NAME (PRINT): ______________________________ ______________________________
Last/Surname First/Given Name

STUDENT #: ______________________ **SIGNATURE:** ______________________

UNIVERSITY OF TORONTO MISSISSAUGA
APRIL 2012 FINAL EXAMINATION

MAT302H5S
Introduction to Algebraic Cryptography
Vinod Vaikuntanathan

Duration - 3 hours
Aids: 01 page(s) of double-sided Letter (8-1/2 x 11) sheet

The University of Toronto Mississauga and you, as a student, share a commitment to academic integrity. You are reminded that you may be charged with an academic offence for possessing any unauthorized aids during the writing of an exam, including but not limited to any electronic devices with storage, such as cell phones, pagers, personal digital assistants (PDAs), iPods, and MP3 players. Unauthorized calculators and notes are also not permitted. Do not have any of these items in your possession in the area of your desk. Please turn the electronics off and put all unauthorized aids with your belongings at the front of the room before the examination begins. If any of these items are kept with you during the writing of your exam, you may be charged with an academic offence. A typical penalty may cause you to fail the course.

Please note, you **CANNOT** *petition to* **re-write** *an examination once the exam has begun.*

Marks:

P1	P2	P3	P4	P5	Total
/10	/15	/30	/20	/25	/100

Problem 1: True or False (10 Marks)

Please circle the correct answer.

(a) Finding discrete logarithms over $\mathbb{Z}_N^*$ for a large composite number N is computationally easy, given the prime factorization of N. TRUE FALSE

(b) The following is a valid 2-out-of-3 secret sharing of a number $K \in \mathbb{Z}_{19}$: TRUE FALSE

$$s_1 = 5, \quad s_2 = 14, \quad s_3 = 3$$

Problem 2: Do you know your Crypto? (15 Marks)

Consider the El Gamal encryption scheme that works over $\mathbb{Z}_p^*$ where the prime $p = 17$. Let the El Gamal secret key $x = 8$.

1. **(10 marks)** Find a generator g of $\mathbb{Z}_{17}^*$. Use the generator to determine the public key corresponding to the secret key $x = 8$.
2. **(5 marks)** Illustrate how the El Gamal encryption and decryption algorithms work for a message $M = 7 \in \mathbb{Z}_{17}^*$.

Problem 3: Chinese Remaindering and RSA (30 Marks)

Let $N = 221$ be a product of two primes, namely 17 and 13.

1. **(5 Marks)** What is $\phi(N)$?
2. **(5 Marks)** Exactly one of the two possibilities $e = 3$ and $e = 5$ is a valid RSA exponent for the modulus $N = 221$. Which one is it? Explain the reasoning behind your answer.
3. **(10 Marks)** Let e be the valid RSA modulus from part (2). Let d_p and d_q be numbers such that

$$ed_p = 1 \pmod{p-1} \text{ and}$$
$$ed_q = 1 \pmod{q-1}$$

Moreover, let

$$M_p = C^{d_p} \pmod{p} \text{ and}$$
$$M_q = C^{d_q} \pmod{q}$$

Let M be the message encrypted in C. Show that $M = M_p \pmod{p}$ and $M = M_q \pmod{q}$.

4. **(10 Marks)** Assume that you are given a (vanilla) RSA ciphertext $C = 86 \pmod{221}$. Let e be the valid RSA modulus from part (2). Compute numbers d_p, d_q, M_p and M_q that satisfy the equations in part (3). Then, use Chinese remaindering to reconstruct the message M encrypted under RSA.

Problem 4: Zero Knowledge (20 Marks)

1. **(10 marks)** Describe a zero knowledge protocol to prove that a given number $y \in \mathbb{Z}_N^*$ is a square modulo N (where N is some natural number). In particular, clearly describe what the prover and the verifier do, and the messages exchanged in the protocol.

2. **(10 marks)** Here is a protocol between a prover Peggy and a verifier Victor to prove that a given natural number N is strongly composite (namely, it is neither a prime p nor a prime power p^e). Assume that both Peggy and Victor know N, but only Peggy knows the factorization of N.

   The protocol proceeds as follows:

   (a) (Victor sends to Peggy) Victor picks a random number $x \in \mathbb{Z}_N^*$ computes $y = x^2 \pmod{N}$ and sends y to Peggy.

   (b) (Peggy responds to Victor) Peggy finds a number z such that $y = z^2 \pmod{N}$ and sends it back to Victor.

   Victor checks that $y = z^2 \pmod{N}$ and that $z \neq \pm x \pmod{N}$. If this checks out, he accepts Peggy's proof. Otherwise, he rejects.

   If N is indeed neither a prime nor a prime power, there are at least four square roots of $y \pmod{N}$. Peggy will send one that is neither x nor $-x$ with probability $1/2$, in which case Victor will accept Peggy's proof. On the other hand, if N is a prime or a prime power, then x and $-x$ are the only two square roots of y mod N, thus Victor will never accept Peggy's proof.

   It turns out, though, that this protocol is not zero-knowledge. In particular, after talking to Peggy, Victor will know the factorization of N. Why?

Problem 5: Secret Sharing (25 Marks)

1. **(5 Marks)** Describe how the Shamir t-out-of-N secret sharing scheme works. Illustrate this by producing a 3-out-of-4 sharing of the secret $K = 9$ over the group $\mathbb{Z}_{13}$.

2. **(5 Marks)** Given three shares $s_1 = 1$, $s_2 = 12$ and $s_4 = 9$ in a 3-out-of-4 secret sharing scheme over $\mathbb{Z}_{13}$, what is the secret K?

3. **(15 Marks)** A secret is shared among nine people $\{A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3\}$, divided into three groups of three each (the A-group, the B-group and the C-group).

   Your goal is to come up with a way of sharing the secret such that if all three of the A's, any two of the B's AND any one of the C's come together, they can reconstruct the secret. In all other cases, the secret should remain completely hidden.

   For example, the set $\{A_1, A_2, A_3, B_2, B_3, C_3\}$ should be able to recover the secret. On the other hand, the set $\{A_1, A_2, B_1, B_2, B_3, C_1, C_2, C_3\}$ should NOT be able to recover any information about the secret.

   Assume that the key is a number in $\mathbb{Z}_q$ for some prime number q.