Cryptography, winter term 16/17: Assignment 4

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

Due November 30, 2016

Exercise 4.1 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 4.2 (CTR mode, 4 Points) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be the CTR mode encryption scheme and let $\widetilde{\Pi} = (\widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}}, \widetilde{\mathsf{Dec}})$ be the encryption scheme obtained from Π by using a truly random function f instead of a pseudorandom function F_k.[1] Show that there is a negligible function negl, such that for any PPT adversary $\mathcal{A}$, it holds that

$$\left|\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] - \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\widetilde{\Pi}}(n) = 1]\right| \leq \mathsf{negl}(n)$$

Exercise 4.3 (Indistinguishability and CPA-security, 8 Points) Let F be a PRF and G be a PRG with expansion factor $n \mapsto n + 1$. For each of the following encryption schemes, decide whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

(a) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

(b) The one-time pad.

(c) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(d) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2| = n$, then choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Exercise 4.4 (Birthday paradox, 4 Points) Let $k \leq n$. You are in a room with k people, and everyone is born on one out of n possibly dates, i.e., the typical terrestrial case asks for $n = 365$ (ignoring leap years). What is, for arbitrary n and k, the probability that at least two people have the same birthday, assuming that the dates of birth are uniformly distributed and independent of each other?

Additionally, for $n = 365$, what is the smallest number of people k such that this probability is at least $\frac{1}{2}$?

[1] That is to say that $\widetilde{\mathsf{Gen}}$ picks uniformly $f \in \mathsf{Func}_n$ where Gen picks uniformly $k \in \{0,1\}^n$, and $\widetilde{\mathsf{Enc}}$ uses f where Enc uses F_k.