Review Questions

1.1 What is the OSI security architecture?
1.2 What is the difference between passive and active security threats?
1.3 List and briefly define categories of passive and active security attacks.
1.4 List and briefly define categories of security services.
1.5 List and briefly define categories of security mechanisms.
1.6 List and briefly define the fundamental security design principles.
1.7 Explain the difference between an attack surface and an attack tree.

cryptanalysis	key distribution	

Review Questions

2.1 What are the essential ingredients of a symmetric cipher?
2.2 What are the two basic functions used in encryption algorithms?
2.3 How many keys are required for two people to communicate via a symmetric cipher?
2.4 What is the difference between a block cipher and a stream cipher?
2.5 What are the two general approaches to attacking a cipher?
2.6 Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?
2.7 What is triple encryption?
2.8 Why is the middle portion of 3DES a decryption rather than an encryption?

(ECC) MAC	public key

Review Questions

3.1 List three approaches to message authentication.

3.2 What is a message authentication code?

3.3 Briefly describe the three schemes illustrated in Figure 3.2.
3.4 What properties must a hash function have to be useful for message authentication?
3.5 In the context of a hash function, what is a compression function?
3.6 What are the principal ingredients of a public-key cryptosystem?
3.7 List and briefly define three uses of a public-key cryptosystem.
3.8 What is the difference between a private key and a secret key?
3.9 What is a digital signature?

roblems

3.1 Consider a 32-bit hash function defined as the concatenation of two 16-bit functio
which are defined in Section 3.2 as "two simple hash functions.
caused by an odd number of error b