ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Exercise 4

4.1 The (In)security of the ElGamal Public-Key Cryptosystem

Goal*: The ElGamal public-key cryptosystem uses the Diffie-Hellmann protocol to build a PKE scheme. We prove that this scheme is IND-CPA secure, but not IND-CCA secure.*

The Diffie-Hellman protocol can be used as a PKE scheme, as discussed in the lecture. In this task we consider the security of one such scheme, the well known ElGamal public-key cryptosystem. Let the group G and the generator g be fixed and the order q be publicly known. The ElGamal scheme then works as follows:

Key generation: Choose x_B uniformly at random from $\mathbb{Z}_q$. The secret key is x_B, the public key is $y_B \coloneqq g^{x_B}$.

Encryption: On input a message $m \in G$, choose $x \in \mathbb{Z}_q$ uniformly at random. The ciphertext for a message $m \in G$ is the pair $(g^x, m \cdot y_B^x)$.

a) Describe the decryption of the ElGamal scheme, i.e., show how to obtain the message m given $(g^x, m \cdot y_B^x)$ and the secret key x_B.

b) Show that the ElGamal cryptosystem is IND-CPA secure under the DDH-assumption. More precisely, show that if there is an efficient distinguisher D that has advantage α in the IND-CPA game for public-key encryption, then there is an efficient distinguisher D' that given $(A, B, C) \in G^3$ has advantage $\alpha/2$ in distinguishing the case where A, B, C are independent and uniform in G from the case $A = g^a$, $B = g^b$, and $C = g^{ab}$ for uniform and independent $a, b \in \mathbb{Z}_q$.

c) Prove that the ElGamal scheme is not IND-CCA secure, that is, present an efficient attacker with non-negligible advantage in the IND-CCA game for public-key encryption.

4.2 On the (In)security of RSA

Goal*: We discuss attacks on the "textbook" version of the RSA cryptosystem and prove a related reduction.*

a) Consider the naive RSA public-key cryptosystem (Figure 2.12 in the lecture notes) with $e = 3$ in Bob's public key. Find a "large" subset of the message space such that an eavesdropper can efficiently recover any message of this set from the corresponding ciphertext and the public key.

b) We now want to show that any message from the message space can be recovered by an eavesdropper, if this message is sent to three different users who all use the exponent $e = 3$. More precisely, consider the naive RSA public-key cryptosystem with three different users, who have distinct moduli n_1, n_2, n_3, but all use the exponent $e = 3$. Assume some message is encrypted for these users and an attacker observes the resulting ciphertexts. Show how the attacker can efficiently compute the message from these ciphertexts and the public keys.

c) It is clear that one efficiently compute $\varphi(n)$ from a factorization of n (and thus compute the private exponent d and therefore decrypt all messages). Show that conversely, given n and $\varphi(n)$, one can efficiently find the two prime factors of n.

4.3 Homomorphic Public-Key Encryption

Goal*: We discuss encryption schemes with a homomorphic property and their limitations and use-cases.*

Let (E, d) denote the pair consisting of the encryption function E and the decryption function d of a public-key encryption scheme. We assume that the message space is identified with a finite abelian group $\langle \mathbb{G}; \circ \rangle$.

(E, d) is said to be *homomorphic* if for all key pairs $(pk, sk) \in \mathcal{P} \times \mathcal{S}$ in the support of the key-pair distribution, given two ciphertexts $c_1 := E(m_1, pk)$ and $c_2 := E(m_2, pk)$, one can efficiently compute a valid ciphertext c (with respect to the same public key pk) for the message $m' := m_1 \circ m_2$. This means that c is such that $d(c, sk) = m_1 \circ m_2$ (and in particular no secret key is required to obtain such a c).

a) Show that the ElGamal cryptosystem is homomorphic.

b) Show that the naïve RSA cryptosystem is homomorphic.

c) Assume a homomorphic encryption scheme (E, d). Show a concrete attacker for the CCA-game that guesses the bit b correctly with probability 1.

d) Describe in words an application scenario that makes reasonable use of a homomorphic encryption scheme (note that being homomorphic does not exclude CPA security, as the ElGamal system shows).

4.4 The Rabin Trapdoor One-Way Permutation

Goal*: We present a trapdoor one-way permutation provably based on the hardness of factoring.*

A quadratic residue modulo an integer n is an integer x such that there exists an integer y with $y^2 \equiv x \pmod{n}$.

For this exercise let p, q be two uniformly chosen primes smaller than some bound such that $p \equiv q \equiv 3 \pmod{4}$. Let $n = pq$.

a) List all elements in $\mathbb{Z}_{35}$ that are quadratic residues modulo 35.

b) Show that $\frac{1}{4}$ of the elements in $\mathbb{Z}_n^*$ are quadratic residues modulo n.
Hint: Use the Chinese remainder theorem: $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

c) Describe an easy algorithm to compute square roots modulo p. That is, an algorithm that given p and a quadratic residue x modulo p, it computes a y such that $y^2 \equiv x \pmod{p}$.

d) Show that the function $f : x \mapsto x^2 \bmod n$ is a permutation of the invertible quadratic residues modulo n, i.e. of the quadratic residues in $\mathbb{Z}_n^*$. Give an efficient algorithm that computes the inverse of f when the prime factors p and q of n are known.

e) Show that if you have an algorithm that inverts the permutation f of **a)** with probability $\alpha > 0$ for uniformly chosen inputs x then you can factor n with probability $1 - \varepsilon$ for every $\varepsilon > 0$.
Hint: Consider the equation $x^2 - y^2 = kn$.

Discussion of solutions:

19/20.3.2018 (Tasks 4.1 and 4.2)

26/27.3.2018 (Tasks 4.3 and 4.4)

The Monday and Tuesday sessions of each week cover the same material.