Crypto III (A)

1) Why is it important that an encryption algorithm be characterized as a bijection?

2) Which of the fundametal cipher operations (substitution or transposition) does the Shift-rows operations within AES perform?

Multiple choice:

1) The following sub-functions are included in each of the rounds of AES except

a) SBOX
b) Mixcols
c) Inverse
d) Shift-rows

2) How many copies of the SBOX sub-function are needed in a fully parallelized version of the 128-bit version of AES?

a) 20
b) 16
c) 8
d) 4

Crypto III (B)
1) Mixcol carries out a mathematical operation that is described as

Multiple choice:
1) The mathematical operation carried out by mixcol sub-operation within AES is best characterized by which of the following
a) Multiplication of each column by a fixed polynomial
b) Substitution using each of the bytes in each column
c) XOR with the next round key
d) Division of each column by a fixed polynomial

2) SHA-3 is characterized as a
a) Transposition function
b) Substitution function
c) Pseudo-random function
d) Sponge function

Crypto III (C)
1) Define a length extension attack

Multiple choice:
1) HMAC is used to accomplish which of the following
a) Encrypts messages between Alice and Bob
b) Authenticates messages between Alice and Bob
c) Allows a shared secret to be derived between Alice and Bob
d) Provides non-repudiation of the message sent by Alice

2) Diffie-Hellman is used to accomplish which of the following
a) Encrypts messages between Alice and Bob
b) Authenticates messages between Alice and Bob
c) Allows a shared secret to be derived between Alice and Bob
d) Provides non-repudiation of the message sent by Alice