Cryptography, winter term 16/17: Sample solution to assignment 5

Cornelius Brand, Marc Roth

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.

Solution 5.1 (Warm up, 5 Bonus Points) a) Yes, proof was e.g. on sheet 2.

b) Yes, by definition of conditional probability, the first product is just $\Pr A \cap B$, and now by additivity of $\Pr\cdot$, the claim follows (since $(A \cap B) \cup (A \cap \neg B) = A$).

c) No, because every y in the image of F'_k has the property that $y_i = y_{i+|y|/2}$ for $1 \leq i \leq |y|/2$, which a random string has only with negligible probability.

d) No, the adversary can brute-force the key.

e) Yes, e.g. the one-time-pad.

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.

Solution 5.2 (Basic Probability, 4 Bonus Points) By linearity of expectation and the fact that $0 + 0 = 0$, it suffices to show that the expected gain of a student is 0 for a single question. The correct answer is picked with probability $1/4$, and gives one point. Thus, the expectation is $\frac{1}{4} \cdot 1 - \frac{3}{4}k$. Setting this expression to 0 and solving for k yields $k = 1/3$.

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 $\ell(n) = \ell_1(\ell_2(n))$.

Solution 5.3 (Composition of PRGs, 4 Bonus Points) First, note that if ℓ_1 and ℓ_2 are polynomials, then $\ell_1 \circ \ell_2 =: p$ is one as well. Assume we had a distinguisher D for $G_1 \circ G_2$ that succeeds with probability, say, $\frac{1}{q(n)}$ for some positive polynomial q.

We claim that this enables us to construct a distinguisher D_2 for G_2 as follows: Upon input x, D_2 just runs $D(G_1(x))$ and returns its answer. We analyse the success probability:

$$
\begin{aligned}
&\left|\Pr_{s\in\{0,1\}^n}[D_2(G_2(s)) = 1] - \Pr_{r\in\{0,1\}^{\ell_2(n)}}[D_2(r) = 1]\right| = \\
&\left|\Pr_{s\in\{0,1\}^n}[D(G_1(G_2(s))) = 1] - \Pr_{r\in\{0,1\}^{\ell_2(n)}}[D(G_1(r)) = 1]\right| = \\
&\left|\Pr_{s\in\{0,1\}^n}[D(G(s)) = 1] - \Pr_{r\in\{0,1\}^{\ell_2(n)}}[D(G_1(r)) = 1]\right| = \\
&|\Pr_{s\in\{0,1\}^n}[D(G(s)) = 1] - \Pr_{r\in\{0,1\}^{\ell_1(\ell_2(n))}}[D(r) = 1] \\
&+ \Pr_{r\in\{0,1\}^{\ell_1(\ell_2(n))}}[D(r) = 1] - \Pr_{r\in\{0,1\}^{\ell_2(n)}}[D(G_1(r)) = 1]| \geq \\
&\left|\Pr_{s\in\{0,1\}^n}[D(G(s)) = 1] - \Pr_{r\in\{0,1\}^{\ell_1(\ell_2(n))}}[D(r) = 1]\right| \\
&- \left|\Pr_{r\in\{0,1\}^{\ell_1(\ell_2(n))}}[D(r) = 1] - \Pr_{r\in\{0,1\}^{\ell_2(n)}}[D(G_1(r)) = 1]\right| \\
&\geq \frac{1}{q(n)} - \mathsf{negl}(p(n))
\end{aligned}
$$

where the first inequality follows from the reverse triangle inequality $|x + y| \geq |x| - |y|$, and the second from the assumption on D and the fact that we know that G_1 is a pseudorandom generator, and hence D can only have success probability bounded by $\mathsf{negl}(\ell_1(\ell_2(n)) = \mathsf{negl}(p(n))$, which is again negligible.

The proof is finished by noting that $\frac{1}{q(n)} - \mathsf{negl}(n)$ is non-negligible for all positive polynomials q and negligible functions negl.

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.

Solution 5.4 (Modification of CBC, 4 Bonus Points) We design an adversary $\mathcal{A}$ that wins over guessing with non-negligible probability. It proceeds as follows:

a) Query the encryption oracle with $m = 0^{n-1}1$ and receive a ciphertext $\langle IV, c\rangle$.

b) If IV is odd, i.e. has as last bit 1, then output a random bit

c) If IV is even, i.e. has as last bit 0, then output $m_0 = 0^n$ and arbitrary m_1 to be encrypted.

d) Receive the challenge ciphertext $\langle IV+1, c'\rangle$, and output 0 if $c' = c$, and 1 otherwise.

We claim that this adversary succeeds with probability that is greater than $1/2$ by a non-negligible function (in fact, even a constant). First, by guessing randomly, $\mathcal{A}$ succeeds with probability $\frac{1}{2}$ if IV is odd, which is $\frac{1}{4}$ of the cases.

If IV is even, then $IV + 1 = IV \oplus 0^{n-1}1$. Therefore, $c = F_k(IV \oplus m_0) = F_k(IV \oplus 0^{n-1}1) = F_k(IV+1) = F_k(IV+1\oplus 0) = F_k((IV+1)\oplus m_0)$, and so if m_0 was encrypted, then $c = c'$. On the other hand, if m_1 was encrypted, then $c \neq c'$. That is, whenever IV is even, $\mathcal{A}$ decides correctly which message was encrypted. This covers exactly $\frac{1}{2}$ of the cases. In total, this shows that $\mathcal{A}$ wins in $\frac{3}{4}$ of all cases.