UEE4611 Final Exam (Sample) ID: Name:

---

1. Suppose Alice, Bob, and Charlie are communicating using RSA encrytion. Key generation is as follows:

   1) Select two distinct primes p, q.
   2) Calculate $n = pq$.
   3) Calcuate $\phi(n) = (p-1)(q-1)$.
   4) Select integer e such that $gcd(\phi(n), e) = 1$ for $1 < e < \phi(n)$.
   5) Calculate $d = e^{-1}(\mod \phi(n))$.
   6) Public key $PU = \{e, n\}$ Private key $PR = \{d, n\}$

   Their public and private keys are as follows:

	private key$\{e, n\}$	public key$\{d, n\}$
Alice	$\{e_a, n_a\}$	$\{d_a, n_a\}$
Bob	$\{e_b, n_b\}$	$\{d_b, n_b\}$
Charlie	$\{e_c, n_c\}$	$\{d_c, n_c\}$

   Answer the following questions.

   (a) Suppose that Alice want's to send a message $M_1 < n_a$ to Bob so that no one else can see the content. What should they do? (5%)

   (b) If Charlie wants to do a broadcasting of a message $M_2 < n_c$ and makes sure that no alternation occurs. What should he do? (5%)

   (c) If Eve intercepts a ciphertext $C = 20$ sent to a Bob whose public key is $e = 13, n = 77$. What is the plaintext M? (10%)

2. Consider the elliptic curve $E_7(2, 1)$; that is, the curve is defined by $y^2 = x^3 + 2x + 1$ with a modulus of $p = 7$. It is clear that $P_1 = (0, 1)$, $P_2(1, 2) \in E_7(2, 1)$.

   (a) Determine all of the points in $E_7(2, 1)$. (5%)

   (b) What is $-P_2$? (5%)

   (c) What is $P_1 + P_2$? (5%)

   (d) What is $21P_1$? (5%)

3. Given 5 as a primitive root of 23, solve the following congruence:

$$5^x \equiv 6 \pmod{23}.$$

   (10%) (Hint: you may want to construct the table of discrete logarithms first.)

4. Consider the following random number generator

$$X_{n+1} = (aX_n) + c \mod m,$$

   where a, c, m are integers.

   (a) It is known that the linear congruential algorithm is not cryptographically secure. Suppose that the opponent is able to determine four consectuive values for $X_0 = 17$, $X_1 = 10$, $X_2 = 15$, and $X_3 = 7$. Then what is the next value? (10%)

   (b) In the special case that m is a prime, $c = 0$, and a is a primitive root of m, the period of this random number generator is $m - 1$. Suppose now we replace a by a^k for $1 < k < m$ and $gcd(k, m - 1) = 1$. What is the period of this new generator? Please justify your answer. (10%)

(***See the next page for more problems.***)

5. (Elegamal cryptosystem) Global parameters: a prime number q and its primitive root α.
   Alice's key generation

   - Select private key X_A: $X_A < q - 1$.
   - Calculate public key $Y_A = \alpha^{X_A} \mod q$.

   Encryption with Alice's public key:

   - Plaintext: $M < q$
   - Select random integer $k < q$
   - Calculate $K = (Y_A)^k \mod q$
   - Ciphertext: $(C_1 = \alpha^k \mod q, C_2 = KM \mod q)$

   Decryption by Alice with Alice's Private Key

   - Calculate $K = (C_1)^{X_A} \mod q$
   - Plaintext: $M = (C_2 K^{-1}) \mod q$

   Bob sends a ciphertext $(11, 5)$ to Alice. What's the plaintext? (10%)

6. In this problem we consider using an encryption algorithm to construt a hash function or a MAC function.

   (a) (Hash function) Suppse $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is an encryption that takes as input an n-bit key and an n-bit message and outputs an n-bit ciphertext. Fix a known key $K \in \{0,1\}^n$. Now we define a hash function $H : \{0,1\}^{2n} \to \{0,1\}^n$ by $H(M_1||M_2) = E(K, E(K, M_1) + M_2)$ for $M_1, M_2 \in \{0,1\}^n$, where the addition is bitwise modulo 2. However, this hash function does not satisfy the requirements of a cryptographically secure hash function. Find one violation of the requirement by giving an example. (10%)

   (b) (MAC) Suppse $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$ is an encryption that takes as input an k-bit key and an n-bit message and outputs an n-bit ciphertext. Now we define a MAC function $EMAC : \{0,1\}^{2n} \to \{0,1\}^{2n}$ by $EMAC(M_1||M_2) = E(K, M_1)||E(K, E(K, M_2))$ for $M_1, M_2 \in \{0,1\}^n$, where the addition is bitwise modulo 2. Now suppose K is a shared key between two parties. However, this MAC function is insecure. Prove it. (10%) (Hint: you may query several messages and get their tags. Then you have to conceive a message with its tag.)