COS 433 — Cryptography — Homework 2.

Boaz Barak

Total of 120 points. Due October 4th, 2007.

Exercise 1 (20 points)**.** Prove that if (E, D) is a computationally secure encryption with $\ell(n)$-long messages then for every polynomial-time algorithm Eve and large enough n, the probability that Eve wins in the following game is smaller than 0.34:

1. Eve gets as input 1^n, and gives Alice three strings $x_0, x_1, x_2 \in \{0,1\}^{\ell(n)}$.
2. Alice chooses a random key $k \leftarrow_{\mathrm{R}} \{0,1\}^n$ and $i \leftarrow_{\mathrm{R}} \{0,1,2\}$ and computes $y = \mathsf{E}_k(x_i)$.
3. Eve gets y as input, and outputs an index $j \in \{0,1,2\}$.
4. Eve *wins* if $j = i$.

Note: This proof can be generalized to show that the probability Eve guesses which one of c messages was encrypted is at most $1/c + \mu(n)$ where μ is a negligible function (see also Exercise 6). It can also be shown that computational security implies many other reasonable conditions of security. For example, the KL book shows that if a message x is chosen at random, then the probability that a polynomial-time adversary can compute the i^{th} bit of x from an encryption of x is at most $1/2 + \mu(n)$ for a negligible μ (of course, she can always compute that bit with probability half by randomly guessing). This can also be generalized to show that for example that the probability that an adversary guesses the first c bits of x from an encryption of x is at most $2^{-c} + \mu(n)$ for a negligible μ.

Exercise 2 (20 points)**.** Prove the equivalence of the two definition of computational security we gave in class. That is, prove that an encryption scheme (E, D) with $\ell(n)$-long messages is C/S1 iff it is C/S2, where these two notions are defined as follows:

C/S1 (E, D) is C/S1 if for every polynomial-time Adv and polynomially bounded $\epsilon : \mathbb{N} \to [0,1]$, large enough n, and $x_0, x_1 \in \{0,1\}^{\ell(n)}$,

$$\left|\Pr[\mathsf{Adv}(\mathsf{E}_{U_n}(x_0)) = 1] - \Pr[\mathsf{Adv}(\mathsf{E}_{U_n}(x_1)) = 1]\right|$$

C/S2 (E, D) is C/S1 if for every polynomial-time Eve and polynomially bounded $\epsilon : \mathbb{N} \to [0,1]$, large enough n, the probability that Eve wins the following game is at most $1/2 + \epsilon(n)$: **1.** Eve gets as input 1^n, and gives Alice two strings $x_0, x_1 \in \{0,1\}^{\ell(n)}$ **2.** Alice chooses a random key $k \leftarrow_{\mathrm{R}} \{0,1\}^n$ and $i \leftarrow_{\mathrm{R}} \{0,1,2\}$ and computes $y = \mathsf{E}_k(x_i)$, **3.** Eve gets y as input, and outputs an index $j \in \{0,1\}$, **4.** Eve *wins* if $j = i$.

Exercise 3 (30 points)**.** For each of the following statements decide whether it's true or false, and prove it or give a counterexample:

1. If (E,D) is a perfectly secure encryption then it is also computationally secure.

2. If (E,D) is a computationally secure encryption then it is also perfectly secure.

3. If (E,D) is a computationally secure encryption with n-sized key and $\ell(n)$-sized messages then the following encryption scheme $(\mathsf{E}',\mathsf{D}')$ with n-sized key and $2\ell(n)$-sized messages is also computationally secure: To encrypt the string $x = x_1 \ldots x_{2\ell(n)}$ with key $k \in \{0,1\}^n$, $\mathsf{E}'_k(x) = \mathsf{E}_k(x_1 \ldots x_{\ell(n)}) \circ \mathsf{E}_k(x_{\ell(n)+1} \ldots x_{2\ell(n)})$, where $\circ$ denotes string concatenation. (Decryption is done in the obvious way.)

4. If (E,D) is a computationally secure encryption with n-sized key and $\ell(n)$-sized messages then the following encryption scheme $(\mathsf{E}',\mathsf{D}')$ with $2n$-sized key and $2\ell(n)$-sized messages is also computationally secure: To encrypt the string $x = x_1 \ldots x_{2\ell(n)}$ with key $k \in \{0,1\}^{2n}$, $\mathsf{E}'_k(x) = \mathsf{E}_{k_1 \ldots k_{\ell(n)}}(x_1 \ldots x_{\ell(n)}) \circ \mathsf{E}_{k_{\ell(n)+1} \ldots k_{\ell(n)}}(x_{\ell(n)+1} \ldots x_{2\ell(n)})$, where $\circ$ denotes string concatenation. (Decryption is done in the obvious way.)

Exercise 4 (20 points)**.** Prove the following properties of computational indistinguishability:

1. It's weaker than statistical indistinguishability: if for every n, $\Delta(X_n, Y_n) \leq \epsilon(n)$ for some negligible function $\epsilon : \mathbb{N} \to \mathbb{N}$ (i.e., $\epsilon(n) = n^{-\omega(1)}$) then $\{X_n\} \approx \{Y_n\}$. (Recall that Δ denotes statistical distance.)

2. If $\{X_n\} \approx \{Y_n\}$ and $f : \{0,1\}^* \to \{0,1\}^*$ is a function computable in polynomial time, then $\{f(X_n)\} \approx \{f(Y_n)\}$.

Exercise 5 (20 points)**.**

1. Let X, Y, X', Y' be four distributions over $\{0,1\}^n$ such that $\Delta(X,Y) \leq \epsilon$ and $\Delta(X',Y') \leq \epsilon$. Prove that $\Delta(X \circ X', Y \circ Y') \leq 10\epsilon$, $X \circ X'$ denotes the distribution obtained by concatenating two independent samples from X and X', and $Y \circ Y'$ is defined analogously. See footnote for hint[1]

2. Let $\{X_n\}, \{X'_n\}, \{Y_n\}, \{Y'_n\}$ be four sequences of distributions such that $\{X_n\} \approx \{Y_n\}$ and $\{X'_n\} \approx \{Y'_n\}$, prove that $\{X_n \circ X'_n\} \approx \{Y_n \circ Y'_n\}$. See footnote for hint[2]

Exercise 6 (10 points)**.** Recall that we defined a function $\epsilon : \mathbb{N} \to [0,1]$ to be *polynomially bounded* if $\epsilon(n) = n^{-O(1)}$ (equivalently, $\log(1/e(n)) = O(\log n)$) and *negligible* if $\epsilon(n) = n^{-\omega(1)}$ (equivalently, $\log(1/\epsilon(n)) = \omega(\log n)$). Let $\{A_n\}$ be a sequence of probabilistic events. Prove that the following two conditions are equivalent:

- For every polynomially bounded $\epsilon : \mathbb{N} \to [0,1]$ and large enough n, $\Pr[A_n] \leq \epsilon(n)$.
- There exists a negligible function $\mu : \mathbb{N} \to [0,1]$ such that $\Pr[A_n] \leq \mu(n)$ for every n.

Note: This exercise means that in making various game-type definitions, instead of saying "for every polynomially-bounded ϵ and large enough n, the probability that Eve wins is at most $1/2 + \epsilon(n)$", we can equivalently say "for every n, the probability that Eve wins is at most $1/2 + \mu(n)$ where μ is some negligible function"

[1] **Hint:** Use the definition of statistical distance based on functions, and the following simple fact: if f is a function mapping $\{0,1\}^{2n}$ to $\{0,1\}$ and Z and W are two independent distributions over $\{0,1\}^n$ such that $\Pr[f(Z,W) = 1] \geq p$, then there exists a fixed string z in the support of Z such that $\Pr[f(z,W) = 1] \geq p$.

[2] **Hint:** use the fact that "hardwiring" of advice to the adversary/distinguisher is allowed.