Crypto I (A)
1) Name the 4 tenets of information security

2) Distinguish between symmetric and asymmetric encryption

3) What is the mathematical tool called that is used to ensure data integrity and authenticity in a symmetric setting

Multiple choice:
1) The following were discussed as the basic tenets of information security except
a) Data Integrity
b) Availability
c) Non-repudiation
d) Confidentiality

2) Which of the following is false regarding symmetric and asymmetric encryption schemes
a) Asymmetric encryption uses a public-private key pair
b) Symmetric encryption uses a MAC for data integrity and authentication
c) It is not possible to attain all of the security properties associated with a cryptonium pipe
d) Symmetric encryption defines the mechanism that the two parties use to exchange the shared key

Crypto I (B)
1) What is the achilles heal of the asymmetric scheme

2) What is the technique used for data integrity and authentication in asymmetric scheme

3) What is the challenge of the symmetric scheme that doesn't exist for asymmetric scheme

Multiple choice:
1) Non-repudiation refers to
a) The inability of the sender to deny that she sent the message
b) The indisputable fact that a key exists
c) Denial-of-service
d) The ability to decrypt a message

2) The achilles heal of the asymmetric scheme
a) The huge computational burden associated with decrypting messages
b) The complex relationship between the public and private key
c) Ensuring a party is bound to a specific public key
d) The lack of a data integrity mechanism

Crypto I (C)
1) Define what a ‘commitment’ refers to in cryptography

2) What is the underlying component of the electronic form of coin flipping

3) Name the two commonly used ‘difficult-to-solve’ problems employed in cryptographic protocols

Multiple choice:
1) Other goals of cryptography include which of the following
a) Electronic form of coin flipping
b) Solving difficult mathematical problems
c) Pseudo-random number generation
d) Providing physical protection mechanisms for computing equipment

2) Why are NP problems not used in cryptographic algorithms as ‘difficult-to-solve’ problems?
a) They are only difficult to solve in some cases
b) They don’t have solutions in some cases
c) They are non-deterministic and therefore require statistical approaches
d) There is no way to formulate them for cryptographic applications