University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Summer 2007
Examiners: D. Jao and A. Menezes

June 26, 2007
1:00 pm — 4:00 pm
MC 5158A

Instructions

Answer as many questions as you can. Complete answers are preferred over fragmented ones. Questions have equal value.

Questions

1. **Hash functions**

   (a) Is a collision-resistant hash function necessarily preimage resistant?

   (b) Let (n, e) be an RSA public key, where n is 2048 bits in length. The corresponding RSA private key is not known to anyone. Define a hash function $H : \{0,1\}^* \longrightarrow [0, n-1]$ as follows: $H(m) = \overline{m}^e \bmod n$, where $\overline{m}$ denotes the integer whose binary representation is m. Is H preimage resistant? (Justify your answer.) Is H collision resistant? (Justify your answer.)

   (c) Let $IV \in \{0,1\}^n$ be a fixed initialization vector, and let $f : \{0,1\}^{n+r} \longrightarrow \{0,1\}^n$ be a compression function. Define the hash function H as follows: to hash a message x of bitlength $b < 2^r$, the message is first divided into r-bit blocks: $\overline{x} = x_1, x_2, \ldots, x_t$ (where the last block is padded with 0 bits if necessary). Define x_{t+1} to be the right-justified binary representation of b. Define $H_0 = IV$ and $H_i = f(H_{i-1}, x_i)$ for $i = 1, 2, \ldots, t+1$. Then $H(x)$ is defined to be H_{t+1}.
   Prove that if f is collision resistant, then H is also collision resistant.

2. **Elementary number theory**

   (a) Let p be an odd prime. Prove that a quadratic residue modulo p can never be a generator of $\mathbb{F}_p^*$.

   (b) Let p be an odd prime. Prove that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 3$.

   (c) Let $p > 3$ be a Mersenne prime. Prove that 3 is a quadratic nonresidue modulo p.

3. **Discrete logarithm problem**
   Let $p = 2^{2^k} + 1$ be a prime number. Describe and analyze a polynomial-time algorithm for solving the discrete logarithm problem in $\mathbb{F}_p^*$. (Recall that the DLP in $\mathbb{F}_p^*$ is the following: given p, a generator α of $\mathbb{F}_p^*$, and $\beta \in \mathbb{F}_p^*$, find the integer $l \in [0, p-2]$ such that $\beta = \alpha^l \bmod p$.)

4. **Security of the basic ElGamal public-key encryption scheme**
   Let G be a (cyclic) group of prime order $n > 2$, and let α be a generator of G. We assume that the group operation in G can be computed in polynomial time. Recall that the Diffie-Hellman problem for G with respect to α (DHP_α) is the following: given α^a and α^b, compute α^{ab}. The decision Diffie-Hellman problem for G with respect to α (DDHP_α) is the following: given α^a, α^b and α^c, decide whether $c \equiv ab \pmod n$.

   In the basic ElGamal public-key encryption scheme, Alice's private key is an integer $a \in [1, n-1]$, and her public key is $\beta = \alpha^a$. To encrypt a plaintext message $m \in G$ for Alice, Bob selects $k \in_R [1, n-1]$, and sends the ciphertext $C = (\alpha^k, m\beta^k)$ to Alice.

   In the following, we consider ciphertext-only attacks on the basic ElGamal public-key encryption scheme. The attacker has knowledge of the group parameters, Alice's public key β, and one or more ciphertexts.

(a) The ElGamal-decrypt problem is the following: Given a public key β and a ciphertext C, compute the corresponding plaintext. Prove that the ElGamal-decrypt problem is polynomial-time equivalent to DHP_α.

(b) Prove that the semantic security of the basic ElGamal public-key encryption scheme (under ciphertext-only attack) is polynomial-time equivalent to DDHP_α.

(c) Is the basic ElGamal public-key encryption scheme semantically secure against chosen-ciphertext attacks? (Justify your answer.)

5. **Weil pairing**
Let E be an elliptic curve over a field, and suppose $P, Q \in E[n]$ for some $n > 0$.

(a) Give the formula for the Weil pairing $e(P, Q)$ of P and Q.

(b) Prove that the choice of divisors in the formula does not affect the value of $e(P, Q)$. You may assume Weil reciprocity.

(c) Prove that the Weil pairing is bilinear.

6. **Embedding degree**
Let E be an elliptic curve defined over $\mathbb{F}_q$, and denote by n the largest prime factor of $\#E(\mathbb{F}_q)$. Recall that the *embedding degree* of E is by definition equal to the multiplicative order of q in $(\mathbb{Z}/n\mathbb{Z})^*$.

(a) Let k be an integer. Prove that the embedding degree of E divides k if and only if $n \mid (t-1)^k - 1$, where t is the trace of E.

(b) Suppose $q = p^2$ and $t = p$ where p is prime. Determine the embedding degree of E.