University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Spring 2020
Examiners: A. Menezes and D. Stebila

June 4, 2020
1:00 pm — 4:00 pm

Instructions

Answer as many questions as you can. *Complete answers are preferred over fragmented ones.* We do not expect complete answers to all 7 questions.

Questions

1. **Shannon's theory**

   (a) Define what it means for a symmetric-key encryption scheme to have perfect secrecy.

   (b) Suppose that a symmetric-key encryption scheme with encryption function $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ satisfies $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. Prove that, if the encryption scheme has perfect secrecy, then every key is used with equal probability $1/|\mathcal{K}|$, and for every message $x \in \mathcal{M}$ and ciphertext $y \in \mathcal{C}$, there is a unique key k such that $E(k, x) = y$.

2. **Authenticated encryption**
   Let $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ and $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ be the encryption and decryption functions for a symmetric-key encryption scheme, and let $MAC : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ be a message authentication code. Consider the following two candidate constructions for an authenticated encryption scheme, which aims to simultaneously provide confidentiality and integrity:

   (i) Split k into two keys k_1, k_2. Compute $c \leftarrow E(k_1, m)$ and $t \leftarrow MAC(k_2, c)$. Return (c, t).

   (ii) Split k into two keys k_1, k_2. Compute $c \leftarrow E(k_1, m)$ and $t \leftarrow MAC(k_2, m)$. Return (c, t).

   Assume that (E, D) constitute a secure encryption scheme, and MAC is a secure message authentication code. For each of (i) and (ii), is the candidate construction guaranteed to provide both confidentiality and integrity? If not, give a counterexample. If so, give an argument to that effect.

3. **Primality testing**
   Recall that if n is a composite integer, and $a \in [1, n-1]$ satisfies $a^{n-1} \equiv 1 \pmod{n}$, then a is called a *Fermat liar* for n.
   Now, let $n = pq$, where p and q are distinct odd primes, let $a \in \mathbb{Z}_n^*$, and let $d = \gcd(p-1, q-1)$. ($\mathbb{Z}_n^*$ is the set of numbers in $[1, n-1]$ that are invertible modulo n.)

   (a) Prove that a is a Fermat liar for n if and only if $a^d \equiv 1 \pmod{n}$.
   (Hint: Note that $n - 1 = pq - 1 = (p-1)q + (q-1)$.)

   (b) Suppose now that $q = 2p + 1$. How many $a \in \mathbb{Z}_n^*$ are Fermat liars for n? List them all (in terms of p).

4. **Integer factorization**

   (a) Describe the *random squares method* for factoring a number n that is not a prime or a prime power. You are not expected to analyze the running time of the algorithm.
   (Note: In Stinson's book, the algorithm is called "Dixon's random squares algorithm". In Koblitz's book, the algorithm is called "Factor base algorithm".)

   (b) Explain the trade-off that dictates the optimal size of the factor base.

5. **Discrete logarithm and Diffie-Hellman problems**
Let G be a multiplicatively-written group of prime order $n > 3$ generated by g. The Diffie-Hellman Problem (DHP) is the following: given $g^a, g^b \in G$, compute g^{ab}.

   (a) The problem SQUARE is the following: given $g^x \in G$, compute g^{x^2}.
   Prove that DHP $\leq_P$ SQUARE. (Recall that the notation $A \leq_P B$ means that problem A polynomial-time reduces to problem B.)

   (b) The problem CUBE is the following: given $g^x \in G$, compute g^{x^3}.
   Prove that CUBE $\leq_P$ SQUARE.

   (c) Prove that DHP $\leq_P$ CUBE. (Hint: Recall that $(x+1)^3 = x^3 + 3x^2 + 3x + 1$.)

6. **Hash functions**
Let p be a 256-bit prime, and let E be an elliptic curve defined over $\mathbb{Z}_p$ with $\#E(\mathbb{Z}_p) = n$ a prime. Let $P, Q \in_R E(\mathbb{Z}_p)$ be randomly selected points, neither of which is the point at infinity; these points are fixed and public.
Define the hash function $H : [0, n-1] \times [0, n-1] \longrightarrow E(\mathbb{Z}_p)$ by $H((a,b)) = aP + bQ$. That is, messages are pairs (a, b) of integers in the interval $[0, n-1]$, and the hash of such a message is the elliptic curve point $aP + bQ$.

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

   (b) Define what it means for H to be collision resistant.

   (c) Prove, under a reasonable computational assumption (which you should state), that H is collision resistant.

   (d) Prove, under a reasonable computational assumption (which you should state), that H is preimage resistant.

7. **Signature schemes**

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

   In the basic (textbook) RSA signature scheme, the public key is a pair (n, e) and the secret key is a pair (n, d). The signature on a message $m \in \mathbb{Z}_n$ is $s = m^d \bmod n$, and verification is done by checking if $s^e \equiv m \bmod n$.

   (b) Show how to come up with some valid message/signature pairs under a *key only* attack on the basic RSA signature scheme.

   (c) Show how to come with a forgery for any given message m under a *chosen message attack* on the basic RSA signature scheme, wherein the adversary is allowed to obtain signatures for at most two messages (neither of which is equal to m).

   (d) One way of building a secure RSA-based signature scheme is to sign $H(m)$ using a "full domain" hash function H. The security proof for RSA-FDH is "in the random oracle model". Briefly explain what the random oracle model is.