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

Cornelius Brand, Marc Roth

Please read the following remarks first!

a) This is a sample exam. It gives a general flavour of the type of exercises you should expect for the final exam.

b) We will not correct or grade your solutions, and there are no points to be gained. However, we will present the solutions in the last week of lectures.

c) To assess your performance optimally, try to solve the exercises only with the help of your prepared cheat sheet within two hours.

d) If you are not admitted to the exam yet, it is possible to get bonus points for submitting a solution of the sample exam on Wednesday, February 15th before the lecture. Please contact a TA if you would like to make use of this option.

Name: _____

Matriculation number: _____

Exercise	max.	achieved
1	10	
2	8	
3	15	
4	10	
5	7	
6	10	
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) Every perfectly secret private key encryption scheme has indistinguishable encryptions in the presence of an eavesdropper.

(b) CCA secure private key encryption schemes exist if pseudorandom functions exist.

(c) Let $a, b, c \in \mathbb{Z}$. Then, $gcd(gcd(a, b), c) = gcd(a, gcd(b, c))$.

(d) The Miller-Rabin test always outputs `composite` on input a number N whenever N is composite.

(e) Given a CPA secure KEM, it is possible to construct a CPA secure public key encryption scheme in the random-oracle model.

Solution No.1 (Warm up) (a) True. A scheme is perfectly secret if it wins the eav-experiment with probability *exactly* $\frac{1}{2}$ (for every security parameter n) which is certainly smaller than $\frac{1}{2} + \mathsf{negl}$ for a negligible function negl.

(b) True. If pseudorandom functions exist then we can construct CPA secure private key encryption schemes as in the canonical construction. Furthermore we can construct strongly secure MACs. Combining both via encrypt-then-authenticate yields a CCA secure private key encryption scheme.

(c) True. Let $d = gcd(gcd(a, b), c), d' = gcd(a, gcd(b, c))$. Then d divides c and $gcd(a, b)$, hence d divides a, b, c and thus, d divides $gcd(b, c)$. Therefore, divides $gcd(a, gcd(b, c)) = d'$. The direction $d'|d$ follows in the same way, hence $d = d'$.

(d) False. This holds only with high probability. If the algorithm always chooses a non-witness by chance, the algorithm might in fact output `prime` although the number is composite.

(e) True. In the random-oracle model PRFs exist. Therefore CPA secure private key encryption schemes exists. Combining one of those with the CPA secure KEM via the hybrid construction yields a CPA secure public key encryption scheme.

Exercise No.2 (Perfect secrecy) *(8 points)*
In this problem we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$; we let M_1 , M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.) We generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \mathsf{Enc}_k(m_1)$ and $c_2 \leftarrow \mathsf{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables. We say that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

is *perfectly secret for two messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\mathsf{Pr}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathsf{Pr}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathsf{Pr}[M_1 = m_1 \wedge M_2 = m_2]$$

Prove that no such encryption scheme can exist.

Solution No.2 (Perfect secrecy) The idea is that two different messages cannot be mapped to the same ciphertext by Enc_k. Let c be a ciphertext such that

$$\mathsf{Pr}[C_1 = c \wedge C_2 = c] > 0\,.$$

Now just let $m_1 \neq m_2$ for $m_1, m_2 \in \mathcal{M}$ and take the uniform distribution over $\mathcal{M}$. It holds that

$$\mathsf{Pr}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c \wedge C_2 = c] = 0$$

as there is no decryption error in private key encryption schemes. Furthermore we have that

$$\mathsf{Pr}[M_1 = m_1 \wedge M_2 = m_2] = \frac{1}{|\mathcal{M}|^2} \neq 0$$

which concludes the proof.

Exercise No.3 (PRGs) *(15 points)*
Let G be a function with expansion factor ℓ and consider the following experiment:

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

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

(2) *If* $b = 1$ *then choose a uniform* $r \in \{0,1\}^{\ell(n)}$ *and let* $t := r$*. Otherwise let* $t := G(s)$ *for* $s \in \{0,1\}^n$ *choosen uniformly at random.*

(3) *The adversary* $\mathcal{A}$ *is given* t*, and outputs a bit* b'*.*

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

Define a pseudorandom generator based on this experiment and prove that your definition is equivalent to the definition used in the lecture.

Solution No.3 (PRGs) We say that G is a PRG if $\ell(n) > n$ and for every ppt adversary $\mathcal{A}$:

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

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

(1) Let G be a function satisfying the definition above. We first note that $\ell(n) > n$ is satisfied. Now, given a ppt distinguisher D we denote D^c as the algorithm that simulates D and then flips the output, that is

$$\forall t : D(t) = 1 \leftrightarrow D^c(t) = 0\,.$$

Now we need to show that $|\mathsf{Pr}[D(G(s) = 1] - \mathsf{Pr}[D(r) = 1]|$ is negligible. First, assume that

$$\mathsf{Pr}[D(r) = 1] \geq \mathsf{Pr}[D(G(s) = 1]\,.$$

Then it holds that

$$\begin{aligned}
&|\mathsf{Pr}[D(G(s) = 1] - \mathsf{Pr}[D(r) = 1]| \\
&= \mathsf{Pr}[D(r) = 1] - \mathsf{Pr}[D(G(s)) = 1] \\
&= \mathsf{Pr}[D(r) = 1] - (1 - \mathsf{Pr}[D(G(s)) = 0]) \\
&= \mathsf{Pr}[D(r) = 1] + \mathsf{Pr}[D(G(s)) = 0] - 1 \\
&= 2 \cdot \left(\frac{1}{2}\mathsf{Pr}[D(r) = 1] + \frac{1}{2}\mathsf{Pr}[D(G(s)) = 0]\right) - 1 \\
&= 2 \cdot (\mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRG}_{D,G}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRG}_{D,G}(n) = 1 \mid b = 0]) - 1 \\
&= 2 \cdot \mathsf{Pr}[\mathsf{PRG}_{D,G}(n) = 1] - 1 \\
&\leq 2 \cdot \left(\frac{1}{2} + \mathsf{negl}(n)\right) - 1 \\
&= 2 \cdot \mathsf{negl}(n)
\end{aligned}$$

which is also negligible. Now assume that

$$\mathsf{Pr}[D(r) = 1] < \mathsf{Pr}[D(G(s) = 1]\,.$$

Then we have

$$\begin{aligned}
&|\mathsf{Pr}[D(G(s) = 1] - \mathsf{Pr}[D(r) = 1]| \\
&= \mathsf{Pr}[D(G(s)) = 1] - \mathsf{Pr}[D(r) = 1] \\
&= \mathsf{Pr}[D^c(G(s)) = 0] - \mathsf{Pr}[D^c(r) = 0] \\
&= \mathsf{Pr}[D^c(G(s)) = 0] - (1 - \mathsf{Pr}[D^c(r) = 1]) \\
&= \mathsf{Pr}[D^c(r) = 1] + \mathsf{Pr}[D^c(G(s)) = 0] - 1 \\
&= 2 \cdot \left(\frac{1}{2}\mathsf{Pr}[D^c(r) = 1] + \frac{1}{2}\mathsf{Pr}[D^c(G(s) = 0]\right) - 1 \\
&= 2 \cdot (\mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRG}_{D^c,G}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRG}_{D^c,G}(n) = 1 \mid b = 0]) - 1 \\
&= 2 \cdot \mathsf{Pr}[\mathsf{PRG}_{D^c,G}(n) = 1] - 1 \\
&\leq 2 \cdot \left(\frac{1}{2} + \mathsf{negl}(n)\right) - 1 \\
&= 2 \cdot \mathsf{negl}(n)
\end{aligned}$$

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

(2) Now let G be a function that is a PRG with respect to the definition of the lecture. We have to show that G satisfies the definition above. First note that $\ell(n) > n$ holds by definition. Now let $\mathcal{A}$ be a ppt adversary. Then it holds that

$$\begin{aligned}
&\mathsf{Pr}[\mathsf{PRG}_{\mathcal{A},G} = 1] \\
&= \mathsf{Pr}[b = 1] \cdot \mathsf{Pr}[\mathsf{PRG}_{\mathcal{A},G}(n) = 1 \mid b = 1] + \mathsf{Pr}[b = 0] \cdot \mathsf{Pr}[\mathsf{PRG}_{\mathcal{A},G}(n) = 1 \mid b = 0] \\
&= \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}(r) = 1] + \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}(G(s)) = 0] \\
&= \frac{1}{2} \cdot \mathsf{Pr}[\mathcal{A}(r) = 1] + \frac{1}{2} \cdot (1 - \mathsf{Pr}[\mathcal{A}(G(s)) = 1]) \\
&= \frac{1}{2} + \frac{1}{2}(\mathsf{Pr}[\mathcal{A}(r) = 1] - \mathsf{Pr}[\mathcal{A}(G(s)) = 1]) \\
&\leq \frac{1}{2} + \frac{1}{2}|\mathsf{Pr}[\mathcal{A}(r) = 1] - \mathsf{Pr}[\mathcal{A}(G(s)) = 1]| \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot \mathsf{negl}(n)
\end{aligned}$$

which concludes the proof.

Exercise No.4 (Hash-functions) *(5+2+3 points)*
Let h be a collision-resistant hash-function.

(a) Consider

$$h_s^0(x) := \begin{cases} h_s(x)||1 & \text{if } x_1 = 0 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$

$$h_s^1(x) := \begin{cases} h_s(x)||1 & \text{if } x_1 = 1 \\ 0^{|h_s(x)|+1} & \text{otherwise} \end{cases}$$

$$\hat{h}_s(x) := h_s^0(x)||h_s^1(x)$$

Prove that $\hat{h}$ is collision-resistant.

(b) Now let

$$\begin{aligned}
h_s^a(x) &:= h_s(x)_1 \dots h_s(x)_{\lceil \frac{|h_s(x)|}{2} \rceil} \\
h_s^b(x) &:= h_s(x)_{\lceil \frac{|h_s(x)|}{2} \rceil + 1} \dots h_s(x)_{|h_s(x)|}
\end{aligned}$$

Prove or disprove: At least one of h^a and h^b is collision resistant.

(c) What if $h^a = h^b$? Prove your answer.

Solution No.4 (Hash-functions) For reasons of notation we write $h(x)$ instead of $h_s(x)$.

(a) Assume there are $x \neq y$ such that $\hat{h}(x) = \hat{h}(y)$. We claim that $x_1 = y_1$. Assuming not (WLOG assume $x_1 = 0$, $y_1 = 1$) we would have

$$\hat{h}(x) = h(x)||1||0^{|h(x)|+1} \neq 0^{|h(y)|+1}||h(y)||1\,.$$

Now we assume without loss of generality that $x_1 = y_1 = 0$ (the case of $x_1 = y_1 = 1$ is completely similar). Then we have $\hat{h}(x) = \hat{h}(y)$ implies that $h(x) = h(y)$. Therefore every collision of $\hat{h}$ is also a collision of h implying $\hat{h}$ is collision-resistant.

(b) This is not true as we can instantiate h with $\hat{h}$ from part (a). It holds that neither h^0 nor h^1 are collision-resistant because they map every input x with $x_1 = 0$, $x_1 = 1$ respectively, to the same output.

(c) In this case $h^a = h^b$ has to be collision-resistant. Assuming $x \neq y$ is a collision for h^a. Then

$$h(x) = h^a(x)||h^b(x) = h^a(x)||h^a(x) = h^a(y)||h^a(y) = h^a(y)||h^b(y) = h(y)$$

that is, every collision of h^a is also a collision of h.

Exercise No.5 (From public to private key) *(7 points)*
Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme. Construct a *private*-key encryption scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- $\mathsf{Gen}'(1^n) := \mathsf{Gen}(1^n)$, that is, the single private key k of Π' is the pair (sk, pk) output by Gen.
- $\mathsf{Enc}'_{(pk,sk)}(m) := (\mathsf{Enc}_{pk}(m), \mathsf{Enc}_{pk}(m))$, that is, encryption of a message m produces a ciphertext (c_1, c_2), where for c_1 and c_2, encryption is performed independently as in Π, using only the part of k corresponding to pk.
- $\mathsf{Dec}'_{(pk,sk)}(c_1, c_2)$ is defined as follows: Let $m_0 := \mathsf{Dec}_{sk}(c_1), m_1 := \mathsf{Dec}_{sk}(c_2)$. Then, $\mathsf{Dec}'_{(pk,sk)}(c_1, c_2)$ is defined as $\perp$ if $m_0 \neq m_1$ (i.e., decryption failed), and as m_0 otherwise. That is, decryption is performed on both parts of the ciphertext as in Π, using only the second part sk of k. If both parts yield the same message, the algorithm outputs this message, and otherwise outputs an error.

Show that Π' is *not* CCA-secure.

Solution No.5 (From public to private key) Construct an adversary $\mathcal{A}$ as follows: Output two messages $m_0 \neq m_1$ for the experimenter. Upon receiving the challenge ciphertext (c_1, c_2), query the decryption oracle to decrypt (c_2, c_1), receiving a message m'. Then, output b' with $m' = m_{b'}$. Only with negligible probability will it happen that $c_1 = c_2$ (otherwise Π wouldn't be CPA-secure), and hence, in all but negligibly many cases, $(c_1, c_2) \neq (c_2, c_1)$ and querying (c_2, c_1) is thus valid for the experiment. It is clear that, with all but negligible probability, m' is the same as m_b, where b is the bit chosen in the experiment.

Exercise No.6 (An attack on plain RSA signatures) *(10 points)*
Consider the plain RSA signature scheme, where messages m are signed with the signature $\sigma := [m^d \bmod N]$, and verification of (m, σ) if performed by checking whether $m = [\sigma^e \bmod N]$ for public key (N, e) and private key (N, d).

Let $x \in \mathbb{Z}_N$ be some message, $r \in \mathbb{Z}_N$ be arbitrary, and let $s = r^e \bmod N$. Furthermore, let σ be a valid signature for the message $x \cdot s \bmod N$. Show that $\frac{\sigma}{r} \bmod N$ is a valid signature for x. Does this imply that a ppt attacker can forge a signature for *any* message using only a single signing query?

Solution No.6 (An attack on plain RSA signatures) We compute $\left(\frac{\sigma}{r}\right)^e = \frac{\sigma^e}{r^e} = \frac{x \cdot s}{r^e} = \frac{x r^e}{r^e} = x \bmod N$, because of the choice of s and σ. This proves that this is a valid signature for x. All the steps can be performed in polynomial time and there is only one signing query involved for $x \cdot s$, which is $\neq x$ in all but negligibly many cases. So indeed, an attacker can forge any message with only a single query to the signing oracle.