University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Summer 2017
Examiners: D. Jao and A. Menezes

July 13, 2017
1:00 pm — 4:00 pm
MC 4044

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. **Symmetric-key encryption**
   The original DES block cipher is limited to a 56-bit key and 64-bit plaintext/ciphertext blocks. The DES-X block cipher, proposed by Ron Rivest, uses a 184-bit key (k, k_1, k_2) where $k \in \{0,1\}^{56}$ and $k_1, k_2 \in \{0,1\}^{64}$. The encryption of a plaintext $m \in \{0,1\}^{64}$ is given by
   $$E(m) = \mathrm{DES}_k(m \oplus k_1) \oplus k_2,$$
   where $\mathrm{DES}_k(m)$ denotes the DES-encryption of a 64-bit plaintext block m with 56-bit secret key k.

   (a) Describe the decryption procedure.

   (b) Suppose that the XOR with k_1 is omitted, i.e.
   $$E(m) = \mathrm{DES}_k(m) \oplus k_2,$$
   where the key (k, k_2) is now 120 bits. Describe a chosen-ciphertext attack that recovers the secret key using roughly 2^{56} DES operations.

2. **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 *preimage resistant.*

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

   (d) Let $G : \{0,1\}^{2n} \to \{0,1\}^n$ and $H : \{0,1\}^{2n} \to \{0,1\}^n$ be two hash functions. Define the function $F : \{0,1\}^{2n} \to \{0,1\}^n$ by $F(x) = H(G(x), G(x))$. (Here, the comma "," denotes concatenation.) Prove that if G and H are collision resistant, then F is also collision resistant.

   (e) Suppose that $f : \{0,1\}^{n+r} \to \{0,1\}^n$ is a preimage resistant function. Define $H : \{0,1\}^{2(n+r)} \to \{0,1\}^n$ as follows. Given $x \in \{0,1\}^{2(n+r)}$, write
   $$x = x_L \| x_R \quad \text{where} \quad x_L, x_R \in \{0,1\}^{n+r};$$
   here, $\|$ denotes concatenation. Then define
   $$H(x) = f(x_L \oplus x_R).$$
   Prove that H is not second-preimage resistant.

3. **Elementary number theory**
   Note: Parts (a) and (b) are unrelated.

   (a) Let p be a prime, $n \in \mathbb{N}$, and $q = p^n$. Prove that the finite field $\mathbb{F}_q$ has $q-2$ generators if and only if $q-1$ is a Mersenne prime.

   (b) Let $m \geq 3$ be an integer. Prove that if a is a quadratic residue modulo m, and $ab \equiv 1 \pmod{m}$, then b is also a quadratic residue.
   Now let p be a prime of the form $p = 4k+3$. Prove that the product of all the quadratic residues modulo p is congruent to 1.

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. **RSA signatures**
   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.

   (a) Show that FDH RSA is insecure against passive adversaries if H is not preimage resistant.

   (b) 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. **Discrete logarithm and Diffie-Hellman problems**
   Let G be a group of prime order $n > 2$ generated by α.
   The notation $A \leq_P B$ means that problem A polynomial-time reduces to problem B.

   (a) Recall that discrete logarithm problem in G with respect to α (DLP_α) is the following: given $\gamma \in G$, find the integer $\ell \in [0, n-1]$ that satisfies $\gamma = \alpha^\ell$. Now, let β be another generator of G. Prove that $\mathrm{DLP}_\alpha \leq_P \mathrm{DLP}_\beta$. (This proves that hardness of the DLP does not depend on the choice of generator.)

   (b) Recall that the Diffie-Hellman Problem (DHP) is the following: given $\alpha^x, \alpha^y \in G$, compute α^{xy}. The problem INV is the following: given $\alpha^x \in G$, compute $\alpha^{x^{-1}}$. Prove that INV $\leq_P$ DHP.

   (c) The problem SQUARE is the following: given $\alpha^x \in G$, compute α^{x^2}. Prove that DHP $\leq_P$ SQUARE.

7. **Elliptic curves**

Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over $\mathbb{Z}_p$, where $p > 3$ is prime.

(a) Prove the formula

$$\#E(\mathbb{Z}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$$

where the expression inside the summation is the Legendre symbol.

(b) Now suppose that $x^3 + ax + b$ splits into three distinct linear factors modulo p. Show that $E(\mathbb{Z}_p)$ is not cyclic.