# CIS 6930– Emerging Topics in Network Security

**Assignment (100 points)**

Student Name: _____ Score: _____

1. (10 points) Assume we have a secret value x = 10. Split it into 5 shares using Shamir's (k, n) threshold scheme so that any 3 out of the 5 shares can recover x. You also need to explicitly give the recovery algorithm given any 3 shares.

2. (18 points) RSA algorithms are widely used to generate public and private key pairs. A pair of public and private key can be generated using the following steps:

* Find large primes *p* and *q* (*p*, *q* are only known to the key owner).
* Compute $n = p*q$. Let $\Phi(n)$ denote the number of prime numbers that are less than n and relatively prime to *n*. According to number theory, if *n* can be factored into the product of two prime numbers, then $\Phi(n) = (p-1)*(q-1)$.
*Choose an *e* that is relatively prime to $\Phi(n)$ (i.e., the greatest common divisor between *e* and $\Phi(n)$ is 1), and the public key = <*e*, *n*>.
* Find multiplicative inverse *d* of *e* mod $\Phi(n)$ (i.e., find *d* such that $e*d \bmod \Phi(n) = 1$), and the private key = <d, n>.

Let *e* and *d* denote the public and private key respectively. Answer the following questions:

(a) (3 points) A public key is used to encrypt a plaintext M (M < n). What is the ciphertext?

(b) (3 points) A private key is used to decrypt a ciphertext C. What is the decryption result?

(c) (3 points) Prove that the decryption result is equal to M (hint: use Fermat's Theorem: $X^Y \bmod n = X^{Y \bmod \Phi(n)} \bmod n$)

(d) (3 points) A private key is used to sign a plaintext M (M < n). What is the signature?

(e) (3 points) Prove that M = $S^e$ mod $n$, where S is the signature of M (hint: use Fermat's Theorem: $X^Y \bmod n = X^{Y \, mod \, \Phi(n)} \bmod n$)

(f) (3 points) Alice sends a message M and the message's signature S to Bob. How can Bob verify that the received M and S are really generated by the key owner? Assume that Bob knows Alice's public key.

3. (10 points) For a Diffie-Hellman key exchange, p = 7 and g = 3. If Alice sends to Bob the value 6 and Bob sends to Alice the value 5, what is Alice's private key S_A, what is Bob's private key S_B, and what is the shared secret key on which they agree?

4. (10 points) In the secret handshake protocol, the administrator has to create a pair (w, t) for each user based on a random number r. What if this random number r is reused for two different users? Assume these two users will collude.

5. (10 points) Assume Alice and Bob share a symmetric key $K_{AB}$. Also assume Alice has a pair of D-H keys, A and $g^A$, and similarly Bob has a pair of D-H keys B and $g^B$. Design a way so that Alice and Bob can run the D-H key exchange protocol without worrying about man-in-the-middle attacks. Draw a diagram to illustrate your design.

6. (12 points) You are given 8 secret messages $m_1$, … , $m_8$. Construct a Merkle Hash Tree for the authentication of these messages.

(a) (3 points) Draw the Merkle Hash Tree

(b) (3 points) Suppose a sender S uses this Merkel hash tree to authenticate these messages to a receiver R. What should be done before this tree can be used?

(c) (3 points) Describe how you can authenticate message $m_4$.

(d) (3 points) Merkle hash tree has an additional level of hash in the leaves. Is this necessary? Why?

7. (10 points) Does the hash functions in Bloom filter have to be cryptographic hash functions? Why?

8. (10 points) In the secret handshake protocol, a user uses ElGamal encryption system to encrypt a message *m*, and the encryption and decryption functions are defined below

$$\mathrm{Enc}_{PK}(m) = [c_1, c_2] = [g^m \bmod p, m \oplus H'(PK^m \bmod p)]$$

$$\mathrm{Dec}_t([c_1, c_2]) = c_2 \oplus H'(c_1^t \bmod p), \text{ where } PK = wy^{H(w,\mathrm{id})} \bmod p \text{ and } t = r + xH(w, ID)$$

Prove that $\mathrm{Dec}_t([c_1, c_2]) = m$.

9. (10 points) Juels and Brainard decided to use *m* *k*-bit sub-puzzles instead of one (*l*+*k*)-bit puzzle in their approach, where $m = 2^l$. Both options have the same expected number of trials (hash operations) to find the solution. Why did they make that decision?