Cryptography, winter term 16/17:
Sample solution to the Endterm 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	10	
2	8	
3	15	
4	10	
5	10	
6	7	
Σ	60	

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) Combining a CCA secure KEM and a *perfectly secret* private-key encryption scheme via the hybrid construction[1] yields a *perfectly secret* public-key encryption scheme.

(b) CCA-secure private-key encryption schemes exist *unconditionally* in the random-oracle model.

(c) Let $a, b, s, t, s', t' \in \mathbb{Z}$ such that $gcd(a, b) = as + bt = as' + bt'$. Then, $s = s'$ and $t = t'$.

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

(e) Plain RSA is a CPA-secure public-key encryption scheme.

Solution No.1 (Warm up)

a) False, there are no perfectly secret public key encryption schemes.

b) True, in the random-oracle model PRFs exist and hence CPA-secure private key encryption schemes and strongly secure MACs exists and therefore, by encrypt-then-authenticate, CCA secure private key encryption schemes exist as well.

c) False, for a variety of reasons. For instance, if $a = b$, then $gcd(a, a) = a = 1 \cdot a + 0 \cdot a = 2 \cdot a - 1 \cdot a$. Even if $a \neq b$, then all pairs $(s', t') = (s + k \cdot \frac{b}{gcd(a,b)}, t - k \cdot \frac{a}{gcd(a,b)})$ satsify the equation for $k \in \mathbb{Z}$.

d) True, this was shown in the lecture.

e) False, several attacks were shown in the lecture.

[1] Let $\Pi = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ be a KEM and $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be a private-key encryption scheme. Then the hybrid construction yields a public-key encryption scheme $\Pi^{\mathsf{hy}} = (\mathsf{Gen}^{\mathsf{hy}}, \mathsf{Enc}^{\mathsf{hy}}, \mathsf{Dec}^{\mathsf{hy}})$ defined as follows:

- $\mathsf{Gen}^{\mathsf{hy}}$ outputs $(\mathsf{pk}, \mathsf{sk})$ obtained by running Gen.
- $\mathsf{Enc}^{\mathsf{hy}}$, given pk and a message m, runs $\mathsf{Encaps}_{\mathsf{pk}}$ to obtain (c, k), then runs ${\mathsf{Enc}'}_k(m)$ to obtain c' and outputs (c, c').
- $\mathsf{Dec}^{\mathsf{hy}}$, given sk and a ciphertext (c, c'), computes $k := \mathsf{Decaps}_{\mathsf{sk}}(c)$ and outputs $m := {\mathsf{Dec}'}_k(c')$.

Exercise No.2 (PRGs) *(8 points)*
Let G be a PRG with expansion factor $\ell(n) = n + 1$. Prove that for every constant $c \in \mathbb{N}, c > 0$ there exists a PRG G_c with expansion factor $\ell_c(n) = n + c$.
Hint: It may be advisable to do a proof by induction on c.

Solution No.2 (PRGs) This can be proven by induction on c. For $c = 1$ we can set $G_1 = G$ which is a PRG with expansion factor $\ell(n) = n + 1$ by assumption.
For the induction step, we assume that there already exists a PRG G_c with expansion factor $\ell_c(n) = n + c$ (induction hypothesis) and we need to construct a PRG G_{c+1} with expansion factor $\ell_{c+1}(n) = n + c + 1$. We set $G_{c+1} := G \circ G_c$. It clearly holds that G_{c+1} has the desired expansion factor. For the pseudorandomness it suffices to know that the concatenation of two PRGs is a PRG. This result was shown in the preparatory assignment for the midterm exam and may be used. However, we will do the proof (by reduction) for the sake of completeness:
We assume that G_{c+1} is not a PRG. Then there exists a distinguisher D for G_{c+1} such that

$$|\mathsf{Pr}_{s\in\{0,1\}^n}[D(G_{c+1}(s)) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c+1}}[D(r) = 1]| \geq \frac{1}{q(n)}$$

for a polynomial q. We claim that this enables us to construct a distinguisher D_c for G_c as follows: Upon input x, D_c computes $D(G(x))$ and returns its answer. We analyse the success probability:

$$\begin{aligned}
&\left|\mathsf{Pr}_{s\in\{0,1\}^n}[D_c(G_c(s)) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c}}[D_c(r) = 1]\right| = \\
&\left|\mathsf{Pr}_{s\in\{0,1\}^n}[D(G(G_c(s))) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c}}[D(G(r)) = 1]\right| = \\
&\left|\mathsf{Pr}_{s\in\{0,1\}^n}[D(G_{c+1}(s)) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c}}[D(G(r)) = 1]\right| = \\
&|\mathsf{Pr}_{s\in\{0,1\}^n}[D(G_{c+1}(s)) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c+1}}[D(r) = 1] \\
&+ \mathsf{Pr}_{r\in\{0,1\}^{n+c+1}}[D(r) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c}}[D(G(r)) = 1]| \geq \\
&|\mathsf{Pr}_{s\in\{0,1\}^n}[D(G_{c+1}(s)) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c+1}}[D(r) = 1]| \\
&- |\mathsf{Pr}_{r\in\{0,1\}^{n+c+1}}[D(r) = 1] - \mathsf{Pr}_{r\in\{0,1\}^{n+c}}[D(G(r)) = 1]| \geq \\
&\geq \frac{1}{q(n)} - \mathsf{negl}(n + c)
\end{aligned}$$

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 is a pseudorandom generator. Finally, $\frac{1}{q(n)} - \mathsf{negl}(n + c)$ is not negligible.

Exercise No.3 (PRFs) *(3+12 points)*
Let F be a keyed function and consider the following experiment:

The PRF indistinguishability experiment $\mathsf{PRF}_{\mathcal{A},F}(n)$:

(1) *Choose* $b \in \{0,1\}$ *uniformly at random.*

(2) *If* $b = 0$ *then choose a uniform* $k \in \{0,1\}^n$ *and let* $\mathcal{O} = F_k$*. Otherwise let* $\mathcal{O} = f$ *for* $f \in \mathsf{func}_n$ *chosen uniformly at random.*

(3) *The adversary* $\mathcal{A}$ *is given* 1^n *as input and access to oracle* $\mathcal{O}$*, and outputs a bit* b'*.*

(4) *The output of the experiment is* 1 *if* $b' = b$ *and* 0 *otherwise.*

(a) Give an alternative definition of pseudorandom functions based on this experiment.

(b) Prove that your definition from (a) is equivalent to the definition of pseudorandom functions used in the lecture.

Solution No.3 (PRFs) We say that a keyed function F is a PRF if for every ppt adversary $\mathcal{A}$:

$$\mathsf{Pr}[\mathsf{PRF}_{\mathcal{A},F}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$$

for a negligible function negl. To prove that this definition is equivalent, we need to show both implications:

(1) Let F be a keyed function satisfying the definition above. Given a ppt distinguisher $D^{\mathcal{O}}$ with oracle access to $\mathcal{O}$ we denote $\overline{D}^{\mathcal{O}}$ as the algorithm with oracle access to $\mathcal{O}$ that simulates $D^{\mathcal{O}}$ and then flips the output, that is

$$\forall t : D^{\mathcal{O}}(t) = 1 \leftrightarrow \overline{D}^{\mathcal{O}}(t) = 0\,.$$

Now we need to show that $|\mathsf{Pr}[D^{F(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1]|$ is negligible. First, assume that

$$\mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] \geq \mathsf{Pr}[D^{F(\cdot)}(1^n) = 1]\,.$$

Then it holds that

$$\begin{aligned}
&|\mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1]| \\
&= \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] \\
&= \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] - (1 - \mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 0]) \\
&= \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] + \mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 0] - 1 \\
&= 2 \cdot \left(\frac{1}{2}\mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] + \frac{1}{2}\mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 0]\right) - 1 \\
&= 2 \cdot (\mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRF}_{D,F}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRF}_{D,F}(n) = 1 \mid b = 0]) - 1 \\
&= 2 \cdot \mathsf{Pr}[\mathsf{PRF}_{D,F}(n) = 1] - 1 \\
&\leq 2 \cdot \left(\frac{1}{2} + \mathsf{negl}(n)\right) - 1 \\
&= 2 \cdot \mathsf{negl}(n)
\end{aligned}$$

which is also negligible. Now assume that

$$\mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] < \mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1]\,.$$

Then we have

$$\begin{aligned}
&|\mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1]| \\
&= \mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] \\
&= \mathsf{Pr}[\overline{D}^{F_k(\cdot)}(1^n) = 0] - \mathsf{Pr}[\overline{D}^{f(\cdot)}(1^n) = 0] \\
&= \mathsf{Pr}[\overline{D}^{F_k(\cdot)}(1^n) = 0] - (1 - \mathsf{Pr}[\overline{D}^{f(\cdot)}(1^n) = 1]) \\
&= \mathsf{Pr}[\overline{D}^{f(\cdot)}(1^n) = 1] + \mathsf{Pr}[\overline{D}^{F_k(\cdot)}(1^n) = 0] - 1 \\
&= 2 \cdot \left(\frac{1}{2}\mathsf{Pr}[\overline{D}^{f(\cdot)}(1^n) = 1] + \frac{1}{2}\mathsf{Pr}[\overline{D}^{F_k(\cdot)}(1^n) = 0]\right) - 1 \\
&= 2 \cdot \Big(\mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRF}_{\overline{D},F}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRF}_{\overline{D},F}(n) = 1 \mid b = 0]\Big) - 1 \\
&= 2 \cdot \mathsf{Pr}[\mathsf{PRF}_{\overline{D},F}(n) = 1] - 1 \\
&\leq 2 \cdot \left(\frac{1}{2} + \mathsf{negl}(n)\right) - 1 \\
&= 2 \cdot \mathsf{negl}(n)
\end{aligned}$$

which is also negligible. This concludes the proof of the first direction.

(2) Now let F be a keyed function that is a PRF with respect to the definition of the lecture. We have to show that F satisfies the definition above. Let $\mathcal{A}$ be a ppt adversary. Then it holds that

$$\begin{aligned}
&\mathsf{Pr}[\mathsf{PRF}_{\mathcal{A},F}(n) = 1] \\
&= \mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRF}_{\mathcal{A},F}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRF}_{\mathcal{A},F}(n) = 1 \mid b = 0] \\
&= \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}^{f(\cdot)}(1^n) = 1] + \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}^{F_k(\cdot)}(1^n) = 0] \\
&= \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}^{f(\cdot)}(1^n) = 1] + \frac{1}{2} \cdot (1 - \mathsf{Pr}[\mathcal{A}^{F_k(\cdot)}(1^n) = 1]) \\
&= \frac{1}{2} + \frac{1}{2}(\mathsf{Pr}[\mathcal{A}^{f(\cdot)}(1^n) = 1] - \mathsf{Pr}[\mathcal{A}^{F_k(\cdot)}(1^n) = 1]) \\
&\leq \frac{1}{2} + \frac{1}{2}|\mathsf{Pr}[\mathcal{A}^{f(\cdot)}(1^n) = 1] - \mathsf{Pr}[\mathcal{A}^{F_k(\cdot)}(1^n) = 1]| \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot \mathsf{negl}(n)
\end{aligned}$$

which concludes the proof.

Exercise No.4 (MACs) *(6+1+3 points)*

(a) Let F_k be a PRF and let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a MAC defined as follows:

- Gen outputs a uniform $k \in \{0,1\}^n$.
- $\mathsf{Mac}_k(m) := (F_k(m)||F_k(m))$
- $\mathsf{Vrfy}_k(m,t)$ outputs 1 if and only if $t = (F_k(m)||F_k(m))$

Prove that Π is a secure MAC.
Remark: You may use *without proof* that the following MAC $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ is secure:

- Gen' outputs a uniform $f \in \mathsf{func}_n$.
- $\mathsf{Mac}'_f(m) := (f(m)||f(m))$
- $\mathsf{Vrfy}'_f(m,t)$ outputs 1 if and only if $t = (f(m)||f(m))$

(b) Is Π from (a) also strongly secure? Explain your answer.

(c) Prove or disprove: If $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a strongly secure MAC then Mac is a pseudorandom function.

Solution No.4 (MACs)

a) We do a proof by reduction. Assuming Π is not secure yields the existence of an adversary $\mathcal{A}$ such that

$$\mathsf{Pr}[\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}(n) = 1] > \frac{1}{p(n)}$$

for a polynomial p. We construct a distinguisher D as follows: On input 1^n and with access to oracle $\mathcal{O}$, D simulates $\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}(n)$. Whenever $\mathcal{A}$ queries $\mathsf{Mac}_k(m)$, D returns $\mathcal{O}(m)||\mathcal{O}(m)$. Finally D outputs 1 if $\mathcal{A}$ wins and 0 otherwise. Then it holds that $\mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] = \mathsf{Pr}[\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi}(n) = 1] > \frac{1}{p(n)}$ and $\mathsf{Pr}[D^{f(\cdot)}(1^n) = 1] = \mathsf{Pr}[\mathsf{Mac\text{-}forge}_{\mathcal{A},\Pi'}(n) = 1] \leq \mathsf{negl}(n)$. Therefore

$$\left|\mathsf{Pr}[D^{F_k(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1]\right| \geq \frac{1}{p(n)} - \mathsf{negl}(n)$$

which is not negligible.

b) Yes, because it uses canonical verification.

c) This does not hold. Π from (a) is strongly secure but $m \to F_k(m)||F_k(m)$ is not a PRF. To prove this, let D be a distinguisher that, given 1^n as input and oracle access to $\mathcal{O}$, computes $t = \mathcal{O}(0^n)$ and checks whether $t_1 \dots t_{\frac{|t|}{2}} = t_{\frac{|t|}{2}+1} \dots t_{|t|}$. Then it holds that

$$\left|\mathsf{Pr}[D^{\mathsf{Mac}(\cdot)}(1^n) = 1] - \mathsf{Pr}[D^{f(\cdot)}(1^n) = 1]\right| = 1 - 2^{-n}$$

which is not negligible.

Exercise No.5 (Key-exchange protocols) *(5+5 points)*
Let Π be a key exchange protocol.

(a) Prove that two executions of Π with the same transcript result in the same key. More precisely, let (trans, k) be the outcome of an execution of Π. Prove that every execution of Π with transcript trans outputs k.

(b) We say that Π is *perfectly secure* if for every[2] adversary $\mathcal{A}$ it holds that

$$\mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}\,.$$

Prove that a perfectly secure key-exchange protocol cannot exist.
Remark: You may use the result of (a) even if you did not solve it.

Solution No.5 (Key-exchange protocols)

a) Let A and B be the two parties of Π. Now we say that $(s_a, s_b, \mathsf{trans}, k)$ is a *trace* of Π if the execution of Π with random bits s_a used by A and random bits s_b used by B yields transcript trans and key k. Now assume that there is a transcript trans such that k_1 and k_2 are valid keys with respect to trans. Then there exist $s_a^1, s_b^1, s_a^2, s_b^2$ such that $T_1 = (s_a^1, s_b^1, \mathsf{trans}, k_1)$ and $T_2 = (s_a^2, s_b^2, \mathsf{trans}, k_2)$ are traces of Π. Now assume Π is executed and A uses random bits s_a^1 and B uses random bits s_b^2 and let m_1 be the first message A sends to B. As $(s_a^1, s_b^1, \mathsf{trans}, k_1)$ is a trace of Π is follows that m_1 is also the first message of trans. From then on B behaves as in T_2 and A behaves as in T_1 as both send messages according to trans by assumption. This yields A outputting k_1 and B outputting k_2 which implies that $k_1 = k_2$.

b) We construct an adversary $\mathcal{A}$ that wins the experiment with probability $> \frac{1}{2}$ for every key-exchange protocol Π. First let $r(n)$ be the number of random bits used by Alice and Bob during the key exchange for security parameter n.

(1) On input trans and $\hat{k} \in \{0,1\}^n$, $\mathcal{A}$ enumerates all bitstrings $s \in \{0,1\}^{r(n)}$.

(2) For every s, $\mathcal{A}$ simulates the Π with random bits s. This yields a transcript trans_s and a key k_s. If $\hat{k} = k_s$ and $\mathsf{trans} = \mathsf{trans}_s$ then $\mathcal{A}$ outputs 0 and terminates. Otherwise it continues.

(3) If no s yields termination, then $\mathcal{A}$ outputs 1.

We observe that, given trans and a valid key k, $\mathcal{A}$ will eventually find a sequence of random bits whose simulation will end up in k. Therefore

$$\mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] = 1$$

where b is the bit choosen in the KE experiment. Furthermore it clearly holds that

$$\mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] > 0$$

[2] That is, $\mathcal{A}$ has unbounded computational resources.

as otherwise every $k \in \{0,1\}^n$ would be valid for any transcript trans which is impossible by (a). Therefore it holds by the law of total probability:

$$\begin{aligned}
\mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] &= \frac{1}{2} \cdot \mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] + \frac{1}{2} \cdot \mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] \\
&> \frac{1}{2} \cdot \mathsf{Pr}[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] \\
&= \frac{1}{2} \cdot 1 = \frac{1}{2}
\end{aligned}$$

Exercise No.6 (Digital signatures) *(7 points)*
Consider the Lamport signature scheme. Describe an adversary who obtains signatures on two messages of its choice and can then forge signatures on any message it likes.

Solution No.6 (Digital signatures) By the definition of sk, for messages of length ℓ, requesting the signatures of 0^ℓ and 1^ℓ gives the two rows of sk.