NAME (PRINT): ____

Last/Surname First/Given Name

STUDENT #: ____________________ **SIGNATURE:** ____________________

UNIVERSITY OF TORONTO MISSISSAUGA
APRIL 2012 SPECIAL DEFERRED 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 (/10)	P2 (/10)	P3 (/10)	P4 (/15)	P5 (/30)	P6 (/25)	Total (/100)

Problem 1: True or False (10 Marks)

Please circle the correct answer.

(a) There are odd numbers N for which $N-1$ is a Fermat Witness.

TRUE FALSE

False. $N-1=-1 \pmod{N}$ is always a Fermat Liar for N since $(-1)^{N-1}=1 \pmod{N}$.

(b) Alice claims that she shared a number $K \in \mathbb{Z}_{11}$ into five shares

TRUE FALSE

$$s_1=5,\ s_2=8,\ s_3=0,\ s_4=4,\ s_5=6$$

using a 2-out-of-5 Shamir secret sharing scheme. This is indeed a valid 2-out-of-5 secret sharing.

False. The points $(1,5)$, $(2,8)$, $(3,0)$, $(4,4)$, $(5,6)$ do not lie in a line, as they should if the s_i are valid Shamir shares.

Problem 2: Do you know your Crypto? (10 Marks)

Alice and Bob run the Diffie-Hellman Key Exchange Protocol with the following parameters: a prime $p=37$, a generator $g=2$ for $\mathbb{Z}_{37}^*$, and exponents $x_A=9$ for Alice, and $x_B=11$ for Bob. What are the messages that Alice and Bob send to each other, and what is the shared key? (I expect answers as concrete numbers in $\mathbb{Z}_{37}^*$ and not, say, of the form a^b).

Problem 3: Chinese Remaindering (10 Marks)

Find all integers that leave a remainder of 3 when divided by 5, a remainder of 5 when divided by 7, and a remainder of 7 when divided by 11.

A straightforward application of Chinese Remainder Theorem gives us $x=348+385y$ for any $y \in \mathbb{Z}$.

$x=3 \pmod{5} \Rightarrow x=3+5y$ for some integer y.
$x=3+5y=5 \pmod{7} \Rightarrow y=-1 \pmod{7}$, and $x=-2+35z$ for some integer z.
$x=-2+35z=7 \pmod{11} \Rightarrow z=-1 \pmod{11}$, and $x=-37+385w$ for some integer w.

We thus get the claimed answer.

Problem 4: Primality Testing and Factoring (15 Marks)

Is $2^{35} - 1$ prime?
`(Hint: Use the fact that 35 is composite, and consider the polynomial` $x^{rs}-1$`.)`

Note that $x^{rs} - 1 = (x^r - 1)(x^{r(s-1)} + x^{r(s-2)} + \ldots + 1)$. This says that $x^r - 1$ is a factor of $x^{rs} - 1$. Thus, a factor of $2^{35} - 1$ is $2^5 - 1 = 31$. Also, $2^7 - 1 = 127$.

Problem 5: Elliptic Curves (30 Marks)

Consider the elliptic curve $E : Y^2 = X^3 + X \pmod 7$.

1. **(10 marks)** What are the points on the curve?

   The squares in $\mathbb{Z}_7^*$ are $1, 2$ and 4.

   The points on the curve are { $\mathcal{O}$, (0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5) }

2. **(5 marks)** What is / are the identity elements in the elliptic curve group generated by these points?

   The point at infinity $\mathcal{O}$.

3. **(15 marks)** $P = (1, 3)$ is a point on this curve. What is its order?

   We know that the order of any point divides the order of the group, namely 8. Since $P \neq \mathcal{O}$, the order is 2, 4 or 8. Let us try computing $2P$, $4P$ and $8P$ where $P = (1, 3)$.

   For $2P$: The tangent at $(1, 3)$ of the curve has slope

   $$\lambda = (3x_1^2 + A)(2y_1)^{-1} \pmod 7 = 4 \cdot 6^{-1} \pmod 7 = 3 \pmod 7$$

   The tangent line, thus, is $y = 3x \pmod 7$. Thus, $x_3 = \lambda_1^2 - 2x_1 = 0 \pmod 7$, and $y_3 = 0 \pmod 7$. Thus, $2P = (0, 0)$.

   For $4P$: Let us compute $(0, 0) \oplus (0, 0)$. The tangent at $(0, 0)$ of the curve has slope $\lambda = (3x_1^2 + A)(2y_1)^{-1} \pmod 7$, which is undefined. Thus, $(0, 0) \oplus (0, 0) = \mathcal{O}$, the point at infinity.

   The consequence being, $4P = \mathcal{O}$, and the order of P is 4.

Problem 6: Secret Sharing (25 Marks)

1. **(10 Marks)** Describe how the Shamir t-out-of-N secret sharing scheme works, for arbitrary numbers N and $t \leq N$. Illustrate this by producing a 2-out-of-5 sharing of the secret $K = 6$ over the group $\mathbb{Z}_{11}$.

   Refer to your notes.

2. **(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 at least two representatives from at least two groups come together, they will be able to recover the secret. In all other cases, the secret should remain completely hidden.

   For example, the set $\{A_1, A_2, C_2, C_3\}$ should be able to recover the secret since it has two members from the A-group and two from the C-group. On the other hand, the set $\{A_1, A_2, A_3, B_1, C_1\}$ should NOT be able to recover the secret since it has only one member from the B-group and the C-group.

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

   [`Hint:` *Try to think of a "hierarchical" solution.*]

   Here is a solution: Think of first secret sharing K among three "virtual groups", namely the A group, the B group and the C group. That is, compute 2-out-of-3 shares (s, t, u) of K.

   (One way to do this (following what we did in class) is to choose a random line $y = mx + K$, where m is a random number in $\mathbb{Z}_q$ and K is the secret, and set $a = m \cdot 1 + K$, $b = m \cdot 2 + K$ and $c = m \cdot 3 + K$.)

   Now, secret share each of these numbers again using a 2-out-of-3 secret sharing scheme. That is,

   - compute three shares a_1, a_2 and a_3 of the "secret" a (as before). Give a_1 to A_1, a_2 to A_2 and a_3 to A_3.
   - compute three shares b_1, b_2 and b_3 of the "secret" b (as before). Give b_1 to B_1, b_2 to B_2 and b_3 to B_3.
   - compute three shares c_1, c_2 and c_3 of the "secret" c (as before). Give c_1 to C_1, c_2 to C_2 and c_3 to C_3.

   The point is this: let's say two people from any group come together, for example groups A and B. They can together reconstruct a and b (in this example) since they have two shares each for the "secrets" a and b. Given a and b, they can also reconstruct K.

   On the other hand, if say three people from the A group and one person each from the B and C group come together, they can together reconstruct a, but not b or c. Now, given only a, they have no information about what the original secret K is!