UW i310

Week 3 Questions:

Rev 1/2016

1) Define cryptography (according Bishop definition)

2) What are transpositional ciphers ?

3) What are subsitutional ciphers?

4) Describe the Diffie-Hellman key exchange:

5) Briefly describe public key encryption

6) What is a replay attack - how relevant to crypto ?.

7) Key Mgmt – used for distribution of crypto keys. What mechanisms are used to bind an identity to a key ?

8) High level function of Kerberos ?

9) What is a man-in-the-middle attack - how relevant to crypto ?

10) Describe (high level) Secure Socket Layer – Transport Layer Security (TLS) ?