University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Spring 2013
Examiners: D. Jao and A. Menezes

July 2, 2013
9:00 am — 12:00 pm
MC 5136B

Instructions

Answer as many questions as you can. *Complete answers are preferred over fragmented ones.*

Questions

1. **Hash functions**

   (a) Define what it means for a hash function to be preimage resistant.

   (b) Let E be a block cipher with 80-bit keys and an 80-bit block size. Fix a publicly known 80-bit initialization vector IV. Define a hash function $H\colon \{0,1\}^{160} \to \{0,1\}^{80}$ as follows:

   $$H(m) = E_{m_2}(E_{m_1}(IV)),$$

   where m_1 (respectively, m_2) represents the first (respectively, last) 80 bits of m.

   Give (and analyze) an algorithm to find preimages for H. Your algorithm should use no more than $\approx 2^{40}$ invocations of E.

2. **Block Ciphers**

   Recall that the CBC block cipher mode of operation encrypts a message $m_1 m_2 \cdots m_n$ to the ciphertext $c_0 c_1 c_2 \cdots c_n$ where c_0 is chosen at random and

   $$c_i = E_k(m_i \oplus c_{i-1}).$$

   (a) Explain how decryption is performed with CBC.

   (b) We define a new block cipher mode of operation known as UBC (Useless Block Chaining), with

   $$c_i = E_k(m_i) \oplus c_{i-1}.$$

   Show that Useless Block Chaining is, in fact, useless.

3. **Elementary Number Theory**

   Let p denote an odd prime.

   (a) Let g be a *generator* (a.k.a. a *primitive root*) modulo p. Show that g is not a quadratic residue modulo p.

   (b) Suppose $y \equiv g^x \pmod{p}$ for some integer $0 < x < p-1$. Show how one can efficiently find the least significant bit of the binary expansion of x.

4. **Provable Security**

Let p be a large prime, and let q be a large prime divisor of $p-1$. Let g be an element of order q in $\mathbb{Z}_p^*$, and let G denote the subgroup of $\mathbb{Z}_p^*$ generated by g. We consider the *ElGamal encryption scheme* in the group G, which is defined as follows:

Setup: Public parameters p, q, g are chosen.

Key generation: Choose $x \in \mathbb{Z}_q^*$ at random. The public key is g^x and the private key is x.

Encryption: The message space is the set G. Given a message $m \in G$ and a public key g^x, choose a random integer r and output the ciphertext $c = (g^r, mg^{xr})$.

Decryption: Given a ciphertext $c = (\rho, \sigma)$, output $m = \sigma/\rho^x$.

(a) It is conjectured that the Decision Diffie-Hellman (DDH) assumption holds in the group G. Assuming this conjecture, prove that the ElGamal encryption scheme is **IND-CPA** secure.
(Recall that IND-CPA means "indistinguishable against chosen-plaintext attacks".)

(b) Suppose that, in the encryption function defined above, the message space is taken to be $\mathbb{Z}_p^*$ instead of G. Show that the resulting encryption scheme is not **IND-CPA** secure.

5. **RSA**

Alice has a corrupted copy of Bob's RSA public key (n, e), in which one bit of the public exponent e is wrong. Alice encrypts a message m under the textbook RSA scheme using this corrupted public key, and sends the resulting ciphertext c_1 to Bob. Later, Alice obtains a correct copy of Bob's RSA public key, and sends an encryption c_2 of the same message m under textbook RSA using the correct key. An adversary, who knows Bob's public key, obtains both c_1 and c_2. Show how the adversary can obtain m.

6. **Elliptic Curves**

Let p be an odd prime satisfying $p \equiv 2 \pmod 3$. Consider the elliptic curve $E : y^2 = x^3 + b$ defined over $\mathbb{F}_p$ ($b \neq 0$).

(a) Prove that the mapping $x \mapsto x^3$ is a bijection on $\mathbb{F}_p$.

(b) Prove that the number of points in $E(\mathbb{F}_p)$ is $p+1$.

(c) Let $R = (x_R, y_R)$ be a point on $E(\mathbb{F}_p)$. Given y_R, explain how to compute x_R efficiently.