6.875J/18.425J Cryptography and Cryptanalysis	September 12, 2001
Handout 2: Problem Set 2	
Instructor: Anna Lysyanskaya	*Teaching Assistant: Moses Liskov*

This problem set will be due on Wednesday, September 26.

For reference, here is the definition of a GM-secure cryptosystem on a sequence of message spaces $\{M_n\}$. (G, E, D) is a GM-secure cryptosystem if the following two properties hold:

Faithfulness: (G, E, D) has faithfulness p (for $0 \leq p \leq 1$) if

$$\forall k, \forall m \in M_k, \forall (PK, SK) \in \text{Supp}(G(1^k))$$
$$\Pr[c \leftarrow E(PK, m); a \leftarrow D(SK, c) : a = m]$$
$$\geq p$$

GM-security: (G, E, D) is secure if

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

Problem 1

(40 points.) For each of the following definitions of security for a cryptosystem, compare them to GM-security. Some of the definitions may be too strong, that is, unattainable. If the definition is unattainable, prove it. Otherwise, for each definition you should prove or disprove that

1. If (G, E, D) is secure under that definition then it is GM-secure, and
2. If (G, E, D) is GM-secure then it is secure under the given definition.

(a) 2^{-k} *security.* Do we need to be so general about the negligible function?

$$\forall \{A_n\} \in PPT \; \exists K \in \mathbb{N} \text{ such that } \forall k > K,$$
$$\Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow \{0,1\};$$
$$c \leftarrow E(PK, b); b' \leftarrow A_k(PK, c) : b' = b] \leq 1/2 + 2^{-k}$$

(b) *Almost-all-parameter security.* Do *all* sufficiently large k have to work?

$$\forall \{A_n\} \in PPT \; \exists f \in neg, K \in \mathbb{N} \text{ such that } \forall k > K \text{ such that } k \neq 2^i \text{ for any } i,$$
$$\Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow \{0,1\};$$
$$c \leftarrow E(PK, b); b' \leftarrow A_k(PK, c) : b' = b] \leq 1/2 + f(k)$$

(c) *All-parameter security.* Do we need the assertion that k has to be sufficiently large?

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

(d) *All-message security.* Do we need to pick the message randomly during the protocol?

$\forall \{A_n\} \in PPT\ \exists f \in neg, K \in \mathbb{N}\ \ \forall k > K\ \forall b \in \{0,1\}$,
$Pr[(PK, SK) \leftarrow G(1^k);$
$c \leftarrow E(PK, b); b' \leftarrow A_k(PK, c) : b' = b] \leq 1/2 + f(k)$

(e) *Ciphertext game security.* Can we define security differently: say a cryptosystem is secure if the chance an adversary determines a message given its encryption is only negligibly better than the probability that the adversary determines the message given a random encryption of some kind?

$\forall \{A_n\} \in PPT\ \exists f \in neg, K \in \mathbb{N}\ \ \forall k > K$,
$\Pr[(PK, SK) \leftarrow G(1^k); b_0, b_1 \leftarrow \{0,1\}$
$c \leftarrow E(PK, b_0); b' \leftarrow A_k(PK, c) : b' = b_0] -$
$\Pr[(PK, SK) \leftarrow G(1^k); b_0, b_1 \leftarrow \{0,1\}$
$c \leftarrow E(PK, b_1); b' \leftarrow A_k(PK, c) : b' = b_0] \leq f(k)$

Problem 2

For any $0 \leq q \leq 1/2$, let the notation "$x \leftarrow \{q : a, b\}$" denote that with probability q, the value of x becomes a, and with probability $1 - q$, the value of x becomes b. The following is a definition of q-GM-security for a cryptosystem (G, E, D), given a sequence of message spaces $\{M_n\}$:

$\forall \{A_n\} \in PPT\ \exists f \in neg\ \ \forall k \in \mathbb{N}, \forall \{m_0, m_1\} \in M_k$
$\Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow \{q : 0, 1\};$
$c \leftarrow E(PK, m_b, 1^k); b' \leftarrow A_k(PK, c, m_0, m_1) :$
$b = b'] < 1 - q + f(k)$

(20 points.) Prove that if for any $0 < q \leq 1/2$, the Goldwasser-Micali cryptosystem is q-GM-secure, then it is GM-secure.

Problem 3

(20 points.) Is q-GM-security equivalent to GM-security? Prove or disprove each[1]: For any $0 < q \leq 1/2$, q-GM-security implies GM-security; for any $0 < q \leq 1/2$, GM-security implies q-GM-security.

[1] To prove A-security implies B-security, you must prove that if (G, E, D) is A-secure, then it is also B-secure. To disprove that A-security implies B-security, you may (and will need to) assume that an A-secure cryptosystem (G, E, D) exists. Based on that assumption you must then construct a cryptosystem (G', E', D') which is A-secure but is not B-secure.

Problem 4

(20 points.) Prove that if there exists a GM-secure cryptosystem (G, E, D) then $P \neq NP$. For simplicity, you may assume that (G, E, D) has faithfulness 1.