University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Summer 2018
Examiners: D. Jao and A. Menezes

June 18, 2018
1:00 pm — 4:00 pm
MC 5417

Instructions

- Answer as many questions as you can.
- You are *not* expected to answer all 7 questions.
- Complete answers are preferred over fragmented ones.
- Some questions may require additional assumptions, such as complexity-theoretic assumptions. State any additional assumptions that you require.
- Justify all answers.

Questions

1. **Block ciphers**
   Recall that DES is a block cipher with key space $K = \{0,1\}^{56}$, plaintext space $M = \{0,1\}^{64}$, and ciphertext space $C = \{0,1\}^{64}$.

   (a) Let $\overline{m}$ denote the bitwise complement of a bit string m (i.e., $\overline{m} = m \oplus 11\cdots1$). By examining the description of DES, one can see that if $c = \mathrm{DES}_k(m)$ then $\overline{c} = \mathrm{DES}_{\overline{k}}(\overline{m})$. Can you use this property of DES to (slightly) improve the running time of exhaustive key search under a chosen-plaintext attack?

   (b) Recall that Triple-DES has key space $K = \{0,1\}^{168}$. A plaintext $m \in \{0,1\}^{64}$ is encrypted under key $k = (k_1, k_2, k_3)$ (where $k_1, k_2, k_3 \in \{0,1\}^{56}$) as follows:

   $$E_k(m) = \mathrm{DES}_{k_3}(\mathrm{DES}_{k_2}(\mathrm{DES}_{k_1}(m))).$$

   Describe a known-plaintext attack on Triple-DES that is significantly faster than exhaustive key search. Estimate the time and space requirements of your attack.

2. **Hash functions**
   Let q be a prime, and let G be a (multiplicatively written) group of order q. Let g and h be randomly selected elements from $G \setminus \{1\}$. Consider the function $H_{g,h} : \mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow G$ defined by $H_{g,h} : (x, y) \mapsto g^x h^y$. Henceforth we will denote $H_{g,h}$ by H.

   (a) Show that for any $k \in G$, there are exactly q distinct solutions $(x, y) \in \mathbb{Z}_q \times \mathbb{Z}_q$ to the equation $g^x h^y = k$.

   (b) Prove that if the discrete logarithm problem in G is intractable then H is collision resistant.

   (c) Is H preimage resistant?

3. **Elementary number theory**

   (a) Let $n \geq 3$ be an integer. Suppose that there exists an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime divisors q of $n-1$. Prove that n is prime.

   (b) The *Fermat numbers* are $F_k = 2^{2^k} + 1$ for $k \geq 1$. Prove that for $k \geq 2$, F_k is prime if and only if $5^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.
   (It may help to remember Euler's Theorem: If p is an odd prime, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.)

4. **Number-theoretic algorithms**

   (a) An instance of CHREM (Chinese Remainder Problem) is a pair of distinct primes p and q, and two integers $a \in [0, p-1]$ and $b \in [0, q-1]$ The problem is to determine the unique integer $x \in [0, n-1]$ (where $n = pq$) such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$. Design (and analyze) a polytime algorithm for CHREM.

   (b) Let $n = pq$, where p and q are distinct primes satisfying $p \equiv q \equiv 3 \pmod{4}$. Let FACTOR be the problem of factoring n. Let SQUARE-ROOT be the problem of finding one square root of $a \in QR_n$. Prove that SQUARE-ROOT $\leq_P$ FACTOR. (Recall that QR_n is the set of quadratic residues modulo n. Recall also that $A \leq_P B$ means that problem A polynomial-time reduces to problem B.)

5. **RSA**

   (a) Suppose that Alice's RSA public key is $(n = 143, e = 7)$. Determine her private key d.

   (b) Let (n, e) be an RSA public key, where $n = pq$, and e is an integer with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. It is known that the number of plaintexts $m \in [0, n-1]$ satisfying $m^e \equiv m \pmod{n}$ is

   $$[1 + \gcd(e-1, p-1)] \cdot [1 + \gcd(e-1, q-1)].$$

   Such a plaintext message m is called an *unconcealed message* since its RSA ciphertext is equal to m itself.
   Prove that there is at least one value of e, $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$, such that $m^e \equiv m \pmod{n}$ for all $m \in [0, n-1]$.

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 $R = (x, y)$ be a point in $E(\mathbb{F}_p)$. Given y, explain how to compute x efficiently.

7. **ECDSA**

Recall the ECDSA signature scheme. The domain parameters consist of a 256-bit prime p, an elliptic curve E defined over $\mathbb{Z}_p$ with prime $n = \#E(\mathbb{Z}_p)$, and a point $P \in E(\mathbb{Z}_p)$ with $P \neq \infty$. Alice's private key is $a \in_R [1, n-1]$ and her public key is $A = aP$. To sign a message $M \in \{0,1\}^*$, Alice does the following:

(i) Select a per-message secret $k \in_R [1, n-1]$.
(ii) Compute $m = \text{SHA256}(M)$.
(iii) Compute $R = kP$. Let $r = x(R) \bmod n$ and check that $r \neq 0$.
(r is the x-coordinate of R, reduced modulo n.)
(iv) Compute $s = k^{-1}(m + ar) \bmod n$, and check that $s \neq 0$.
(v) Alice's signature on M is (r, s).

To verify A's signature (r, s) on M, Bob does the following:

(i) Obtain an authentic copy of Alice's public key A.
(ii) Check that $1 \leq r, s \leq n-1$.
(iii) Compute $m = \text{SHA256}(M)$.
(iv) Compute $u_1 = ms^{-1} \bmod n$ and $u_2 = rs^{-1} \bmod n$.
(v) Compute $V = u_1P + u_2A$ and let $v = x(V) \bmod n$.
(vi) Accept if and only if $v = r$.

(a) Define what it means for a signature scheme to be *secure*.

(b) Suppose now that an adversary knows a message M such that $\text{SHA256}(M) = 0$. Show that the adversary can efficiently compute a valid signature for M. (The adversary knows the domain parameters and Alice's public key A, but does not have access to a signing oracle.)