**Module 7 (30 points) – Chapter 8**

1. (Whitman & Mattord, 2016, p. 462) What are cryptography and cryptanalysis? What are they used for?

Cryptography is the process of securing information by using codes. Cryptoanalysis is the process of solving the cipher to get the readable message without knowing the key for the encryption. They are used to secure information and pass messages in a safe fashion.

1. (Whitman & Mattord, 2016, p. 462) What is a hash function and what can it be used for? Give an example of where a hash function is used.

Hash functions are algorithms that are used to generate a summary of a message to help confirm the message identity. An example of this would be the recipients’ signature on emails.

1. (Whitman & Mattord, 2016, p. 462) What is the fundamental difference between symmetric and asymmetric encryption? Give an example of each.

The fundamental difference between symmetric and asymmetric encryption is the number of keys that can decipher a message. The symmetric has a single key to a single cipher. Asymmetric has a public key and private key that are both able to decipher the message. An example of symmetric encryption would be DES while asymmetric would be DSA.

1. (Whitman & Mattord, 2016, p. 462) What is the difference between digital signatures and digital certificates? Are they valid forever?

Digital certificates allow the PKI system components and end users a means to validate a public key and identify its owner. Digital signatures are encrypted messages that can be used to prove authenticity. Digital certificates will last a couple of years while a digital signature is valid forever.

1. (Whitman & Mattord, 2016, p. 463) What critical issue in symmetric and asymmetric encryption is resolved by using a hybrid method like Diffie-Hellman? Name a cryptographic method where this is used.

The critical issue that is solved with the hybrid method is updating the keys, so they are not out of date. A cryptographic method that uses this is steganography.

1. (Whitman & Mattord, 2016, p. 463) Which security protocols are predominantly used in Web-based electronic commerce? Are they totally secure?

The security protocols that are predominantly used are S-HTTP, SSL, and SET. They are more secure than without, but they cannot be totally secure.

1. (Whitman & Mattord, 2016, p. 463) If you were setting up an encryption-based network, what key size would you choose and why? Would a key size of 1007 be easy to implement?

I would choose the 128-bit key as it has improved authentication and it uses more dynamic keys to overcome some problems WEP had.

**Bibliography**

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security*. Course Technology.