Homework 3

Due April 23

1. The following is one of the discrete logarithm problem. Answer the question.

Z^*_{11} = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

P=11, a=6, b=7. Then, find x such that a^x = b mod p

In order to find x, you have to compute all power of a. Keep computing and find that this makes the cyclic group, i.e., the order is 10.

2. Given the elliptic curve

E: $y^2 = x^3 + 7x + b \mod 11$

And the point P=(4,5), determine b so that P is on E. List all points on E and find the sum (4,5) + (5,4) on E.

3. Alice's RSA public key is (N,e) = (33,3) and her private key is d=7.

(a) Let S be the result when Alice digitally signs the message M=25. What is S?

(b) If Bob receives M and S, show that the signature verification succeeds.

4. Alice uses the ElGamal digital signature. Let p=23, g=5, d=9, X=10. Suppose we use the same notation shown in the our lecture note. Alice chooses i=7.

(a) Compute the digital signature (r, s).

(b) Show that the signature verification succeeds.

5. Alice uses the DSS for digital signature. Let p=27, q=13, X=5, and H(X)=5. Choose the proper g and d(private key) and K arbitrarily.

(a) Compute the digital signature.

(b) Verify that the digital signature is correct.

6. Do the following digital signature schemes:

(a) In the RSA scheme, find the relationship between the size of S and the size of N.

(b) In the ElGamal scheme, find the r and s in relation to the size of p.

(c) In the DSA scheme, find the size of r and s in relation to the size of p and q.

7. Suppose Alice has four blocks of plaintext, P_0, P_1, P_2, P_3. She computes a MAC using key K_1, and then CBC encrypt the data using key K_2 to obtain C_0, C_1, C_2, C_3. Alice sends the IV, the ciphertext, and the MAC to Bob. However, an attacker (Cain) intercepts the message and replaces C_1 with X so that Bob receives the IV, C_0, X, C_2, C_3, and the MAC. Bob attempts to verify the integrity of the data by decrypting (using key K2) and the computing a MAC (using key K1) on the putative plaintext.

(a) Show that Bob will detect Cain's tampering.

(b) Suppose that Alice and Bob only share a single symmetric key K. They agree to let K_1=K and K_2=K$\oplus$Y, where Y is known to Alice, Bob, and Cain. Does this create any security problem?

8. Write an algorithm in pseudocode for HMAC.

9. Write an algorithm in pseudocode for CMAC.

10. Fill in the following table.

	algorithm	Security objectives(service)				Requirements for the same security level as AES-128
		Confidentiality	integrity	Authentication	Non-repudiation	
Sym. crypto	Stream cipher					
	Block cipher					
Public(Asymmetric) crypto	RSA					
	ElGamal					
	ECC					
Digital signature	RSA					
	ElGamal					
	EC-DSA					
Hash function	SHA					
MAC	Hash MAC					
	HMAC					
Authenticated encryption	CMAC					
	CCM					
	GCM					