Indian Institute of Technology Kharagpur

AUTUMN Semester, 2016
COMPUTER SCIENCE AND ENGINEERING
CS60065: Cryptography and Network Security
End semester Examination

Full Marks: 60

Time allowed: 3 hours

INSTRUCTIONS: This exam is closed book and closed notes. Calculators are allowed. This question paper has two pages. ANSWER ALL QUESTIONS.

1. (a) Define a *Quadratic Residue* modulo-p, where $p > 3$ is an odd prime. QP $\boxed{q = p?}$ $p \in \mathbb{Z}_p^*$ (2 marks)

(b) State and prove *Euler's Criterion* which gives the necessary and sufficient condition for a given integer to be a Quadratic Residue modulo-p. $a^{\frac{p-1}{2}} \equiv 1 \pmod p$? (6 marks)

(c) Euler's Criterion does not suggest any method to find the "square root" of a Quadratic Residue in $\mathbb{Z}_p^*$, where $p > 3$ is an odd prime. Can you suggest a (conditional) polynomial-time technique to perform the same? $a^{\frac{p+1}{4}}$ $p \equiv 3 \pmod 4$ (3 marks)

(d) Suppose a is not a quadratic residue modulo-p, where $p > 3$ is an odd prime. What is the value of $a^{(p-1)/2} \pmod p$? -1 (2 marks)

(e) Find $5^{-1} \pmod{12}$ using the fact that $\mathbb{Z}_n^*$ is a cyclic group of order $\phi(n)$. 5 (3 marks)

(f) If for an integer $a > 1$, an odd composite number n satisfies $a^{n-1} \equiv 1 \pmod n$, then n is called a *Fermat pseudoprime* to the base-a, because a makes n behave similar to a prime number. The smallest base-2 Fermat pseudoprime is 341, because $341 = 11 \times 31$ is composite, but $2^{340} \equiv 1 \pmod{341}$. If n is a Fermat pseudoprime to *every integer* $a > 1$ coprime to itself (i.e. for every $a > 1$ such that $gcd(a, n) = 1$), then n is called a *Carmichael number* (or an *absolute Fermat pseudoprime*). The smallest Carmichael number is 561. Although Carmichael numbers are relatively rare, it can be proved that there are infinitely many Carmichael numbers. Such numbers cause a non-zero probability of error in probabilistic primality testing schemes based on *Fermat's Little Theorem*.

(i) Suppose $n = pq$ where p, q are distinct odd primes. Then, prove that if $p|t$ and $q|t$, then $n|t$. trivial ?! (2 marks)

(ii) Using the result in part-(a), prove that for an integer $a > 1$, if $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$, then n is a *Fermat pseudoprime* to the base-a. $a^{p-1} \equiv 1 \ (p)$ (4 marks)

(g) Define the RSA public-key cryptosystem. (5 marks)

(h) A plaintext $x \in \mathcal{P}$ is said to be *fixed*, if $y = e_k(x) = x$, i.e., the encryption with *a given key k* results in the cipherext $y \in \mathcal{C}$ to be identical to the plaintext x (note that this an extremely undesirable situation, and should be carefully avoided). Show that for the RSA cryptosystem the number of fixed plaintexts $x \in \mathbb{Z}_n^*$ is equal to $\gcd(b-1, p-1) \times \gcd(b-1, q-1)$, where the parameters n, b, p and q have their usual significance. (Hint: consider the following system of two congruences: $e_k(x) \equiv x \pmod p$ and $e_k(x) \equiv x \pmod q$). (5 marks)

(i) Suppose Bob wants to send an RSA-encrypted message to Alice to inform Alice about his bank account number to which Alice should transfer some money. Suppose, Bob's bank account number is $x \in \mathbb{Z}_n^*$, where n is the RSA modulus being used. However, an intelligent adversary Oscar has opened a bank account such that Oscar's bank account number is $x_1 \equiv 2x \pmod n$. During the communication from Bob to Alice, Oscar has the capability of launching a *man-in-the-middle attack*. Describe how can Oscar fool Alice to transfer money to his account instead of Bob's. (5 marks)

$b \to$ public exp $\qquad 2^b$?

$n = pq$

(x_1, y_1)
$x_3 = \lambda^2 - x_1 - x_2$ (x_2, y_2)
$y = \lambda x + \nu$
$\lambda = (3x^2 + 2)|_{x_1} (2y_1)^{-1}$ no of points on $E(\mathbb{Z}_p)$

2. (a) Let E be an elliptic curve defined over $\mathbb{Z}_p$ where $p > 3$ is prime. Suppose $\#E$ be prime, $P \in E$ and $P \neq \mathcal{O}$. Prove that $\log_P(-P) = \#E - 1$. (2 marks)

(b) Consider the elliptic curve E: $y^2 \equiv x^3 + 2x + 2 \pmod{17}$ defined over $\mathbb{Z}_{17}$, and the given point $P(5, 1)$ on it. Find the point $2P$ on E. (6 marks)

(c) Describe how to find $\#E(\mathbb{Z}_p)$ in $O(p^{1/4})$ time using *Hasse's bound* on $\#E(\mathbb{Z}_p)$, and a modification of *Shank's Baby-step Giant-step Algorithm*. Give a pseudocode description of the algorithm. (6 marks)

(d) Explain why is its said that the "Discrete Logarithm Problem (DLP) is actually solved modulo $(p-1)$", when you want to solve it in $\mathbb{Z}_p^*$, where p is a prime. (3 marks)

(e) Consider a (t, w)-threshold secret sharing scheme, with parameters $p = 31$, $t = 3$, $w = 8$. Suppose three participants ~~come~~ together with shares $a(1) = 16$, $a(2) = 5$ and $a(3) = 5$ respectively. Find the secret key $k \in \mathbb{Z}_{31}$. (6 marks)

quadratic eqn, constant term key