Cryptography, winter term 16/17: Assignment 5

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due December 07, 2016[1]

Exercise 5.1 (Warm up, 5 Bonus Points) Decide for each of the following statements whether it is true or false. Explain your answer *briefly.*

(a) Perfect indistinguishability and perfect secrecy are equivalent.

(b) For all events A and B it holds that

$$\Pr[A] = \Pr[A|B]\Pr[B] + \Pr[A \wedge \neg B]$$

(c) Given a PRF F_k, the function $F'_k(x) := F_k(x)||F_k(x)$ is also a PRF.

(d) It is possible to construct an encryption scheme with a keyspace of constant size that has indistinguishable encryptions in the presence of an eavesdropper.

(e) It is possible to construct an encryption scheme that is perfectly secret but not CPA-secure.

Exercise 5.2 (Basic Probability, 4 Bonus Points) Assume you are a TA in the cryptography lecture and you want to pose a fair multiple choice exercise in the midterm exam. There will be n questions and each question has 4 options from which exactly one is correct. This exercise will be graded as follows:
A correct answer will give 1 point. An answer is correct if the right option was chosen *and no other option was.* An invalid answer will give 0 points. An answer is invalid if no or more than one option was chosen. To avoid the possibility of guessing, a wrong answer will give $-k$ points. An answer is wrong if exactly one wrong option was picked. Your task is to compute the value of k such that a student who picks one option of each question uniformly at random will get 0 points in expectation.

Exercise 5.3 (Composition of PRGs, 4 Bonus Points) Let G_1 and G_2 be PRGs with expansion factors ℓ_1 and ℓ_2, respectively. Prove that $G(s) := G_1(G_2(s))$ is a PRG with expansion factor $\ell(n) = \ell_1(\ell_2(n))$.

Exercise 5.4 (Modification of CBC, 4 Bonus Points) Consider the variant of CBC-mode where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

[1]The purpose of this assignment is preparation for the midterm exam. Submission is not mandatory and all points you can gather are bonus points. Solutions will be presented on December 07 during the lecture.