Cryptography – Questionnaire 1

Name: ______________________________

Matr.: ______________________________

"One-liners"

Exercise 1.1 — 2P

Let k be a positive integer and let $K_1 := \{0, 1, 2, 3\}^k$ and $K_2 := \{A \mid A \subseteq \{1, \ldots, k\}, |A| = 5\}$. Give closed-form expressions for $|K_1|$ and $|K_2|$.

Answer: ______________________________

Exercise 1.2 — 2P

Often, encryption schemes (ES) are based on block ciphers which can only process inputs of a fixed size l (called the block length). If we want to process messages $m \in \{0, 1\}^*$ of arbitrary length, we need to pad the message to a multiple of l in a suitable way. Briefly describe one possible way to do so. (We want to be able to recover m in the end!)

Answer: ______________________________

Exercise 1.3 — 2P

Briefly state the meaning of the *sufficient keyspace principle*:

Answer: ______________________________

Exercise 1.4 — 2P

Name a major disadvantage of publice-key schemes compared to private-key schemes.

Answer: ______________________________

Exercise 1.5 — 2P

Name one ES from the lecture that satisfies $\mathsf{Enc}_k = \mathsf{Dec}_k$ for a given key k.

Answer: ______________________________

Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2018/12/11

Cryptography – Questionnaire 2

Name: ______________________________

Matr.: ______________________________

"One/Two-liners" – 5P

Exercise 2.1 — 2P

How many *injective* functions $f : \{0,1\}^n \to \{0,1\}^{2n}$ are there? Give a closed-form expression!

Answer: ______________________________

Exercise 2.2 — 1P

State the name of a computationally secret fixed-length ES such that every PPT-algorithm $\mathcal{A}$, which, on input 1^n and ciphertext c, tries to compute the parity of the original message m, succeeds with probability exactly $1/2$. (The parity of a message $x_1||\ldots||x_n \in \{0,1\}^n$ is just the xor of all bits $\bigoplus_i x_i$)

Answer: ______________________________

Exercise 2.3 — 2P

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a DPT-computable function such that f is a permutation on $\{0,1\}^n$ for all n.

Show that $G : \{0,1\}^n \to \{0,1\}^{2n}$ with $G(x) = f(x)||x \oplus f(x)$ is never a PRG of stretch $l(n) = 2n$. To this end, briefly describe a PPT distinguisher, and (roughly) estimate its success probability.

Questions—1P each = 5P

	true	false
$f\colon \mathbb{N} \to \mathbb{R}$ is negligible with $f(n) := \begin{cases} \frac{1}{2^n} & \text{if } n \text{ is even,} \\ \frac{1}{\log_2(n)} & \text{otherwise.} \end{cases}$	☐	☐
Let $f\colon \mathbb{N} \to \mathbb{N}$ and $g\colon \mathbb{N} \to \mathbb{N}$. If $(f \circ g)$ is negligible, then f and g are both negligible.	☐	☐
If $\varepsilon : \mathbb{N} \to \mathbb{R}^+$ is negligible, then $f : \mathbb{N} \to \mathbb{R}^+$ with $f(n) := \varepsilon(\lceil \log n \rceil)$ is also negligible.	☐	☐
Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a computationally secret fixed-length PPT-ES. Every PPT-algorithm $\mathcal{A}$, which, on input 1^n and ciphertext c, tries to compute the parity of the original message m, succeeds with probability exactly $1/2$.	☐	☐
There exists a PRG G with strech $l(n) > n$ such that $\Pr\left[\mathsf{Win}_{n,G}^{\text{IndPRG}}(\mathcal{D})\right] = \frac{1}{2}$ for every probabilistic exponential time distinguisher $\mathcal{D}$ and all $n \in \mathbb{N}$.	☐	☐

Technische Universität München (I7) **Winter term 2017/2018**
Dr. M. Luttenberger / S. Jaax **2018/12/11**

Cryptography – Questionnaire 3

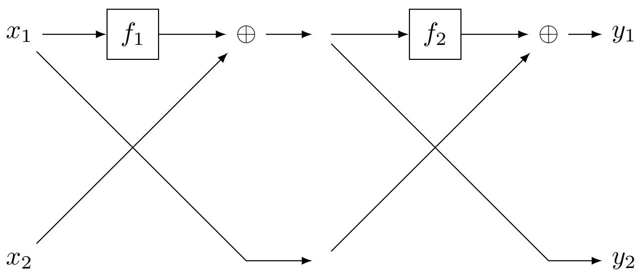
Name: ______________________________

Matr.: ______________________________

"One-liners"

Exercise 3.1 **Feistel-Networks** **1P+1P+1P = 3P**

Consider the two-round Feistel-Network drawn below, with $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$.



(a) Compute the outputs y_1, y_2 of the network for $x_1 = 0^n$ and $x_2 = 0^n$
Answer:______________________________

(b) Compute the outputs y_1, y_2 of the network for $x_1 = 0^n$ and $x_2 = f_1(0^n)$
Answer:______________________________

(c) Does the two-round Feistel-Network realize a PRP if used with two PRFs f_{k_1}, f_{k_2}? Why/why not?
Answer:______________________________

Exercise 3.2 **PRG from PRF** **2P**

Let F be a PRF with $l_{\text{in}}(n) = l_{\text{out}}(n) = n$. Construct from F a PRG G of stretch $2n$.

Answer: $G(k) :=$ ______________________________

Questions– 1P each = 5P

	true	false
Let F be a PRP, F-rCBC is computationally secret.	☐	☐
Let G be a PRG of stretch $s \cdot n$, then $F_k : \{0,1\}^{sn} \to \{0,1\}^{sn}$ defined by $F_k(x) = G(k) \oplus x$ is a PRF.	☐	☐
Let F be a PRF of block length $l(n) = n$. We define $\widetilde{F}$ for every $n \in \mathbb{N}$, $k \in \{0,1\}^n$ and $x_1 \dots x_{2n} \in \{0,1\}^{2n}$ by using F in a one-round Feistel-network: $$\widetilde{F}_k(x_1 \dots x_{2n}) = \mathsf{FN}_{F_k}(x_1 \dots x_n, x_{n+1} \dots x_{2n}).$$ $\widetilde{F}$ is a PRP of block length $2n$.	☐	☐
Let RO be a random function oracle of input and output length n. Then $G(k) := \mathsf{RO}(k) \| \mathsf{RO}(k)$ is a PRG of stretch $2n$.	☐	☐
Let F be a PRF. Then F-rCTR is CCA-secure.	☐	☐

Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2019/02/06

Cryptography – Questionnaire 4

Name: ______________________________

Matr.: ______________________________

"One-liners"– 1+2+4 = 7P

Exercise 4.1 **1P**

Let F be a PRP. How do you obtain a PRF from F?
Answer:

Exercise 4.2 **2P**

Let F be a PRP. Sketch graphically the computation of F-NMAC.

Exercise 4.3 **2P+2P**

Let F be a PRF with block length $l(n) = n$. Consider the following two MAC schemes where in both cases $\mathsf{Gen}(1^n)$ outputs $k \overset{u}{\in} \{0,1\}^n$ and $\mathsf{Vrf}_k(t,m)$ outputs 1 iff $\mathsf{Mac}_k(m) = t$. The message space is $(\{0,1\}^n)^+$. We can write every message m as $m = m^{(1)}||\cdots||m^{(|m|/n)}$ with $m^{(i)} \in \{0,1\}^n$ for $1 \le i \le |m|/n$. Show for each of the following two choices of Mac_k how Eve can use her oracle access to Mac_k to forge a tag for the message 0^n0^n in the MAC-experiment:

(a) $\mathsf{Mac}_k(m) := F_k(m^{(1)}) \oplus \cdots \oplus F_k(m^{(|m|/n)})$
Answer:

(b) $\mathsf{Mac}_k(m) := F_k^*(m)$
Answer:

Recall that $F_k^*(m)$ for $m = m^{(1)}||\cdots||m^{(d)}$ is the "cascading-construction" defined by the algorithm:

- Set $k^{(0)} := k$
- For $i = 1$ to d: set $k^{(i)} := F_{k^{(i-1)}}(m^{(i)})$.
- Output $F_k^*(m) := k^{(d)}$

Questions–1P each = 3P

	true	false
Let F be a PRP of block length n. Define an ES $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with $\mathsf{Gen}(1^n)$ choosing a key k uniformly at random from $\{0,1\}^n$ and $\mathsf{Enc}_k(x_1 \dots x_{2n}) = F_k(x_1 \dots x_n) \| F_k(x_{n+1} \dots x_{2n})$. $\mathcal{E}$ is CPA-secure.	☐	☐
Let F be a PRP. Then there is a PPT adversary which can distinguish F from a random-permutation-oracle with non-zero advantage.	☐	☐
Let F be a PRF. F-rCTR Mode, i.e. $\mathsf{Mac}_k(m) := \text{ctr}\|m^{(1)} \oplus F_k(\lfloor \text{ctr} + 1 \rceil) \| \dots \| m^{(t)} \oplus F_k(\lfloor \text{ctr} + t \rceil).)$ yields a secure MAC.	☐	☐

Cryptography – Questionnaire 5

Name: ______________________________

Matr.: ______________________________

Questions – 1P each = 4P

	true	false
$\mathbb{Z}_{35}^{*}$ is cyclic.	☐	☐
There exists a prime p such that $\lambda(2 \cdot p^k) < \varphi(2 \cdot p^k)$ for some $k > 0$.	☐	☐
Every cyclic group is commutative.	☐	☐
Let G be cyclic and $H \leq G$ be a subgroup of G. Then H is cyclic as well.	☐	☐

"One-liners" – 2P each = 6P

Exercise 5.1

- When is a prime p a "safe prime"?
- Let p be a safe prime. Compute $\varphi(p-1)$.

Answer:

Exercise 5.2

Compute 3^{158} in Z_{53}^{*}.
Answer:

Exercise 5.3

How many generators does $\mathbb{Z}_{47}^{*}$ have? (*Hint*: 47 is prime)
Answer:

Cryptography – Questionnaire 6

Name: ______________________________

Matr.: ______________________________

Questions– 1P each= 5P

	true	false
If RSA (i.e. $f(x) = x^e \bmod N$ with modulus $N = pq$) is an OWF then computing a $z < N$ with $\mathsf{gcd}(z, N) > 1$ has to be hard.	☐	☐
Let $f : \mathbb{Z}^*_{77} \to \mathbb{Z}^*_{77}$ with $f(x) = x^{13} \bmod 77$ and $g : \mathbb{Z}^*_{77} \to \mathbb{Z}^*_{77}$ with $g(x) = x^{43} \bmod 77$. Then f and g define the same map.	☐	☐
If OWP with hard-core predicate exist then PRGs of variable stretch exist.	☐	☐
If $\mathcal{P} = \mathcal{NP}$ then there are no CPA-secure ES.	☐	☐
OWF exist if and only if CCA-secure ES exist.	☐	☐

"One-liners"–2P+2P+1P = 5P

Exercise 6.1 **2P**

Compute the *least* positive integer d such that $g(x) := x^d \bmod (5 \cdot 17)$ is the inverse of $f(x) := x^3 \bmod (5 \cdot 17)$.
Answer:

Exercise 6.2 **2P**

Show (i.e. sketch the argument briefly) that $f_n : \{0,1\}^{42} \times \{0,1\}^n \to \{0,1\}^{(n+44)}$ defined as $f(x, y) = (x||0) \cdot (y||1)$ is *not* an OWF (the multiplication $\cdot$ is to be interpreted in $Z^*_{2^{(n+44)}}$).
Answer:

Exercise 6.3 **1P**

How many solutions does the quadratic equation $X^2 \equiv 1 \bmod 51$ have? (*Hint*: $51 = 3 \cdot 17$)
Answer:

Cryptography – Questionnaire 6

Name: ______________________

Matr.: ______________________

Questions

	true	false
OWF exist if and only if CCA-secure ES exist.	☐	☐
RSA "works" for $N = 35$ and $e = 3$, i.e. $x \mapsto x^e \bmod N$ is a permutation (in particular: invertible).	☐	☐
The ElGamal-PKES is CCA-secure.	☐	☐
If DDH is hard w.r.t. $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ then ElGamal based on $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ is CPA-secure.	☐	☐

"(One|two)-liners"

Exercise 6.1 **2P**

Briefly state why the DDH over $\mathbb{Z}_p^*$ (p prime) is *not* hard.
Answer:

Exercise 6.2 **2P**

Suppose Bob's public ElGamal key is $(\mathbb{G}, q, g, h_b) = (\mathbb{Z}_{17}^*, 16, 6, 5)$. Alice wants to send him the message $m = 7$ encrypted using the ElGamal PKES. Compute the ciphertext $c = (c_1, c_2)$ that is sent to Bob assuming Alice has generated $a = 3$ as her secret.
Answer:

Exercise 6.3 **2P**

Briefly state

- why RSA-based PKES use a probabilistic padding scheme and
- name one of these schemes used in practice.

Answer: