Cryptography, winter term 16/17:
Sample solution to the Midterm Exam

Cornelius Brand, Marc Roth

Please read the following remarks first!

a) Please use a non-erasable black or blue pen.

b) You can answer in English or German.

c) Write your name and your Matriculation number on every sheet that you hand in.

d) You can refer to every result in the lecture notes and to every regular exercise unless it is explicitly forbidden.

e) Finally, fill in your personal data. Good luck.

Name: _____

Matriculation number: _____

Exercise	max.	achieved
1	12	
2	7	
3	8	
4	15	
Σ	42	

Exercise No.1 (Warm up) *(2 points for each answer)*
Decide for each of the following statements whether it is true or false. Prove your answer *briefly*, i.e., two or three sentences should be enough.

(a) The one-time pad remains perfectly secret if we exclude the key 0^n.

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

$$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A]\Pr[B]$$

(c) Every perfectly secret encryption scheme is also CPA-secure.

(d) Given a PRG G, the following function G' is also a PRG:

$$G'(s) := G(s)||s$$

(e) Every encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper is CPA-secure.

(f) Every encryption scheme that is not CPA-secure has deterministic encryption.

Solution No.1 (Warm up) All answers are false:

(a) Excluding the keys 0^n will lead to a key space that is smaller than the message space. Therefore the scheme cannot be perfectly secret.

(b) This is wrong as A and B need not to be independent.

(c) This is wrong as the one-time pad is not CPA-secure (as it has deterministic encryptions)

(d) Let ℓ be the expansion factor of G and consider the following distinguisher: On input $t \in \{0,1\}^{\ell(n)+n}$, output 1 if and only if $G(t_{\ell(n)+1} \dots t_{\ell(n)+1}) = t_1 \dots t_{\ell(n)}$. This distinguisher will output 1 on input $G(s)||s$ with probability 1 but it will output 1 on input r for a randomly chosen r only with negligible probability. Therefore the construction does not yield a PRG.

(e) The one-time pad is again a counter example.

(f) This is wrong as not every randomised encryption yields CPA-security. (e.g.: $\mathrm{Enc}_k(m) := (r, m \oplus r)$ for a randomly chosen r).

Exercise No.2 (PRGs) *(7 points)*
Let G be a PRG with expansion factor $\ell(n) > n$ and let $f : \{0,1\}^* \to \{0,1\}^*$ be a length-preserving bijection (i.e., a permutation) such that f is computable in deterministic polynomial time and define G' as follows:

$$G'(s) := f(G(s))$$

Show that G' is also a PRG.

Solution No.2 (PRGs) From the definition it follows that the expansion factor of G' is also ℓ. We prove the claim by reduction: Assuming G' is not a PRG, there is a ppt distinguisher D' for G' such that there is a polynomial q such that for all n

$$\left|\Pr_{s\leftarrow\{0,1\}^n}[D'(G'(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D'(r) = 1]\right| > \frac{1}{q(n)}\,. \tag{1}$$

We construct a distinguisher D for G from D' as follows: On input t, D just simulates $D'(f(t))$, that is, D outputs 1 if and only if D' does on input $f(t)$. As D' is ppt and f is polynomial time computable it follows that D is also ppt. Now we have that for all n:

$$\begin{aligned}
&\left|\Pr_{s\leftarrow\{0,1\}^n}[D(G(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D(r) = 1]\right| \\
=&\left|\Pr_{s\leftarrow\{0,1\}^n}[D'(f(G(s))) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D'(f(r)) = 1]\right| \\
=&\left|\Pr_{s\leftarrow\{0,1\}^n}[D'(G'(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D'(f(r)) = 1]\right| \\
=&\left|\Pr_{s\leftarrow\{0,1\}^n}[D'(G'(s)) = 1] - \Pr_{r'\leftarrow\{0,1\}^{\ell(n)}}[D'(r') = 1]\right| \\
>&\frac{1}{q(n)}
\end{aligned}$$

where the third equality follows from the fact that f is a length-preserving bijection and the inequality follows from (1).
This contradicts the fact that G is a PRG which completes the proof.

Exercise No.3 (PRFs) *(8 points)*
Consider the following keyed function F: For security parameter n, the key is a pair (k_1, k_2) where $k_1, k_2 \in \{0,1\}^n$. Define $F_{(k_1,k_2)} : \{0,1\}^n \to \{0,1\}^n$ by

$$F_{(k_1,k_2)}(x) := k_1 \oplus x \oplus k_2$$

Show that F is not a PRF.

Solution No.3 (PRFs) We construct a distinguisher D as follows: On input 1^n and having access to oracle $\mathcal{O}$, D queries $m_0 := \mathcal{O}(0^n)$ and $m_1 := \mathcal{O}(1^n)$. After that, D checks whether $m_0 \oplus m_1 = 1^n$ and outputs 1 accordingly.
If $\mathcal{O} = F_{(k_1,k_2)}$ for some (randomly chosen) k_1, k_2, we have that

$$m_0 \oplus m_1 = \mathcal{O}(0^n) \oplus \mathcal{O}(1^n) = k_1 \oplus 0^n \oplus k_2 \oplus k_1 \oplus 1^n \oplus k_2 = 1^n$$

and therefore

$$\Pr_{\substack{k_1 \leftarrow \{0,1\}^n \\ k_2 \leftarrow \{0,1\}^n}}[D^{F_{(k_1,k_2)}(\cdot)}(1^n) = 1] = 1\,.$$

Now if $\mathcal{O}$ is a truly random function f, we have that $f(0^n)$ and $f(1^n)$ are random strings and hence $f(0^n) \oplus f(1^n)$ is also. This implies that

$$\Pr_{f \leftarrow \mathrm{func}_n}[D^{f(\cdot)}(1^n) = 1] = 2^{-n}\,.$$

We conclude that

$$\left| \Pr_{\substack{k_1 \leftarrow \{0,1\}^n \\ k_2 \leftarrow \{0,1\}^n}}[D^{F_{(k_1,k_2)}(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow \mathrm{func}_n}[D^{f(\cdot)}(1^n) = 1] \right| = 1 - 2^{-n}$$

which is clearly not negligible. It follows that F is not a PRF.

Exercise No.4 (Perfect secrecy and indistinguishable encryptions)

(a) *(4 points)* Let func_n be the set of all functions $f : \{0,1\}^n \to \{0,1\}^n$ and consider the following encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:

- On input 1^n, Gen outputs an $f \in \mathrm{func}_n$ uniformly at random.
- Given a key $f \in \mathrm{func}_n$ and a message $m \in \{0,1\}^n$, Enc outputs the ciphertext $c = m \oplus f(0^n)$.
- Given a key $f \in \mathsf{func}_n$ and a ciphertext $c \in \{0,1\}^n$, Dec outputs the plaintext $m = c \oplus f(0^n)$.

Prove that Π is perfectly secret. (You can use any characterization of perfect secrecy that was introduced in the lecture.)

(b) *(10 points)* Now let F_k be a length-preserving PRF and consider the following encryption scheme $\Pi' = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:

- On input 1^n, Gen outputs an $k \in \{0,1\}^n$ uniformly at random.
- Given a key k and a message $m \in \{0,1\}^n$, Enc outputs the ciphertext $c = m \oplus F_k(0^n)$.
- Given a key k and a ciphertext $c \in \{0,1\}^n$, Dec outputs the plaintext $m = c \oplus F_k(0^n)$.

Prove that Π' has indistinguishable encryptions in the presence of an eavesdropper. You may use the result from part (a).
Hint: It may be advisable to prove (by reduction) that the existence of an adversary that wins the adversarial indistinguishability experiment with probability non-negligibly greater than $\frac{1}{2}$ can be used to show that F_k is not a PRF.

(c) *(1 point)* Prove or disprove: Π' is CPA-secure.

Solution No.4 (Perfect secrecy and indistinguishable encryptions) (a) We know from the lecture that the one-time pad is perfectly secret , and one can see as follows that the encryption scheme is simply a different way of defining the one-time pad: Guessing a function $f : \{0,1\}^n \to \{0,1\}^n$ is the same as guessing 2^n elements from $\{0,1\}^n$ (i.e., guessing the image of every element in the domain). We can interpret the outcome of this such that the first string is the image of 0^n under f, which is then nothing else as a random element from $\{0,1\}^n$.

This means that picking $f(0^n)$ for uniformly random f is the same as picking uniformly at random some $k \in \{0,1\}^n$. The encryption scheme is then identical to the one-time pad, as claimed.

(b) Let $\mathcal{A}$ be an adversary for the adversarial indistinguishability experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi'}$, and assume $\mathcal{A}$ wins with probability non-negligibly greater than $\frac{1}{2}$, say

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi'} = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$$

for some positive polynomial p. We want to show how to use this to distinguish F_k from a truly random function, and we can do this as follows: Construct a distinguisher D that on input 1^n performs the experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\cdot}$ step-by-step, simulating the adversary $\mathcal{A}$ during the process and using the oracle $\mathcal{O}$ for encryption:

(1) Simulate the adversary $\mathcal{A}$ on input 1^n until it outputs the messages m_0, m_1

(2) Choose uniformly at random a bit $b \in \{0,1\}$ and generate the challenge ciphertext $c \leftarrow \mathcal{O}(0^n) \oplus m_b$

(3) Continue simulating $\mathcal{A}$ on c, until it outputs a bit b'

(4) Output 1 if $b' = b$ and 0 otherwise.

Clearly, since $\mathcal{A}$ is PPT, so is D. Additionally, by the very definition of $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\cdot}$, D behaves exactly like $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ or $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi'}$, depending on what $\mathcal{O}$ is, such that

$$\Pr_{k\in\{0,1\}^n}[D^{F_k(\cdot)} = 1] = \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi'}] = 1]$$

and

$$\Pr_{f\in\mathsf{func}_n}[D^{f(\cdot)} = 1] = \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]\,.$$

Then, since perfect secrecy implies that

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}\,,$$

we have

$$\Pr_{f\in\mathsf{func}_n}[D^{f(\cdot)} = 1] = \frac{1}{2}\,,$$

and thus

$$\begin{aligned}
&\left|\Pr_{k\in\{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f\in\mathsf{func}_n}[D^{f(\cdot)}(1^n) = 1]\right| = \\
&\left|\Pr_{k\in\{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] - \frac{1}{2}\right| \geq \\
&\Pr_{k\in\{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] - \frac{1}{2} \geq \\
&\frac{1}{2} + \frac{1}{p(n)} - \frac{1}{2} = \frac{1}{p(n)}
\end{aligned}$$

which is non-negligible.

(c) It cannot be, since encryption happens deterministically.