CS166 Cheating Quiz

Name _____

Student ID number _____

Notation:	$\{X\}_{\text{Alice}}$	Apply Alice's public key to X
	$[Y]_{\text{Alice}}$	Apply Alice's private key to Y
	$E(P, K)$	Encrypt P with symmetric key K
	$D(C, K)$	Decrypt C with symmetric key K
	$h(x)$	Apply the secure cryptographic hash function h to x

Directions: Read each problem carefully and provide complete but concise answers.

1. (10 points) In the context of cryptography, define the following terms.

   (a) Confidentiality

   (b) Integrity

2. (10 points) Recall that a block cipher can be viewed as a generalization of a classic codebook cipher.

   (a) In a codebook cipher, what is an *additive* and purpose does it serve?

   (b) In a modern block cipher, what is the analog of an additive? Explain.

3. (10 points)

   (a) Give the formula (or formulas) that define Feistel cipher encryption.

   (b) Give the formula (or formulas) that define Feistel cipher decryption.

4. (10 points) This problem deals with block cipher modes.

   (a) Give the formula(s) for CBC mode encryption and decryption.

   (b) Give the formula(s) used to compute a MAC.

5. (10 points) Fill in the entries in the following table with "yes" or "no".

	integrity	non-repudiation
MAC		
HMAC		
CRC		
digital signature		

6. (10 points) Suppose that Alice's RSA public key is $(N, e) = (95, e)$ and Alice's private key is $d = 5$.

   (a) Give the result when Alice digitally signs the message $M = 3$.

   (b) Determine Alice's public encryption exponent e.

7. (10 points) Suppose Bob finds a digital certificate on the Internet that contains (M, S), where $M = (\text{“Alice”}, \text{Alice's public key})$, and $S = [h(M)]_{\text{CA}}$, and “CA” is a certificate authority.

   (a) Precisely, what does Bob compute to verify the signature on the certificate?

   (b) Assuming that Bob trusts the CA, list the 2 crucial pieces of information that Bob gains by verifying the signature on the certificate.

8. (10 points) This problem deals with cryptographic hash functions.

   (a) List the 5 properties that a cryptographic hash function must satisfy.

   (b) Suppose that a secure cryptographic hash function h generates an n-bit output. According to the birthday problem, about how many hashes must you compute before you expect to find one collision?

9. (10 points) Suppose that Sally (a server) needs to share a symmetric key K_A with Alice, a symmetric key K_B with Bob, a symmetric key K_C with Charlie, and so on. Then Sally could generate the keys K_A, K_B, K_C , ... and store them in a database. An alternative is *key diversification*, where Sally generates and stores a single key K_S, with $K_A = h(\text{Alice}, K_S)$ and the keys K_B, K_C, ... being generated in a similar manner.

   (a) Give one significant advantage of key diversification as compared to storing keys in a database.

   (b) Give one significant advantage storing keys in a database as compared to key diversification.

10. (10 points) In class, we discussed a steganographic method for hiding information in uncompressed image files.

    (a) Explain in detail how this method works.

    (b) Clearly explain why this method is *not* robust.

Extra credit: (5 points) Given X, a key K, and a message consisting of three plaintext blocks, P_0, P_1, and P_2, determine an IV (in terms of X, K, P_0, P_1, and P_2) so that the MAC for this message is equal to X.