Technische Universität München (I7) **Winter 2013/14**
Dr. M. Luttenberger / M. Schlund

Cryptography – Endterm

Exercise 1 One Liners **1.5P each = 12P**

For each of the following statements, state if it is true or false **and** give a *short* (one line) justification of your answer (e.g. sketch the argument or give a counter-example).

Example: "If the RSA problem is hard w.r.t. $\mathsf{Gen}\mathbb{P}^2$, then PRGs with variable strecth exist" is true because then the RSA problem yields a OWP family to which we can apply the Blum-Micali construction.

(a) If pseudorandom functions (PRF) exist, then CCA-secure ES exist.

(b) If pseudorandom functions (PRF) exist, then pseudorandom generators (PRG) exist.

(c) If DLP is hard w.r.t. $\mathsf{Gen}\mathbb{Z}^*_{\text{safe}}$, then ElGamal using $\mathsf{Gen}\mathbb{Z}^*_{\text{safe}}$ is CPA-secure.

(d) If the RSA problem is hard, then computing the Carmichael function $\lambda(N)$ for $N = pq$ (p, q prime) is hard.

(e) If the DLP is hard w.r.t. $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$, then collision resistant hash functions exist.

(f) If $P \neq NP$, then computationally secret ES cannot exist.

(g) If F_k is a PRF, the cascading construction $F^*_k(x)$ together with the CBC-padding $F^*_k(\mathsf{pad}_{\text{CBC}}(m))$ yields a secure MAC.

(h) If F_k is a PRP and G is a PRG, then $\mathsf{Enc}_k(m) := F_k(m \oplus G(k+1))$ yields a CPA-secure ES.

Exercise 2 **2P+3P = 5P**

(a) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Show that $G' : \{0,1\}^n \to \{0,1\}^{2n}$ with $G'(x) := \overline{G(x)}$ is also a PRG ($\overline{\cdot}$ is the bitwise negation).

(b) Prove or disprove: Let $G_1, G_2 : \{0,1\}^n \to \{0,1\}^{2n}$ be PRGs with $G_1 \neq G_2$. Then $G : \{0,1\}^n \to \{0,1\}^{4n}$ defined as $G(x) := G_1(x)||G_2(x)$ is a PRG.

Exercise 3 **3P**

Consider the following message authentication code built from a PRF F of key and block length n:

- Gen: On input 1^n, output $k \overset{u}{\in} \{0,1\}^n$.
- Mac: Let $\mathcal{M}_n := \{m \in \{0,1\}^* \mid n \mid |m| \wedge |m| < 2^n\}$.

  On input $k \in \{0,1\}^n$ and $m \in \mathcal{M}_n$, partition m into subsequent n-bit blocks $m = m^{(1)}||\ldots||m^{(l)}$.

  Then output $t := F_k(m^{(1)} \oplus \lfloor 1 \rceil) \oplus F_k(m^{(2)} \oplus \lfloor 2 \rceil) \oplus \cdots \oplus F_k(m^{(l)} \oplus \lfloor l \rceil)$ for some encoding $\lfloor \cdot \rceil \{0, 1, \ldots, 2^n - 1\} \to \{0,1\}^n$.
- Vrf: On input $k \in \{0,1\}^n$, $m \in \mathcal{M}_n$, and $t \in \{0,1\}^n$, output 1 if $\mathsf{Mac}_k(m) = t$, otherwise ouput 0.

Show that this MAC is not secure ("existentially unforgeable under an adaptive chosen-message attack"). E.g. show how to forge a valid tag for the message $0^n||0^n$.

Exercise 4 **2P+2P+2P+1P = 7P**

Consider the multiplicative group $\mathbb{Z}^*_p$ modulo the prime $p = 53$.

(a) Is 2 a generator of $\mathbb{Z}^*_p$?

(b) Compute the probability that $x \overset{u}{\in} \mathbb{Z}^*_p$ is a generator of $\mathbb{Z}^*_p$.

(c) Let $f_k : \mathbb{Z}^*_p \to \mathbb{Z}^*_p : x \mapsto (x^k \bmod p)$.

For which $e \in \mathbb{Z}$ exists a $d \in \mathbb{Z}$ such that for all $x \in \mathbb{Z}^*_p$ we have $f_d(f_e(x)) = x$?

(d) Why is RSA not hard w.r.t. $\mathsf{Gen}\mathbb{Z}^*_{\text{prime}}$?

Exercise 5 **1P+2P+3P = 6P**

Consider the multiplicative group $\mathbb{Z}_n^*$ modulo $n = 13 \cdot 17 = 221$.

(a) Compute the order of $\mathbb{Z}_n^*$.

(b) Compute the exponent of $\mathbb{Z}_n^*$.

(c) Use the CRT to compute a generator of a largest cyclic subgroup of Z_n^*.

Exercise 6 **1P+2P+2P+2P = 7P**

Given a pseudorandom permutation (PRP) F with key-length n and block-length $2n$, consider the fixed-length ES $\mathcal{E}$ (partially) defined by

- Gen: On input 1^n return $k \overset{u}{\in} \{0,1\}^n$.
- Enc: On input $k, m \in \{0,1\}^n$, choose $\rho \overset{u}{\in} \{0,1\}^n$ and return $\mathsf{Enc}_k(m) := F_k(\rho||m)$.

(a) Complete the definition of $\mathcal{E}$ by defining Dec.

(b) Above ES $\mathcal{E}$, given a key of length n, can only encrypt messages of length n.

Under the assumption that $\mathcal{E}$ is CPA-secure, describe how to build from above ES $\mathcal{E}$ an ES $\mathcal{E}'$ which (1) can handle messages of arbitrary length (this rules out some padding schemes!), and (2) is also CPA-secure.

(c) Assume further that $\mathcal{E}$ is even CCA-secure. Is then $\mathcal{E}'$ (your answer to (b)) also CCA-secure? Prove your answer!

(d) Show that $\mathcal{E}$ is CPA-secure if F is a PRP. To this end, analyze the success probability of the following PPT-distinguisher $\mathcal{D}$ for F where $\mathcal{A}$ is any PPT-CPA-attack on $\mathcal{E}$.

Definition of $\mathcal{D}^{\mathcal{O}}(1^n)$:

- Let $\mathsf{Enc}^{\mathrm{sim}}$ by the following function:

  On input $m \in \{0,1\}^n$ choose $\rho \overset{u}{\in} \{0,1\}^n$, then output $\mathsf{Enc}^{\mathrm{sim}}(m) := \mathcal{O}(\rho||m)$.
- $m_0, m_1 \overset{r}{:=} \mathcal{A}(1^n)^{\mathsf{Enc}^{\mathrm{sim}}}$.
- Choose $b \overset{u}{\in} \{0,1\}$.
- $c \overset{r}{:=} \mathsf{Enc}^{\mathrm{sim}}(m_b)$.
- $r \overset{r}{:=} \mathcal{A}^{\mathsf{Enc}^{\mathrm{sim}}}(c)$.
- If $r = b$ output 1 ("$\mathcal{O}$ contains F"); else output 0 ("$\mathcal{O}$ contains RPO").

Remarks: Recall $\mathcal{D}$ has access to an oracle $\mathcal{O}$ where $\mathcal{O}$ is either $\mathcal{O}_0$ ("perfect world") or $\mathcal{O}_1$ ("real world"): $\mathcal{O}_0$ is a random permutation oracle (RPO), i.e. on creation it chooses uniformly at random permutation from the set of all permutations of $\{0,1\}^{2n}$ which it uses to answer all queries; $\mathcal{O}_1$ chooses $k \overset{u}{\in} \{0,1\}^n$ on creation and answers all queries using F_k.

Abbreviations

- RO = random oracle
- RPO = random permutation oracle
- OWF = one-way function (family/collection)
- OWP = one-way permutation (family/collection)
- TDP = trapdoor one-way permutation
- PRG = pseudorandom generator
- PRF = pseudorandom function
- PRP = pseudorandom permutation
- TBC = tweakable block cipher
- ES = (PPT) private-key encryption scheme
- PKES = (PPT) public-key encryption scheme
- UOWHF = universal one-way hash function (family/collection)
- CRHF = collision resistant hash function (family/collection)
- MAC = (PPT) message authentication code
- DSS = (PPT) digital signature scheme
- DLP = discrete logarithm problem
- CDH = computational Diffie-Hellman problem
- DDH = decisional Diffie-Hellman problem
- $\oplus$ = bitwise XOR
- OFB = output feedback
- CBC = cipher block chaining