Crypto II (A)

1) What are the two fundamental operations carried out by encryption algorithms

2) What is the basic mathematical operation used in a statistical attack on a monoalphabetic cipher

Multiple choice:

1) Which of the following is not a fundamental operation that is used in ciphers?
a) Permutation
b) Substitution
c) Multiplication
d) Transposition

2) Statistical attacks on monoalphabetic ciphers involve all of the following except
a) Correlation analysis
b) 1-grams from the English language
c) Frequency analysis of the cipher text
d) Permutation analysis of the cipher text

Crypto II (B)
1) What is the primary advantage of a polyalphabetic cipher over a monoalphabetic cipher

2) Why is the one time pad considered a perfect cipher?
3)

Multiple choice:
1) Polyalphabetic ciphers are more difficult to break than monoalphabetic ciphers because
a) The utilize different spoken languages in the cipher
b) The frequency distribution of the underlying plaintext is not preserved in polyalphabetic cipher
c) They expand the plaintext message, making the ciphertext longer in size
d) They apply complex mathematical transformations to the plaintext

2) What is a weakness of the one time pad?
a) They can only be used once and therefore waste computing resources
b) They require perfect synchronization between sender and receiver
c) They do not require any trusted exchange of secret information in advance of their use
d) They can be broken by random number generators

Crypto II (C)

1) What is the key in a transposition cipher

2) List good properties of encryption algorithms

3) What are the two types of ciphers

Multiple choice:

1) What is a popular attack mechanism for a transposition cipher?
a) Correlation analysis
b) Linear algebra techniques
c) Fourier transform analysis
d) Anagramming

2) All of the following criteria are desirable for ciphers except
a) The encryption algorithm should be free of complexity
b) The encyption algorithm itself should not be made public
c) The implementation of the encryption algorithm should be as simple as possible
d) Ciphertext should not be much larger than the size of the plaintext