University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Summer 2011
Examiners: D. Jao and E. Teske-Wilson

June 14, 2011
9:00 am — 12:00 pm
MC 6005

Instructions

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

Questions

1. **Hash functions**

   (a) Give an example of a hash function $H\colon \{0,1\}^* \to \{0,1\}^*$ that is collision resistant but not preimage resistant. Justify your choice!

   (b) Define what it means for a pair of permutations f_0, f_1 on S to be claw-free.

   (c) Let $p, q \equiv 3 \pmod 4$, and let $n = pq$. Let S denote the set of squares modulo n, coprime with n. Let $a_0, a_1 \in_R S$, and define the functions $f_0\colon S \to S$ and $f_1\colon S \to S$ by $f_0(x) = a_0 x^2 \bmod n$ and $f_1(x) = a_1 x^2 \bmod n$. Then f_0 and f_1 are permutations on S (you do not need to show this). Show that under the assumption that factoring n is computationally infeasible, f_0 and f_1 is a claw-free pair of permutations.

   (d) Using f_0 and f_1, construct a collision-free hash function $H\colon \{0,1\}^* \to S$.

2. **Block Ciphers**
   Recall that a Feistel cipher has a round function of the following form

$$
\begin{aligned}
L^i &= R^{i-1} \\
R^i &= L^{i-1} \oplus f(R^{i-1}, K_i)
\end{aligned}
$$

   The plaintext is $L^0||R^0$ and the ciphertext is $L^n||R^n$.

   (a) What properties does f need to satisfy in order for encryption to be invertible? Justify.

   (b) Describe the decryption algorithm.

3. **Elementary Number Theory**
   Throughout this question, n is an odd integer, and a is an integer, $1 \le a < n$.

   (a) Assume n is prime, and write $n - 1 = 2^k m$ with m odd. Assume $a^{2^i m} \not\equiv -1 \bmod n$ for all $0 \le i < k$.
   Prove that $a^{2^i m} \equiv 1 \bmod n$ for all $0 \le i \le k$.

   (b) Let n be prime. Prove that

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n. \tag{1}$$

   (c) Now let n be composite, again write $n-1 = 2^k m$ with m odd. Assume $\gcd(a, n) = 1$.
   Recall that n is called a strong pseudoprime to the base a if $a^m \equiv 1 \bmod n$ or there exists i, $0 \le i < k$ such that $a^{2^i m} \equiv -1 \bmod n$.
   Further recall that n is called an Euler pseudoprime to the base a if (1) from part (b) holds.
   Prove that for $n \equiv 3 \bmod 4$, n is a strong pseudoprime to the base a if and only if n is an Euler pseudoprime to the base a.

4. **Provable Security**
The *Blum-Goldwasser* public key cryptosystem is given as follows.

- Key generation: Choose distinct primes p and q congruent to 3 mod 4. The public key is $n = pq$ and the private key is (p, q).
- Encryption: A message m consists of a single bit. To encrypt m, choose a random $x \in \mathrm{QR}_n$ and compute
  i. $b = \mathrm{LSB}(x)$
  ii. $c = b \oplus m$
  iii. $y = x^2 \pmod{n}$

  The ciphertext is (c, y).

Prove that the cryptosystem is **IND-CPA**. State any necessary assumptions.

5. **Pseudo-random Bit Generators**
Let (n, e) be an RSA public key, and let d be the corresponding RSA private key.

Let $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ be defined by $f(x) = x^e \bmod n$.

Let $B\colon \mathbb{Z}_n \to \{0, 1\}$ be defined by

$$B(x) = \begin{cases} 1 & \text{if } x^d \bmod n \text{ is odd} \\ 0 & \text{if } x^d \bmod n \text{ is even.} \end{cases}$$

Clearly, $B(x)$ is easy to compute given x and $f^{-1}(x)$ (since $f^{-1}(x) = x^d \bmod n$). It can be shown (and you may assume) that $B(x)$ is hard to compute given only x.

(a) Define (informally) what it means for a PRBG G to pass the next bit test.

(b) Describe a cryptographically secure PRBG G which takes as seed random $x_0 \in \mathbb{Z}_n$ and uses f and B above.

(c) Prove that the generator G passes the next bit test.

6. **Elliptic Curves**
Consider the Koblitz curve defined over $\mathbb{F}_2$:

$$E : y^2 + xy = x^3 + x^2 + 1 \; .$$

(a) Show that $\#E(\mathbb{F}_{2^r})$ is even for all $r \geq 1$.

(b) Show that if $r > 4$ and $\#E(\mathbb{F}_{2^r}) = 2p$ where p is a prime number, then r must be prime.