6.875/18.425J Cryptography and Cryptanalysis February 17, 2005

Handout 5: Problem Set #2

This problem set is due on: Tuesday, March 1, 2005.

Problem 1 - OWF Reductions

Assume that f is a length preserving one-way function. (i.e, $f : \{0,1\}^k \to \{0,1\}^k$). For each of the following functions g, prove or disprove the statement: "g is a one-way function." (Note: $\bar{x}$ denotes the bitwise complement of x and $|$ denotes concatenation, e.g. $1011|\overline{1011} = 10110100$.)

A: $g(x) = f(f(x))$

B: $g(x) = f(\bar{x})$

C: $g(x, y) = f(x \oplus y)$

D: $g(x) = f(x)|f(\bar{x})$

Problem 2 - GM Implies OWF

Prove that the existence of a GM-secure cryptosystem (G, E, D) implies the existence of a one-way function.

Problem 3 - Notions of One-Bit Security

Consider the definition of security for a one-bit cryptosystem which was presented in class:

Unpredictability:

$$\forall PPT\ A\ \forall c > 0, \exists k_0 \text{ s.t. } \forall k > k_0$$

$$\Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow \{0,1\}; x \leftarrow E_{PK}(b); g \leftarrow A(1^k, PK, x) : b = g] < \frac{1}{2} + \frac{1}{k^c}$$

Here are two other possible definitions of security for a one-bit cryptosystem.

Indistinguishability: The intuition behind this definition is that an adversary (with binary output) should not be able to distinguish an encryption of 1 from an encryption of 0.

$$\forall PPT\ A\ \forall c > 0, \exists k_0 \text{ s.t. } \forall k > k_0$$
$$\Pr[(PK, SK) \leftarrow G(1^k); x \leftarrow E_{PK}(0); y \leftarrow E_{PK}(1) : A(1^k, PK, x) \neq A(1^k, PK, y)] < \frac{1}{2} + \frac{1}{k^c}$$

Real or Random: The intuition behind this definition is that an adversary should not be able to tell the encryption of a real message from the encryption of a random bit.

$$\forall PPT\ A\ \forall c > 0, \exists k_0 \text{ s.t. } \forall k > k_0$$
$$\Pr[(PK, SK) \leftarrow G(1^k); x_0 \leftarrow E_{PK}(0); r \leftarrow \{0,1\}; x_1 \leftarrow E_{PK}(r);$$
$$b \leftarrow \{0,1\}; g \leftarrow A(1^k, PK, x_b, x_{1-b}) : b = g] < \frac{1}{2} + \frac{1}{k^c}$$

The intuition behind this definition is that an adversary should not be able to tell the difference between the encryption of a real bit and the encryption of a random bit.

Prove that all three definitions are equivalent.

Problem 4 - Ciphertext Expansion

The GM Quadratic Residuosity Cryptosystem (which we discussed in lecture) is GM-Secure but it expands the size of a message by a factor of k (where k is the security parameter). RSA encryption, on the other hand, is not GM-Secure but has the desirable property that the ciphertext is the same length as the plaintext. Prove that no GM-secure public-key cryptosystem (G,E,D) can satisfy the latter property. Namely, prove that, if the message space is $M = \{0,1\}^m$, then the average length of a ciphertext generated by (G,E,D) with security parameter k is $\geq m + \log k$.