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

HOMEWORK 3
DUE: TUESDAY 25/10/2016 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 Construction 4.18 from Katz and Lindell, where one constructs a new encryption scheme Π from an encryption scheme Π_E and a MAC Π_M. Recall that we proved in class that, if Π_E is IND-CPA and Π_M is EUF-CMA, then Π is IND-CCA.

Prove that, if Π_M is EUF-CMA, then Π is unforgeable (Definition 4.16.) Your proof should not require any security from Π_E.

(2) Let f be a one-way function.
   (a) Prove that the function f' defined by $f'(x) = f(x)\,||\,0^n$ (where $n = |x|$) is also a one-way function.
   (b) Prove that the function g defined by $g(x, y) = (f(x), y)$ (where $|x| = |y|$) is also a one-way function.

(3) Prove that, if there exists a one-way function, then there exists a one-way function f such that $f(0^n) = 0^n$ for every n.

(4) We say that a sequence $\{X_n\}_{n\in\mathbb{N}}$, where X_n is a distribution over $\{0,1\}^n$, is *pseudorandom* if it's computationally indistinguishable from the sequence $\{U_n\}$ where U_n is the uniform distribution over $\{0,1\}^n$.
   (a) Let G be a pseudorandom generator with expansion $\ell(n) = n + 1$. Prove that the sequence $\{G(U_{n-1})\}_{n\in\mathbb{N}}$ is pseudorandom.

(b) Let X_n (for each n) be the distribution where we choose bits $x_1, x_2, \ldots, x_{n-1}$ uniformly at random, then let x_n be the XOR of $x_1, x_2, \ldots, x_{n-1}$, and finally output $x_1, x_2, \ldots, x_n$. Prove or disprove: $\{X_n\}$ is pseudorandom.

(c) Let X_n (for each n) be the following sequence of distributions. If $n < 1000000$, we output uniformly random elements of $\{0,1\}^n$. If $n \geq 1000000$, then with probability 2^{-n} we output "This is not a pseudorandom sequence" (encoded in binary and padded by zeroes); otherwise we again output uniformly random elements of $\{0,1\}^n$. Prove or disprove: $\{X_n\}$ is pseudorandom.

(5) Let f and h be two functions. Define a function G by $G(s) = f(s) \,||\, h(s)$. Prove or disprove: if f is a one-way *function* and h is a hard-core predicate of f, then G is a pseudorandom generator.

(6) Prove that the k-round Feistel network is a permutation for all $k \in \mathbb{N}$, regardless of the round functions used.

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