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

HOMEWORK 1
DUE: TUESDAY 20/09/2016 8:30AM

GORJAN ALAGIC

Instructions.

- Collaboration with other students in class is allowed (and 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 lecture 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) A formal description of an encryption scheme requires a precise mathematical description of the key, plaintext, and ciphertext spaces, and likewise for the key generation, encryption, and decryption algorithms. Following the definition of "simple encryption scheme" we gave in class (see also the example of the one-time pad,) give a formal description of:
   (a) the Caesar cipher;
   (b) the substitution cipher;
   (c) the Vigènere cipher;
   ...using your favorite alphabet.

(2) Suppose you and your friend come up with a new language that uses the English alphabet. Since you know about frequency analysis, you carefully construct the language so that the letter frequency is uniform (i.e., for long messages, A appears with approximately the same frequency as B, and as C, etc.) You then use the substitution cipher to communicate in your new language.
   (a) Give a formal description of this scheme. Does it differ substantially from the standard substitution cipher? If so, how?
   (b) Is this a secure scheme? If yes, sketch a proof of security. If no, describe an explicit attack and explain why it works.

(3) Let $V_{f(n)}$ denote the Vigènere cipher with passphrase length n and plaintext length $f(n)$. Characterize the set X consisting of all functions $f : \mathbb{N} \to \mathbb{N}$ such that $V_{f(n)}$ is perfectly secure. Remember to provide proofs in both cases (i.e., prove that it is secure for each

$f \in X$, and prove that it is insecure for all $f \notin X$.)

(4) Prove that we can assume, without loss of generality, that any simple encryption scheme (as defined in the lecture on perfect security) satisfies
   (a) the KeyGen algorithm samples uniformly at random from $\mathcal{K}$;
   (b) the Enc algorithm is completely deterministic.
   To do this, show that you can transform any scheme Π into another scheme Π' with the same output distribution as Π (i.e., $\Pr_k[\mathsf{Enc}_k(m) = c]$ is unchanged for all m and all c) but which satisfies both (a) and (b).

(5) Let $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme, and fix a probability distribution on $\mathcal{M}$. Let M denote the resulting random variable, taking values in $\mathcal{M}$. Let C denote the corresponding random variable on ciphertexts, i.e., C is the result of choosing a plaintext m according to our distribution on $\mathcal{M}$, then choosing a key k by running KeyGen, and finally outputting $\mathsf{Enc}_k(m)$. Now prove that the following definition of security is equivalent to the notion of perfect security from lecture.

   Definition 0.1. *An encryption scheme is* ***semantically secret*** *if, for every probability distribution on $\mathcal{M}$, we have*

$$\Pr[M = m | C = c] = \Pr[M = m]$$

   for all $m \in \mathcal{M}$ and all $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$.

(6) A **polynomial-time reduction** from a language $A \subset \{0,1\}^*$ to a language $B \subset \{0,1\}^*$ is a function $f : \{0,1\}^* \to \{0,1\}^*$ satisfying $w \in A \Leftrightarrow f(w) \in B$, together with a deterministic polynomial-time Turing Machine which computes f. Prove that the class P of all polynomial-time decidable languages is closed under polynomial-time reductions.

(7) Prove the following facts about negligible functions:
   (a) The sum of two negligible functions is a negligible function.
   (b) The product of a negligible function with a positive polynomial is a negligible function.
   (c) If an experiment succeeds with negligible probability, then repeating the experiment any polynomial number of times will still succeed with only negligible probability.

(8) Let $G : \{0,1\}^* \to \{0,1\}^*$ be a function satisfying $|G(s)| = \ell(|s|)$ for some ℓ. Consider this experiment:
   1. Choose a uniform $b \in \{0,1\}$. If $b = 0$ choose uniform $r \in \{0,1\}^{\ell(n)}$; otherwise choose uniform $s \in \{0,1\}^n$ and set $r = G(s)$.
   2. The adversary $\mathcal{A}$ receives r and outputs a bit b'.
   3. We say $\mathcal{A}$ wins if and only if $b' = b$.

   Write down a definition of pseudorandom generator (PRG) based on the above experiment. Prove that your definition is equivalent to the one given in lecture (Definition 3.14 in Katz and Lindell.)

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