorials' using polyalphabetic cipher.
14. Encrypt the plaintext “I study Cryptography” with the key ‘guys’ using playfair cipher.
15. Encrypt the plaintext “I study Cryptography” with depth 2 and 3 separately using Rail fence cipher.
16. what is one time pad cipher? Explain with example.
    what is Hill cipher? Encrypt the message 'paymoremoney' with key given below

17	17	5
21	18	21
2	2	9