Cryptography, winter term 16/17: Sample Exam

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

February 10th, 2017

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.

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.

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.

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

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

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.

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.

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?