University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Fall 2004
Examiners: A. Menezes and E. Teske

November 9, 2004
1:30 pm — 4:30 pm
MC 5045

Instructions

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

Questions

1. **Hash functions**

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

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

   (c) Let E denote the family of encryption functions for the AES block cipher where plaintext blocks, ciphertext blocks, and keys are each 128 bits in length. Define a hash function $H : \{0,1\}^{256} \longrightarrow \{0,1\}^{128}$ by $H(x,y) = E_x(y)$. Here, x and y are 128-bit blocks, and $E_x(y)$ denotes the encryption of the plaintext block y using the key x. Is H collision resistant? (Justify your answer.)

   (d) Is the hash function in (c) second preimage resistant? (Justify your answer.)

2. **Elementary number theory**
   Let p be an odd prime and let $n > 1$ be a positive integer. Recall that the multiplicative group $\mathbb{Z}_{p^n}^*$ is cyclic. Suppose that the integer g is a generator of $\mathbb{Z}_p^*$, and let $h = (p+1)g$. Prove that at least one of g or h is a generator of $\mathbb{Z}_{p^n}^*$.
   Hint: First prove that at least one of g^{p-1} or h^{p-1} can be expressed in the form $1 + kp$ where k is an integer that is not divisible by p.

3. **Bit security of the Discrete Logarithm Problem**
   Let p be an odd prime, and let g be a generator of $\mathbb{Z}_p^*$. Consider the following three problems:
   DLP: Given p, g, and $x \in \mathbb{Z}_p^*$, determine the integer $a \in [0, p-2]$ such that $x \equiv g^a \pmod{p}$. (We write $a = \log_g x$.)
   DLP-LSB: Given p, g, and $x \in \mathbb{Z}_p^*$, determine $A(x)$ where

$$A(x) = \begin{cases} 1, & \text{if } \log_g x \text{ is even,} \\ 0, & \text{if } \log_g x \text{ is odd.} \end{cases}$$

   DLP-MSB: Given p, g, and $x \in \mathbb{Z}_p^*$, determine $B(x)$ where

$$B(x) = \begin{cases} 1, & \text{if } 0 \le \log_g x < (p-1)/2 \\ 0, & \text{if } (p-1)/2 \le \log_g x \le (p-2). \end{cases}$$

   (a) Prove that DLP-MSB $\le_P$ DLP.
   (Recall that $A \le_P B$ means that problem A polynomial-time reduces to problem B.)

   (b) Prove that DLP $\le_P$ DLP-MSB.

   (c) Does DLP $\le_P$ DLP-LSB? (Justify your answer.)

4. **Fault analysis attack on the RSA signature scheme**
Suppose that a smart card is using the Chinese Remainder Theorem for RSA signature generation. That is, if (n, e) is the RSA public key and d is the corresponding private key, then signing a message m is performed as follows:

   i) Compute $M = H(m)$.

   ii) Compute $s_p = M^{d_p} \bmod p$ and $s_q = M^{d_q} \bmod q$, where $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$.

   iii) Find s, $0 \leq s \leq n-1$, such that

$$\begin{cases} s \equiv s_p \pmod{p} \\ s \equiv s_q \pmod{q}. \end{cases}$$

   (a) Prove that s is the correct signature of m (that is, prove that $s = H(m)^d \bmod n$).

   (b) Explain why it might be advantageous to compute s using the procedure described above instead of computing $s = M^d \bmod n$ directly using the repeated square-and-multiply algorithm.

   (c) Suppose now that an adversary can somehow induce the smart card to compute s_p incorrectly (and s_q correctly) while signing a message. Let s' be a resulting (incorrect) signature on m. Suppose that the adversary has access to the public key (n, e) and also the signed message (m, s'). Show how the adversary can efficiently factor n.

   (d) Suggest a (realistic and practical) method for preventing this attack.

5. **Provable security**
Recall that in the Full-Domain Hash (FDH) RSA signature scheme, an entity with public key (n, e) and private key d generates a signature s on a message m by computing $s = H(m)^d \bmod n$. Here $H : \{0,1\} \longrightarrow [0, n-1]$ is a hash function. Prove that if finding eth roots modulo n is intractable, and if H is a random function, then FDH RSA is existentially unforgeable by an adversary who can mount an adaptive chosen-message attack.

6. **Elliptic curves and finite fields**

   (a) Recall that the Trace function $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by $\mathrm{Tr}(\alpha) = \sum_{i=0}^{m-1} \alpha^{2^i}$. Prove that exactly half of the elements in $\mathbb{F}_{2^m}$ have trace 0 (and the other half have trace 1).

   (b) Let $\alpha \in \mathbb{F}_{2^m}$. Prove that the equation $x^2 + x = \alpha$ has a solution $x \in \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(\alpha) = 0$.

   (c) Let $E : y^2 + y = x^3$ be an elliptic curve over $\mathbb{F}_{2^m}$ where m is an odd positive integer. Prove that $\#E(\mathbb{F}_{2^m}) = 2^m + 1$.