University of Waterloo
Department of Combinatorics & Optimization

PhD Comprehensive Examination in Cryptography
Spring 2019
Examiners: D. Jao and D. Stebila

June 27, 2019
1:00 pm — 4:00 pm
MC 6460

Instructions

- Answer as many questions as you can.
- You are not expected to answer all 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 unless otherwise stated.

Questions

1. **Elementary Number Theory**
   Let $n = pq$ be an RSA modulus. Prove the following:

$$\prod_{x \in \mathbb{Z}_n^*} x \equiv 1 \pmod{n}.$$

2. **Hash functions**
   Recall that AES is a block cipher with message space $\{0,1\}^{128}$ and key space $\{0,1\}^{128}$. Let x and y denote bitstrings of length 128. Which of the following hash functions $H_i \colon \{0,1\}^{256} \to \{0,1\}^{128}$, if any, are preimage resistant? No justification is needed except that a lack of preimage resistance must be justified.

   (i) $H_1(x,y) = \mathrm{AES}_x(y) \oplus y$.
   (ii) $H_2(x,y) = \mathrm{AES}_y(y) \oplus x$.
   (iii) $H_3(x,y) = \mathrm{AES}_y(x) \oplus y$.

3. **Symmetric-key encryption**
   Let E be a block cipher where both the block length and key size are 64 bits. Consider the "improved" block cipher whose encryption function is given by $m \mapsto c = E_{k_0}(m \oplus k_1)$ where m is the 64-bit plaintext, c is the 64-bit ciphertext, k_0 is a 64-bit string, k_1 is a 64-bit string, and the key is the 128-bit string (k_0, k_1).

   (a) Give the decryption algorithm for the "improved" cipher.
   (b) Describe how to break the "improved" cipher by brute force in much less than 2^{128} time using a known plaintext attack.

4. **Cryptanalysis of RSA**
   Suppose that Alice and Bob agree to generate and share a common RSA modulus $n = pq$ for use in RSA encryption. Alice chooses an encryption exponent e_a and corresponding decryption exponent d_a, and Bob chooses an encryption exponent e_b and corresponding decryption exponent d_b. Suppose furthermore $\gcd(e_a, e_b) = 1$. Show that that an adversary who acquires a pair of ciphertexts $c_a = m^{e_a} \bmod n$ and $c_b = m^{e_b} \bmod n$ corresponding to a single message m encrypted to Alice and Bob respectively can recover the plaintext message m efficiently.

5. **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) If furthermore $b = 0$ and $p \equiv 3 \pmod 4$, show that $\#E(\mathbb{Z}_p) = p + 1$.

6. **Provable security**
The Boneh-Franklin cryptosystem is defined as follows.

   Public parameters: A cryptographic pairing $e\colon G \times G \to G_T$, and two elements $g, h \in G$, each of which generates the cyclic group G.

   Key generation: Choose $\alpha \in \mathbb{Z}$. The public key is g^α. The private key is h^α.

   Encryption: Given $m \in \{0,1\}^k$, the encryption of m is $(g^r, e(g^\alpha, h^r) \oplus m)$ for random $r \in \mathbb{Z}$. Here k is the number of bits used to represent an element of G_T.

   Decryption: Given a ciphertext (c_1, c_2), the plaintext is $c_2 \oplus e(c_1, h^\alpha)$.

   (a) Show that the Boneh-Franklin scheme is **OW-CPA** under the Bilinear Diffie-Hellman (BDH) assumption: Given g, g^α, g^r, and h, it is infeasible to compute $e(g,h)^{\alpha r}$.

   (b) Show that the Boneh-Franklin scheme is **IND-CPA** under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

$\text{OW-CPA}^{\mathcal{A}}_{\mathsf{Enc}}$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$
2 : $m \leftarrow\!\!\$\ M$
3 : $c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{pk}, m)$
4 : $m' \leftarrow\!\!\$\ \mathcal{A}(1^\lambda, \mathsf{pk}, c)$
5 : **return** $m \stackrel{?}{=} m'$

$\text{IND-CPA}^{\mathcal{A}}_{\mathsf{Enc}}$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$
2 : $b \leftarrow\!\!\$\ \{0,1\}$
3 : $(m_0, m_1) \leftarrow\!\!\$\ \mathcal{A}(1^\lambda, \mathsf{pk})$
4 : $c \leftarrow\!\!\$\ \mathsf{Enc}(\mathsf{pk}, m_b)$
5 : $b' \leftarrow\!\!\$\ \mathcal{A}(1^\lambda, \mathsf{pk}, c)$
6 : **return** $b \stackrel{?}{=} b'$

Figure 1: OW-CPA and IND-CPA definitions.