University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Spring 2025
Examiners: S. Jaques and A. Menezes

June 11, 2025
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.
- Justify all answers.

Questions

1. **Hash functions**
   Let $H : \{0,1\}^{\leq \ell} \to \{0,1\}^n$ be a hash function mapping binary strings of length at most ℓ, for some $\ell > n$, to binary strings of length n.

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

   (b) Define what it means for H to be second-preimage resistant.

   (c) Prove *one* of the following statements:

   (i) If H is collision resistant, then H is also second-preimage resistant.

   (ii) If H is second-preimage resistant, then H is also collision resistant.

   (d) Define $G : \{0,1\}^{\leq \ell} \to \{0,1\}^n$ by $G(x) = H(H(x))$. Prove that if H is collision resistant then G is also collision resistant.

2. **MAC schemes**

   (a) Let E denote the family of encryption functions for a block cipher where plaintext blocks, ciphertext blocks, and keys are each 128 bits in length. Let $H : \{0,1\}^* \to \{0,1\}^{128}$ be a hash function. Define a MAC scheme $\text{MAC}_k : \{0,1\}^{3072} \to \{0,1\}^{128}$ by $\text{MAC}_k(m) = E_k(H(m))$. Here, k is a 128-bit secret key. Is this MAC scheme secure? (Explain)

   (b) Consider the following MAC scheme for authenticating fixed-length messages from $\{0,1\}^{256}$. For each i, $1 \leq i \leq 128$, let S_i be a fixed subset of $\{1, 2, 3, \ldots, 255, 256\}$. The key space is $\{0,1\}^{128}$. To authenticate a message m with key k, one first forms the 128-bit string $b = b_1 b_2 \cdots b_{128}$ where b_i is the sum modulo 2 of the bits of m indexed by the elements of S_i, and then AES-encrypts b with key k. The resulting ciphertext c is the tag on m.
   Show how a passive adversary who is given a single valid message/tag pair can easily produce new valid message/tag pairs.

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. **RSA signatures**
   Recall that in the Full-Domain Hash (FDH) RSA signature scheme, an entity (Alice) 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.

   (a) Describe how someone can verify Alice's signature s on a message m.

   (b) Prove that if finding eth roots modulo n is intractable, and if H is a random function, then RSA-FDH is *secure* (i.e., existentially unforgeable by an adversary who can mount an adaptive chosen-message attack). Your proof can be informal, but should contain all the essential ideas of a formal proof.

5. **Discrete logarithms.** Let p be a prime, let q be a prime divisor of $p-1$, and let g be an element of order q in $\mathbb{Z}_p^*$. The discrete logarithm problem is the following: given p, q, g and $h \in_R \langle g \rangle$, determine the integer $x \in [0, n-1]$ such that $h = g^x \pmod p$. Here, $\langle g \rangle$ denotes the subgroup of $\mathbb{Z}_p^*$ generated by g.
   Describe and analyze an algorithm for solving the discrete logarithm problem that has running time $O(\sqrt{q})$ $\mathbb{Z}_p$ operations. There is no limit on how much space your algorithm can use.

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. **Elliptic Curve Diffie-Hellman key agreement**
   Let E be an elliptic curve defined over $\mathbb{Z}_p$, where p is a prime. Let $n = \#E(\mathbb{Z}_p)$, and suppose that n is prime. Let $P \in E(\mathbb{Z}_p)$ with $P \neq \infty$.

   (a) Recall that in the *unauthenticated* elliptic curve Diffie-Hellman key agreement protocol (ECDH), Alice selects $x \in_R [1, n-1]$ and sends $X = xP$ to Bob. Similarly, Bob selects $y \in_R [1, n-1]$ and sends $Y = yP$ to Alice. Their shared secret key is $k = H(K)$ where $K = xyP$ and H is a hash function. Alice and Bob subsequently use k to encrypt and decrypt messages using AES.
   Describe the *malicious-intruder-in-the-middle* attack (also known as the *man-in-the-middle* attack) on ECDH.

   (b) Describe a variant of *authenticated* ECDH, and give an informal argument for its security against *active attacks*.