INTRODUCTION TO MODERN CRYPTOGRAPHY
KU BLOCK 1A, 2016-17

HOMEWORK 2
DUE: 10/4/16 8:30AM

GORJAN ALAGIC

Instructions.

- Collaboration is encouraged, but each student *must* understand and write up their own solution set entirely by themselves.
- All answers must be accompanied by complete and clearly explained proofs. A correct answer with no explanation will receive a zero score.
- Your goal in proofs is to convince *me* that your answer is correct, and that you understand why it is correct. It is difficult to do this without words. As in all writing, these words should almost always come in complete sentences.
- For open-ended (e.g., yes/no) questions, think carefully about what constitutes a "proof" that your response is correct. Sometimes, all it takes is a counterexample.
- If you are using a theorem proved in class, indicate it clearly by name (or just restate it.) Theorems from outside class are ok to cite, so long as they are not about cryptography. If you want to use a theorem from cryptography, you have to include the proof.

Problems.

(1) Recall the following from class.

Definition 0.1. *Let X and Y be two random variables, taking values in $\{0,1\}^*$. We say that the distributions of X and Y are* ***computationally indistinguishable*** *if for all probabilistic polynomial-time algorithms $\mathcal{A}$,*

$$|\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Y) = 1]| \leq \mathsf{negl}(n)\,.$$

We say that a symmetric-key encryption scheme (SKES) satisfies *computational indistinguishability of ciphertexts* if for every pair of plaintexts (m_0, m_1), the distributions $\{\mathsf{Enc}_k(m_0)\}_k$ and $\{\mathsf{Enc}_k(m_1)\}_k$ for $k \leftarrow \mathsf{KeyGen}$ are computationally indistinguishable.

Prove that an SKES satisfies IND if and only if it satisfies computational indistinguishability of ciphertexts.

(2) Prove that a symmetric-key encryption scheme satisfies IND if and only if it satisfies semantic security (Definition 3.12 in Katz and Lindell).

(3) Prove that PRGs are enough to satisfy a limited form of multiple-message security:
   (a) Write down a variant of the definition of IND-mult, where no adversary can send more than $t(n)$ pairs of plaintexts, for some fixed polynomial function t which depends only on the scheme.

(b) Prove that, if pseudorandom generators exist, then there is a (stateful) scheme that satisfies your definition. For this problem, do not assume the existence of pseudorandom functions.

(4) Prove that information-theoretic IND-CPA is impossible:
   (a) Following the definition of IND for perfect secrecy, and the definition of IND-CPA for computational secrecy, devise a definition of IND-CPA for perfect secrecy.
   (b) Prove that this definition cannot be met by any scheme.

(5) Prove that, if pseudorandom functions exist, then so do pseudorandom generators.

(6) Let $F : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^l$ be a keyed function, and consider this experiment:
   1. Choose a uniform $b \in \{0,1\}$ and a uniform $k \in \{0,1\}^n$.
   2. The adversary $\mathcal{A}$ receives 1^n as input. If $b = 0$ then $\mathcal{A}$ receives access to a uniformly random function $f : \{0,1\}^m \to \{0,1\}^l$. Otherwise $\mathcal{A}$ receives access to F_k.
   3. $\mathcal{A}$ outputs a bit b', and wins if and only if $b' = b$.

   Write down a definition of pseudorandom function (PRF) based on the above experiment. Then prove that your definition is equivalent to the one given in lecture (Definition 3.25 in Katz and Lindell.)

(7) Let Π be a MAC, and let n denote the key length. Suppose that the tag length $t(n)$ satisfies $t(n) = O(\log n)$. Prove that Π is not a secure MAC.

(8) Prove that the ECB and CBC modes of operation for block ciphers do not yield IND-CCA-secure encryption, regardless of the choice of pseudorandom permutation.

Department of Mathematical Sciences, University of Copenhagen
E-mail address: galagic@gmail.com