Midterm

Name_____

1.(40pts) For each cypto algorithm, mark the security objectives related. And write the requirement for each algorithm to match the same security level of AES-128.

	algorithm	Security objectives(services)				Security level Requirement (AES-128)
		Confiden-tiality	integrity	Authenti-cation	Non-repudiation	
Sym. crypto	Stream cipher					
	Block cipher					
Public(Asymmetric) crypto	RSA					Key size
	ElGamal					Key size
	ECC					Key size
Digital signature	RSA					Signature length
	ElGamal					Signature length
	EC-DSA					Signature length
Hash function	SHA					Hash length
MAC	Hash MAC					Hash length
	HMAC					Hash length
Authenticated encryption	CMAC					
	CCM					
	GCM					

2.(20pts) Given the elliptic curve

E: $y^2 = x^3 + 2x + 3 \pmod 5$

Then the following points are on the curve

(1,1) (1,4) (2,0) (3,1) (3,4) (4,0) and ∞

(a) What is the point $P_3 = (1,4) + (3,1)$

(b) Let P = (3,1) be the generator. Suppose these E and P are used in an ECC Diffie-Hellman key exchange, where Alice chooses the secret value A = 2 and Bob chooses the secret value B=3. What value does Alice send to Bob? What does Bob send to Alice? What is the shared secret?

3(10 pts) Suppose that HMAC uses SHA-1 and the simple double hashing, H(K | H(K|X)) where K is a MAC key. As for the SHA-1 algorithm, In the SHA-1 algorithm, only consider the compression function denoted as CF() and ignore the inside operation of CF and the padding. And the Key size is the same as the message block size 512bits.

Then, based the following input values, write an algorithm in pseudocode for HMAC.

Input: N (the number of message blocks),

X[1, … , N] (N blocks of message),

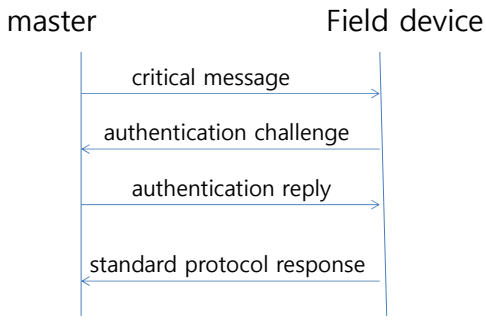
K (MAC key),

H_0(initial hash value)

4.(10pts) Alice and Bob want to communicate over a secure channel, so they want to share a secret symmetric key. How can they establish the secret key? List all possible means.

5.(20pts) There are a master station and field devices in the power substation. The master station has the following information at an initial stage: AES key(K), HMAC key(MACK) and hash algorithm(H()), device numbers(ID). The field devices also have the following information at an installation time: device number(ID), challenge sequence number(SN), random number generator, as well as AES key(K), HMAC key(MACK) and hash algorithm(H()).

(a) When the master station sends a critical message to a field device, the device wants to confirm that the message is originated from the master station and is not compromised (modified). For this purpose the device sends the challenge message to the master station and the master responds a reply to this challenge in the below. Which information do you think each message should contain?



(b) The master wants to update the HMAC key periodically. How can the master do it? Show the procedure.