6.875J/18.425J Cryptography and Cryptanalysis	September 26, 2001
Handout 4: Problem Set 3	
Instructor: Anna Lysyanskaya	*Teaching Assistant: Moses Liskov*

This problem set is due on Wednesday, October 3.

Problem 1: Random-bit hybrid argument

Recall the theorem from lecture, that if (G', E', D') is a GM-secure cryptosystem operating on 1-bit messages, then (G, E, D) is a GM-secure cryptosystem operating on l-bit messages where l is some polynomial on k, and where (G, E, D) just uses (G', E', D') to encrypt a longer message bit-by-bit. That is,

$G(1^k)$:
  1. Return output of $G'(1^k)$

$E(PK, m = b_1 \circ b_2 \circ \ldots \circ b_l)$:
  1. For each $1 \leq i \leq l$, compute $c_i = E'(PK, m_i)$
  2. Return $c_1 \circ c_2 \circ \ldots \circ c_l$

$D(SK, c = c_1 \circ \ldots c_l)$:
  1. For each $1 \leq i \leq l$, compute $b_i = D'(SK, c_i)$
  2. Return $m = b_1 \circ \ldots \circ b_l$.

In class, we gave a reduction R from an algorithm that breaks the GM-security of (G, E, D) to one that breaks the GM-security of (G', E', D'), as follows. Let $m_0 = b_1 \circ \ldots b_l$ and let $m_1 = b'_1 \circ \ldots \circ b'_l$, and let the i^{th} hybrid m^i be $m^i = b'_1 \circ \ldots \circ b'_i \circ b_{i+1} \circ \ldots \circ b_l$.

$R(m_0, m_1, A, PK, c, k)$:
  1. Test A to determine an i for which A distinguishes between encryptions of m^i and m^{i+1}.
  2. For $1 \leq j \leq i$, compute $c'_j = E'(PK, b'_j)$
  3. Set $c'_{i+1} = c$
  4. For $i + 1 \leq j \leq l$, compute $c'_j = E'(PK, b_j)$
  5. Return $b' = A(PK, c'_1 \circ \ldots \circ c'_l, m_0, m_1)$

We proved that if A succeeds in distinguishing encryptions of m_0 from m_1 with probability $1/2 + 1/p(k)$, then R succeeds in decrypting c with probability $1/2 + 1/l \cdot p(k)$.

Consider the following, simpler, reduction R'.

$R'(m_0, m_1, A, PK, c, k)$:
  1. Pick i at random from the range $[0, l]$.
  2-5. Do exactly what R does.

Prove that if A is an adversary that breaks the GM-security of (G, E, D) on messages m_0, m_1, then R' provides an adversary that breaks the GM-security of (G', E', D'). (*Hint:*

Previously, we showed that $\exists i$ such that steps 2-5 of the reduction work with probability $1/2 + 1/l \cdot p(k)$. Here, you should prove that $\Pr_i$ that steps 2-5 of the reduction work is at least $1/2 + 1/q(k)$, for some other polynomial $q(k)$, based on $p(k)$.)

Problem 2: Moses Security

Recall that the Hamming weight of a binary string is the number of 1s in that string. Let $\mathcal{H}_k^i$ be the set of all strings of length exactly k and of Hamming weight exactly i.

We say that a cryptosystem (G, E, D) is i-Moses secure if

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

The intuition behind this definition is that for two strings which differ in exactly i bits, it is impossible to distinguish the encryption of one from the encryption of the other.

(a) Prove or disprove: For all odd i, i-Moses security is equivalent to GM-security.

(b) Prove or disprove: For all even i, i-Moses security is equivalent to GM-security.