Cryptography – Endterm

Exercise 1 **"One-liners"** **1P each = 8P**

Give a short (one line) answer/explanation using the results from the lecture and the exercises.

(a) Our notions of CPA and CCA security are based on the idea of *indistinguishable* encryptions. State the name of another notion of security used for ES.

(b) What is a safe prime?

(c) Name a polynomial-time algorithm for testing primality.

(d) Why is the RSA-problem not a OWF over $\langle \mathbb{Z}_p^*, \cdot, 1 \rangle$ with p prime?

(e) How many generators does $\langle \mathbb{Z}_{113}^*, \cdot, 1 \rangle$ possess? **Remark**: 113 is prime.

(f) How many primes are asymptotically in the interval $[0, 2^n]$?

(g) Give an example of a family of groups w.r.t. which the DDH is conjectured to be hard.

(h) What is OAEP used for?

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

(a) State which of the following cryptographic primitives resp. schemes **are known to exist (as discussed in the lecture)** under the assumption that CPA-secure PKES exist:

$$\text{PRG, CCA-secure PKES, secure MAC, perfectly secret ES, CRHF, secure DSS, UOWHF}$$

(b) For which of the above primitives resp. schemes is their existence known to be equivalent to the existence of OWF?

(c) State a conjecture which is known to suffice for CCA-secure PKES to exist.

Exercise 3 **3P+2P+1P+1P=7P**

Let F be a PRF of key length n and block length $l(n)$.

(a) Define Gen, and Enc for F-rCTR (randomized counter mode) ES.

(b) Show that F-rCTR ES is not CCA-secure.

(c) What is a possible advantage of F-rCTR when compared to F-rCBC (randomized cipher block chaining)?

(d) The CPA-security bound derived for F-rCTR in the lecture depends not only on the probability that an adversary can distinguish F from a RO but also on the block length of F. Why?

Exercise 4 **3P+2P+3P=8P**

Let $(h_n)_{n\in\mathbb{N}}$ be a collection of compression functions with $h_n \colon \{0,1\}^{2n} \to \{0,1\}^n$ for $n \in \mathbb{N}$.

(a) Describe how the Merkle-Damgård construction is used to construct from h_n a collection of hash functions $H_{n,\mathrm{IV}}$.

What is the domain of $H_{n,\mathrm{IV}}$?

Name one cryptographic property that $H_{n,\mathrm{IV}}$ inherits from h_n.

Let F be a PRF of key and block length n. We can extend the domain of F by applying the Merkle-Damgård construction to $h_n(x||y) := F_x(y)$ (for $x, y \in \{0,1\}^n$). Denote by $\overline{F}_{\mathrm{IV}} := H_{n,\mathrm{IV}}$ the resulting function for $\mathrm{IV} \in \{0,1\}^n$.

(b) Show that $\overline{F}_{\mathrm{IV}}$ is not a PRF for $\mathrm{IV} \overset{u}{\in} \{0,1\}^n$ the secret key.

(c) Define $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrf})$ for F-NMAC. Feel free to use $\overline{F}$.

Exercise 5 **3P+1P+1P+2P+2P=9P**

The multiplicative group modulo N is denoted by $\mathbb{Z}_N^* \hat{=} \langle \mathbb{Z}_N^*, \cdot, 1\rangle$. Let

$$f_{(N,e)} \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^* \colon x \mapsto x^e \bmod N$$

be the map defined by taking $x \in \mathbb{Z}_N^*$ to its e-th power modulo N.

Hint: $385 = 5 \cdot 7 \cdot 11$.

(a) What is the order and the exponent of the group $\langle \mathbb{Z}_{385}^*, \cdot, 1\rangle$? Is this group cyclic?

(b) State the precise characterization of those $e \in \mathbb{Z}$ for which $f_{(N,e)}$ is a permutation on $\mathbb{Z}_N^*$.

(c) How many distinct permutations of this form $f_{(N,e)}$ are there? Prove your answer.

(d) Compute a $d \in \mathbb{N}$ such that $f_{(385,d)}$ is the inverse permutation of $f_{(385,7)}$.

(e) Assume you are given public and private RSA-TDP parameters (N, e) and (N, d), respectively. Further, let $h \colon \{0,1\}^* \to \{0,1\}^{160}$ be a concrete hash function, e.g. RIPEMD-160.

Describe how to sign a message, and how to verify a message-signature pair using the RSA-TDP and h based on the *full-domain-hash* heuristic. Assume that $N \in [2^{1023}, 2^{1024}]$.

Exercise 6 **3P**

Let F be a PRF of key and block length n, and $\lfloor\rceil \colon \{1, 2, \ldots, 2^n\} \to \{0,1\}^n$ some encoding function.

Assume we derive from a truly random secret key $k \overset{u}{\in} \{0,1\}^n$, a sequence of pseudorandom keys $k_1, \ldots, k_{r(n)}$ with $k_i := F_k(\lfloor i \rceil)$ and $r(n)$ some fixed polynomial.

Prove that every PPT-algorithm $\mathcal{P}$ which on input $k_1, \ldots, k_{r(n)-1}$ tries to compute $k_{r(n)}$ can only succeed with negligible probability. To this end, define a distinguisher $\mathcal{D}$ for F which uses $\mathcal{P}$ as subprocedure.

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
- UOWHF = universal one-way hash function (family/collection)
- CRHF = collision resistant hash function (family/collection)
- ES = (private-key) encryption scheme
- PKES = public-key encryption scheme
- MAC = message authentication code
- DSS = digital signature scheme
- DLP = discrete logarithm problem
- DDH = decisional Diffie-Hellman problem