Intro to Cybersecurity – WK 6 Tutorial Questions

How is cryptanalysis different from brute-force attack?

Cryptanalysis is the study of different encrypting algorithm to break the code generated from those encryptions. Brute-force attack is trying every possible key until the correct one is found for the algorithm

What are the two principal requirements for the secure use of symmetric encryption?

List the two important aspects of data authentication.

What is one-way hash function?

They are functions that generate a hash that is very time consuming to reverse engineer without knowing the keys and advanced cryptoanalysis techniques

What properties must a hash function have to be useful for message authentication?

What are the principal ingredients of a public-key cryptosystem?

List and briefly define three uses of a public-key cryptosystem.

What is a public-key certificate?