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?

(a) Semantic security

(b) p is safe iff $p = 2q+1$ with q, q prime

(c) Miller - Rabin test (or AKS)

(d) Computation of $\lambda(p) = p-1$ is trivial.

(e) $(\mathbb{Z}_{113}^*, \cdot) \cong (\mathbb{Z}_{112}, +) \rightsquigarrow \varphi(112) = \varphi(16 \cdot 7)$
$= 8 \cdot 6 = \underline{\underline{48}}$

(f) $\Theta\left(\frac{2^n}{n}\right)$

(g) Quadratic residues modulo a safe prime

(h) Probabilistic padding scheme for RSA-TDP

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:

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.

(a) if CPA-secure PKES exist, then OWF exist which implies the existence of PRG, secure MACs, secure DSS, UOWHF } → (b)

Further, perfectly secret ES always exist.

(c) That RSA is a TDP suffices.

(It is also known that the hardness of the DDH problem w.r.t. certain groups suffices.)

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?

(a) Gen: on input 1^n, output $k \xleftarrow{R} \{0,1\}^n$

Enc: Given $m \in \{0,1\}^*$

1) pad m to $\tilde{m} = m \| 10^p$ so that $|\tilde{m}|$ is a (minimal) multiple of $l(n)$.

2) Split $\tilde{m}$ in blocks of length $l(n)$:

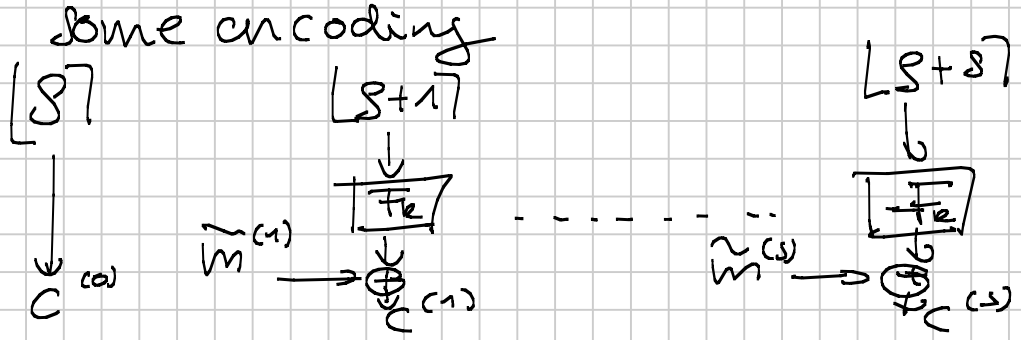
$$\tilde{m} = \tilde{m}^{(1)} \| \dots \| \tilde{m}^{(s)}$$

3) choose $s \xleftarrow{R} \{0, 1, 2, \dots, 2^{l(n)} - 1\}$

4) compute: $c^{(i)} = \tilde{m}^{(i)} \oplus F_k(\langle s + i \bmod 2^{l(n)} \rangle)$

5) output: $c := \langle s \rangle \| c^{(1)} \| \dots \| c^{(s)}$

where $\langle \cdot \rangle : \{0, 1, \dots, 2^{l(n)} - 1\} \to \{0,1\}^{l(n)}$ some encoding



(b) 1. $\mathcal{A}$ challenges A & B for

$m_0 = 0^{\ell(n)}$ and $m_1 = 1^{\ell(n)}$

2. Given $C = C^{(0)} \| C^{(1)} = \langle S \rangle \| m_b \oplus F_k(\langle S+1 \rangle)$

Use the decryption oracle to decrypt

$$C' = C^{(0)} \| \left(C^{(1)} \oplus 1^{\ell(n)} \right) \neq C$$

→ yields : $m_b \oplus 1^{\ell(n)}$

(c) • Encryption in CBC mode requires the encryption of the preceding message block to be known, while in CTR mode all message blocks can be encrypted in parallel.

(d) The probability of a collision, i.e. that F_k is queried on the same value twice, is $\Theta\left(\binom{\ell(n)}{2} 2^{-\ell(n)} \right)$

↝ $\ell(n)$ should be so large that this probability is negligible.

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

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 $\mathrm{IV} \xleftarrow{u} \{0,1\}^n$ the secret key.

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

(a) Given $m \in \{0,1\}^{<2^n}$ and $IV \in \{0,1\}^n$:

1. pad m to $\tilde{m}$ so that $|\tilde{m}|$ is a minimal multiple of n

2. Split $\tilde{m} = \tilde{m}^{(1)} \| \dots \| \tilde{m}^{(s)}$ into blocks of length n

3. Compute: $z_0 := IV$

$$z_i := h_n(z_{i-1} \| \tilde{m}^{(i)})$$

$$z_{s+1} := h_n(z_s \| \underbrace{\lfloor |m| \rceil}_{\text{encoded using } n \text{ bits}})$$

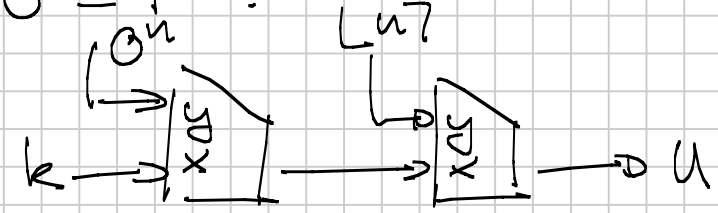
$\rightarrow$ domain: $\{0,1\}^{<2^n}$

If $(h_n)_{n\in\mathbb{N}}$ is collision resistant, so is $(H_{n,IV})$

(b) Distinguisher for $\overline{\overline{F}}$:

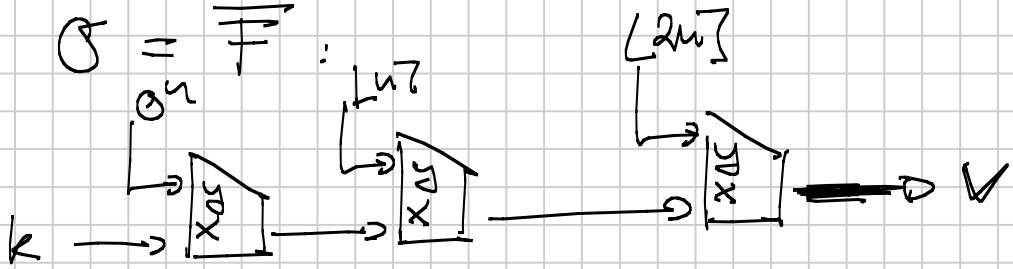
1. Compute $\sigma(0^u) =: U$

if $\sigma = \overline{\overline{F}}$:



2. Compute $\sigma(0^u \| L^u) =: V$

if $\sigma = \overline{\overline{F}}$:



3. Check: $\overline{\overline{F}}_u(L^{2u}) = V$

if $\sigma = F$, always true

if $\sigma = RO$, then $\overline{\overline{F}}_u(L^{2u}) = \sigma(0^u \| L^u)$ with prob. 2^{-u}

→ Distinguisher wins with prob $\underline{\underline{1 - 2^{-u}}}$.

(c) Gen: on input, output $k_0, k_1 \in \{0,1\}^n$

Mac: on input $m \in \{0,1\}^{<2^n}$, $k_1, k_0 \in \{0,1\}^n$

output $F_{k_0}(F_{k_1}(m))$

Vrf: on input, $m \in \{0,1\}^{<2^n}$, $t \in \{0,1\}^n$,
$k_1, k_0 \in \{0,1\}^n$

output 1 iff $Mac_{k_1,k_0}(m) = t$.

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

1P 2P

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

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

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 $h : \{0,1\}^* \to \{0,1\}^{160}$ 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 $N \in [2^{1023}, 2^{1024}]$.

(a) $|\mathbb{Z}_{385}^*| = \varphi(385) = 4 \cdot 6 \cdot 10 = 240$

$\lambda(385) = \operatorname{lcm}(4, 6, 10) = 60$

→ not cyclic

(b) $f_{(N,e)}$ is a permutation on $\mathbb{Z}_N^*$ iff $\gcd(e, \lambda(N)) = 1$

(c) Claim: $|\mathbb{Z}_{\lambda(N)}^*| = \varphi(\lambda(N))$ distinct permutations of the form $f_{(N,e)}$

$\forall x \in \mathbb{Z}_N^* : x^e \equiv x^{\tilde{e}} \ (N)$

iff $\forall x \in \mathbb{Z}_N^* : x^{e-\tilde{e}} \equiv 1 \ (N)$

iff $\lambda(N) \mid e - \tilde{e}$

iff $e \equiv \tilde{e} \ (\lambda(N))$

(d) $1 = \gcd(7, 60)$

$60 = 8 \cdot 7 + 4 \rightarrow 4 = 60 - 8 \cdot 7$

$= \gcd(4, 7)$

$= 2 \cdot 4 - 1 \cdot 7$

$= 2(60 - 8 \cdot 7) - 1 \cdot 7$

$= 2 \cdot 60 - 17 \cdot 7$

$\Rightarrow d \equiv -17 \equiv 43 \pmod{60}$

(e) Let $K(m)$ be the first 1023 (1024) bits of $h(1\|0\|m)\|\ldots\|h(1\|67\|m) \in \{0,1\}^{7 \cdot 160}$

Sign: Given m and (N, d)

this is the secret (large) exponent

compute (e.g.) $(K(m)^d \bmod N) =: \sigma$

Verify: Given m, σ, and (N, e)

public (usually small) exponent

check that $K(m) \stackrel{?}{=} (\sigma^e \bmod N)$.

Exercise 6 **3P**

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

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

Ind. PRF

A & B

$b \xleftarrow{u} \{0,1\}$

If $b=0$:
$\sigma := RO$

If $b=1$:
$\sigma := F_k$ for $k \xleftarrow{u} \{0,1\}^n$

$r := \mathcal{D}^{\sigma}(1^n)$

Win: $r = b$

$\mathcal{D}$ using $\mathcal{P}$

Compute for $i = 1,\ldots,r(n)$

$k_i = \sigma(\lfloor i \rfloor)$

$\tilde{k}_{r(n)} := \mathcal{P}(k_1,\ldots,k_{r(n)-1})$

if $k_{r(n)} = \tilde{k}_{r(n)}$
return 1
else return 0.

If $b=0$: $\mathcal{D}$ wins iff $k_{r(n)} \neq \tilde{k}_{r(n)}$

now $k_{r(n)} = RO(\lfloor u \rfloor)$, so the probability that

$RO(\lfloor u \rfloor) = \mathcal{P}(k_1,\ldots,k_{r(n)-1})$

is 2^{-n}, so $\mathcal{D}$ wins with prob $1-2^{-n}$

If $b=1$: $\mathcal{D}$ wins iff $\mathcal{P}$ succeeds.

$$\varepsilon(n) := \left| \Pr[D \text{ wins } | \text{ ind PRF}] - \frac{1}{2} \right|$$

$$= \left| \frac{1}{2} \cdot (1 - 2^{-n}) + \frac{1}{2} \Pr[P \text{ succeeds}] - \frac{1}{2} \right|$$

$$= \frac{1}{2} \left| \Pr[P \text{ succeeds}] - 2^{-n} \right|$$

$$\Rightarrow \quad \Pr[P \text{ succeeds}] \leq 2\varepsilon(n) + 2^{-n}$$