6.875J/18.425J Cryptography and Cryptanalysis	September 26, 2001

Handout 5: Problem Set 4

Instructor: Anna Lysyanskaya — *Teaching Assistant: Moses Liskov*

This problem set is due on Monday, October 15.

For these three problems, we want you to gain insight into the one-pass definition for GM-security. (This definition will be given in lecture 7, on October 1). For reference, we give the one-pass definition here. A cryptosystem (G, E, D) is (one-pass) GM-secure if

$\forall \{A_n\}\ \exists f \in neg$ such that $\forall k \in \mathbb{N}$
$\Pr[(PK, SK) \leftarrow G(1^k); (\alpha, m_0, m_1) \leftarrow A_k(PK); b \leftarrow \{0,1\};$
$\quad c \leftarrow E(PK, m_b); b' \leftarrow A_k(PK, c, m_0, m_1, \alpha) : b' = b] \leq 1/2 + f(k)$

For simplicity, could also write $b' \leftarrow A_k(c, \alpha)$ without loss of generality, since we could prescribe that α includes PK, m_0, and m_1.

Problem 1: Sampling Domain Security

Consider the following definition of security, which we call sampling domain security (SD security). Let (G, E, D) be a public-key cryptosystem, and let $\mathcal{M} = \{M_n\}$ be a sequence of message spaces, each with a uniform distribution. (G, E, D) is SD secure if there exists a probabilistic polynomial time algorithm S (for "sampling") such that

$\forall \{A_n\}\ \exists f \in neg$ such that $\forall k \in \mathbb{N}$
$\Pr[(PK, SK) \leftarrow G(1^k); m \leftarrow M_k; c_0 \leftarrow E(PK, m); c_1 \leftarrow S(1^k, PK);$
$\quad b \leftarrow \{0,1\}; b' \leftarrow A_k(PK, c_b, m) : b' = b] \leq 1/2 + f(k)$

The intuition behind this definition is that a cryptosystem is secure if no adversary can distinguish the encryption of a random message from a random sample from the domain sampled by S. Prove or disprove each of the following.

(a) If $M_n = \{0,1\}$ for every n, then GM-security implies SD security.

(b) If $M_n = \{0,1\}$ for every n, then SD security implies GM-security.

(c) If $M_n = \{0,1\}^n$ for every n, then GM-security implies SD security.

(d) If $M_n = \{0,1\}^n$ for every n, then SD security implies GM-security.

Problem 2: Random Message Security

Consider the following definition of security, which we call random message security (RM security). We say that a cryptosystem (G, E, D) on a sequence of message spaces $\mathcal{M} = \{M_n\}$ is RM secure if

$\forall \{A_n\}\ \exists f \in neg$ such that $\forall k \in \mathbb{N}$
$\Pr[(PK, SK) \leftarrow G(1^k); (\alpha, m) \leftarrow A_k(PK, 1^k); r \leftarrow M_k;$
$\quad c_0 \leftarrow E(PK, m); c_1 \leftarrow E(PK, r); b \leftarrow \{0,1\};$
$\quad b' \leftarrow A_k(PK, c_b, m, r) : b' = b] \leq 1/2 + f(k)$

The intuition behind this definition is that for any fixed message m it is infeasible to distinguish between an encryption of m and an encryption of some random message r.

Prove or disprove that for all polynomials p, for the sequence of message spaces $\{M_n = \{0,1\}^{p(n)}\}$, RM security is equivalent to GM security.

Problem 3: Security of ElGamal-A

Assume that one can, in probabilistic polynomial time, compute, on input 1^k, a k-bit prime p such that $p = 2q + 1$ where q is also prime. Consider the following cryptosystem, which is a variant of the ElGamal cryptosystem (to be attributed later), call it ElGamal-A.

Alice selects at random (1) a k-bit prime $p = 2q+1$ where q is also prime, (2) an element g in Z_p^* of order q, and (3) an x in $\mathbb{Z}_q^*$. Then, she sets her public key to be (p, g, h), where $h = g^x \bmod p$, and her secret key to be x.

Alice's public key restricts the message space to consist of all elements in Z_p^* having order q. To send such a message m to Alice, one picks an $r \leftarrow \mathbb{Z}_q$ and computes his ciphertext $c = (g^r \bmod p, h^r m \bmod p)$.

To decrypt $c = (a, b)$, Alice computes $b/(a^x) \bmod p$. (Exercise: verify that this indeed produces m.)

Call the procedure for generating p and g described above $\mathcal{DL}$. The *decisional Diffie-Hellman* assumption is as follows:

$\forall \{A_n\}\ \exists f \in neg$ such that $\forall k \in \mathbb{N}$
$\Pr[(p, g) \leftarrow \mathcal{DL}(1^n); x \leftarrow \mathbb{Z}_q^*; y \leftarrow \mathbb{Z}_q^*$
$\quad b \leftarrow \{0,1\}; z_0 \leftarrow xy \bmod q; z_1 \leftarrow \mathbb{Z}_q^*; b' \leftarrow A_k(p, g, g^x, g^y, g^{z_b}) : b' = b] \leq 1/2 + f(k)$

where $\{A_n\}$ is PPTF.[1]

Prove that under the decisional Diffie-Hellman assumption, the ElGamal-A cryptosystem is GM-secure.

[1] In other words, it is hard, given four elements of $\mathbb{Z}_p^*$, (g, g_1, g_2, g_3), each of order q, to determine whether the "discrete logarithm" of g_3 to the base g is the product of the discrete logarithms of g_1 and g_2, or just some random element in $\mathbb{Z}_q$. The name *decisional* Diffie-Hellman describes the relationship between this assumption and that made by Diffie and Hellman.