##### Lukhdhirji engineering college

#### IT Department

Assignment list

1. Differentiate Authentication and Confidentiality with symmetric and asymmetric encryption techniques.
2. Explain Active and passive attacks.
3. Differentiate the Threat and an attack in terms of cryptography.
4. Define Categories of System security and mechanism
5. What are the two basic functions used in encryption algorithm
6. What are the two general approaches of attacking a cipher
7. What are unconditionally and computationally secure algorithms
8. What are the two problems with one time padding?
9. Differentiate Monoalphabetic and Polyaphabetic ciphers
10. Differentiate substitution and transposition with examples each.
11. What is steganography .
12. If the key for the vegeniere cipher is “Miles to go before I sleep” and the plaintext string is “Woods are more dark and deep and I have promises to keep” what would be the cipher text??
13. If the key for the playfair cipher is “Miracle “ and the string is “I cant change the direction of wind”, then find out the cipher text for it.
14. If the key for the transposition cipher is HONEST and plaintext is “Attack is postponed till tomorrow”. Find out the ciphertext for the same
15. If the key for the Hill cipher is 11 2 11

12 12 23

9 10 02

Then find out the cipher text for the plaintext “Charity begins from home”

1. For the above example retrieve the plaintext from the ciphertext and also find the inverse key to do the same

Prepared B y

Ms. Hema Dhadhal

Asst Prof in IT Dept.