Sample Exam

True or False (justify all your answers: no justification → 1no grade, wrong justification11 → half grade)

a. T F The primary use of symmetric encryption is to provide confidentiality.
b. T F One very important applications of public-key cryptosystems is key management.
c. T F Message modification is a passive attack.
d. T F The encryption of “Coolness” using Caesar key “t” is “Dkcklssa”

Multiple Choice Question:

1) How many padding bits are needed in SHA-512 for a message of size 1899bits?
   a) 7 bits
   b) 14 bits
   c) 21 bits
   d) 28 bits

2) Determine if each of the 3 properties of hash functions below is true or false:
   - Given a messages *x, there can never be another message x’* where *H(x)=H(x’)*
   - It should be easy to generate *H(x)* give message *x*
   - It should be easy to generate a message *x* from a given hash *H(x)*

   a) True, True, True
   b) False, True, False
   c) True, False, False
   d) False, False, True

Answer the following questions (5pts each)

1. Using RSA, perform an encryption then a decryption of the message *M*=5 using *p=3, q=11, and e=7.*

2. Given a plaintext of size 256bits that is encrypted using DES-ECB mode, if there is a transmission error in the first transmitted cipher block (i.e. the block is received with errors during transmission NOT before encryption), how does that affect the ability of the receiver to recover *each* subsequent block? How about if the encryption mechanism was DES- CBC? *Note: assume the errors won’t be caught by any transmission protocol.*

3. Does it make sense to use a public-key cryptosystem in counter mode to achieve data confidentiality (i.e. encrypt counter using receiver’s public key and then XOR with message)? Justify your answer by drawing a diagram between Alice and Bob (and Eve if necessary) that represents a scenario where this system works OR does not work.