Technische Universität München (I7)
Dr. M. Luttenberger / M. Schlund **Winter 2014/15**

SOLUTION

Cryptography – Endterm

Exercise 1 **1.5P each = 9P**

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 stretch exist" is true because then the RSA problem yields a OWP family to which we can apply the Blum-Micali construction.

(a) Let $g\colon \mathbb{N} \to \mathbb{N}$ with $g(n) < g(2n)$. Then $n^{-g(n)}$ is negligible.

(b) If Elgamal's DSS (with hashing) is secure, then the DLP is hard w.r.t. the multiplicative groups modulo primes.

(c) The multiplicative group modulo 135 is cyclic.

(d) If the RSA problem is hard w.r.t. $\mathsf{Gen}\mathbb{P}^2$, then CPA-secure PKES exist.

(e) If CCA-secure ES exist, then secure DSS exist.

(f) If computing the Carmichael function $\lambda(N)$ for $N = pq$ (p, q prime, unknown) is hard,

then computing the Euler φ-function $\varphi(N)$ is also hard.

Solution:

(a) False: consider the function $g\colon \mathbb{N} \to \mathbb{N}$ with $g(2^k d) = k$ for $k \in \mathbb{N}$ and d odd. Obviously, $g(2^k d) < g(2^{k+1} d)$. Then for any $N \in \mathbb{N}_0$ and any $c > 0$ there exist infinitely many odd $d > N$ such that $d^{-g(d)} = d^0 = 1 > d^{-c}$.

(b) True: Elgamal-DSS hides the secret $x \in \mathbb{Z}_{p-1}$ in the group via $y = g^x \bmod p$.

(c) False: As discussed in the lecture, $\mathbb{Z}_N^*$ is cyclic if and only if $N \in \{2, 4, p^k, 2p^k\}$ for p prime, $k \in \mathbb{N}$.

(d) True: See the slides; Use the RSA-TDP as KEM and the Blum-Micali construction (as prOTP) as DEM.

(e) True: OWFs suffice to construct secure DSS. And OWFs exist iff CCA-secure ES exist.

(f) True: If we know $\varphi(N)$, we can easily also compute p and q, and thus also $\lambda(N)$; simply solve the quadratic equation $\varphi(N) = (p-1)(\frac{N}{p} - 1)$ for p (see the exercises).

Exercise 2 **8P**

Let F be a PRP of block and key length n. Recall the basic CBC mode:

- Given: $k \in \{0,1\}^n$, $\mathrm{IV} \in \{0,1\}^n$, $x = x^{(1)}||\ldots||x^{(s)}$ for $x^{(i)} \in \{0,1\}^n$.
- Compute: $y^{(0)} := \mathrm{IV}$; for $i = 1$ to $i = s$: $y^{(i)} = F_k(y^{(i-1)} \oplus x^{(i)})$.
- Output: $\mathsf{CBC}^F(\mathrm{IV}, k, x) := y = y^{(0)}||y^{(1)}||\ldots||y^{(s)}$.

Give a **self-contained** description of how $\mathsf{CBC}^F(\mathrm{IV}, k, x)$ can be used to obtain a CCA-secure ES.

(This includes encryption, decryption, padding, key generation, and so on.)

Solution: EtM using rCBC plus some variant of CBC-MAC.

Let $\mathsf{pad}_{10}(m) = m||10\dots0$ with the minimal number of 0s so that the resulting message is a multiple of n.

Let $\mathsf{pad}_{CBC}(m) = \lfloor|m|\rceil||m||0\dots0$ with the minimal number of 0s so that the resulting message is a multiple of n.

- $\mathsf{Gen}(1^n) := k_e||k_i||k_o \overset{u}{\in} \{0,1\}^n$. ($k_o$ can be removed if CBC-MAC is used.)

  Alternatively: $k \overset{u}{\in} \{0,1\}^n$, then e.g. $k_e := F_k(0^n)$, $k_i := F_k(0^{n-1}1)$, and $k_o := F_k(10^{n-1})$.

- $\mathsf{Enc}_{k_e||k_i||k_o}(m)$:

  IV $\overset{u}{\in} \{0,1\}^n$;

  $c := \mathsf{CBC}^F(\text{IV}, k_e, \mathsf{pad}_{10}(m))$;

  $y := y^{(0)}||y^{(1)}||\dots||y^{(s)} = \mathsf{CBC}^F(0^n, k_i, c)$;

  $t := F_{k_o}(y^{(s)})$. (Destroy y.)

  return $c||t$. ($t||y$ is just as fine.)

  - Here, the MAC is based on the CBC-construction plus outer encryption. So we do not need any prefix-free padding as in CBC-MAC. As the ciphertext is already a multiple of the block length, we thus need no padding at all for the MAC.
  - BUT: If you want to use CBC-MAC, then you need to apply the prefix-free padding to the ciphertext (the input to the MAC!).

    (It might be the case that we can get rid of pad_{CBC} for the MAC if pad_{CBC} is already used in the ES, but we haven't shown/seen anything like this in the lecture.)
  - Further note that the IV used for the MAC has to be fixed (here IV $= 0^n$).

- $\mathsf{Dec}_{k_e||k_i||k_o}(c||t)$:

  $y := y^{(0)}||y^{(1)}||\dots||y^{(s)} = \mathsf{CBC}^F(0^n, k_i, c)$;

  $t' := F_{k_o}(y^{(s)})$

  if $t' \neq t$: return "blub";

  Let $c = c^{(0)}||c^{(1)}||\dots||c^{(l)}$;

  for $i = 1$ to $i = l$: $x^{(i)} := c^{(i-1)} \oplus F_{k_e}^{-1}(c^{(i)})$;

  Let m be the unique prefix of $x = x^{(1)}||\dots||x^{(l)}$ such that $x = m||10\dots0$;

  return m;

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

Let $n \in \mathbb{N}$, and $1 \leq r < n$. Let $G\colon \{0,1\}^* \to \{0,1\}^{n-r}$, and $H\colon \{0,1\}^* \to \{0,1\}^r$ be two DPT-computable functions.

The OAEP is then defined a follows:

- Input: $m \in \{0,1\}^{n-r}$.
- Choose $\rho \overset{u}{\in} \{0,1\}^r$.
- return $m \oplus G(\rho)||\rho \oplus H(m \oplus G(\rho))$.

(a) Briefly describe where and why the OAEP is used in cryptography.

(b) Describe how m can be recovered given $m \oplus G(\rho)||\rho \oplus H(m \oplus G(\rho))$.

(c) The OAEP uses a construction already used in DES. State the name of this construction.

Solution:

(a) Basic RSA problem yields a deterministic, stateless PKES. OAEP is used to randomize the input to the RSA problem and obtain a randomized PKES. Mostly used as it can be proven to be CCA-secure in the ROM.

(b)
- Input $x = m \oplus G(\rho)$, $y = \rho \oplus H(m \oplus G(\rho))$
- Recover $\rho = y \oplus H(x)$.
- Recover $m = x \oplus G(\rho)$.

(c) Main computation is a two-round Feistel network.

Exercise 4 **3P+3P=6P**

Let $p = 229$ and $q = 233$ (both prime). Set $N = p \cdot q = 53357$.

(a) Let $k := \min\{\alpha \in \mathbb{N} \mid \mathsf{gcd}(2^\alpha + 1, \lambda(N)) = 1\}$. Set $e := 2^k + 1$.

Compute $d \in \mathbb{Z}^*_{\lambda(N)}$ such that $ed \equiv_{\lambda(N)} 1$.

(b) Compute $29301^{235} \pmod N$ **using the Chinese remainder theorem**.

Remark: All crucial computation steps have to be explicitly stated. It does not suffice to simply give the final result.

Solution:

(a) $\lambda(N) = \mathsf{lcm}(p-1, q-1) = \mathsf{lcm}(228, 232) = \mathsf{lcm}(2^2 \cdot 3 \cdot 19, 2^3 \cdot 29) = 2^3 \cdot 3 \cdot 19 \cdot 29 = 13224$.

So, $e = 5 = 2^2 + 1$.

Computing d does not really require Euclid here as obviously $\lambda + 1$ is a multiple of $e = 5$. So, $d = 2645 = \frac{1+\lambda}{e}$.

(b) CRT isomorphism: $h(x) := (x \pmod p, x \pmod q))$

For the inverse isomorphism $h^{-1}(x_p, x_q) := (x_p \cdot q\beta + x_q \cdot p\alpha) \bmod N$, use Euclid to compute $\alpha = 58, \beta = -57$ s.t. $1 = \alpha \cdot p + \beta \cdot q$. (In fact, this is not need in this case as $h^{-1}(x, x) = x$.)

Then:

$$\begin{aligned}
29301^{235} &= h^{-1}(h(29301^{235})) = h^{-1}(29301^{235} \bmod p, 29301^{235} \bmod q) \\
&= h^{-1}(29301^{235 \bmod p-1} \bmod p, 29301^{235 \bmod q-1} \bmod q) \\
&= h^{-1}(218^7 \bmod p, 176^3 \bmod q) \\
&= h^{-1}((-11)^7 \bmod p, 42) \\
&= h^{-1}(-121^3 \cdot 11 \bmod p, 42) \\
&= h^{-1}(42, 42) \\
&= 42
\end{aligned}$$

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

Let $\mathbb{QR}_{191}$ denote the quadratic residues modulo the prime 191 (as a subgroup of the multiplicative group $\mathbb{Z}^*_{191}$ modulo 191).

(a) What is the probability that a uniformly at random chosen element $a \overset{u}{\in} \mathbb{QR}_{191}$ is a generator of $\mathbb{QR}_{191}$?

(b) Show that 4 is a generator of $\mathbb{QR}_{191}$.

(c) Decide whether $5 \in \mathbb{QR}_{191}$ holds. (*Hint*: $5^7 \equiv_{191} 6$, $6^3 \equiv_{191} 5^2$.)

Solution:

(a) $|\mathbb{QR}_{191}| = \frac{|\mathbb{Z}^*_{191}|}{2} = \frac{\varphi(191)}{2} = \frac{191-1}{2} = 95$. (If p is a prime, then $\mathbb{QR}_p$ has exactly half the size of $\mathbb{Z}^*_p$.)

As $\mathbb{Z}^*_{191}$ is cyclic, so is $\mathbb{QR}_{191}$. Thus, $\mathbb{QR}_{191}$ is ismorphic to the additive group modulo $95 = |\mathbb{QR}_{191}|$ which has $\varphi(95) = 4 \cdot 18 = 72$ generators. So the probability is $\frac{72}{95}$.

(b) Generator test: 4 is a generator of $\mathbb{QR}_{191}$ if and only if $4^{|\mathbb{QR}_{191}|/p} \not\equiv_{191} 1$ for every prime p which divides $95 = |\mathbb{QR}_{191}|$:

$4^5 \equiv_{191} 256 \cdot 4 \equiv_{191} 65 \cdot 4 \equiv_{191} 69$, $4^{19} \equiv_{191} (69)^3 \cdot 4^3 \equiv_{191} 49$

So, 4 is a generator of $\mathbb{QR}_{191}$.

(c) Compute the Legendre symbol $5^{\frac{p-1}{2}} \bmod 191$. 5 is a quadratic residue if and only if the Legendre symbol evaluates to 1.

Using the hint, one can show that 5 has order 19: $(5^7)^3 \equiv_{191} 6^3 \equiv_{191} 5^2$

So: $5^{95} \equiv_{191} 5^{19 \cdot 5} \equiv_{191} 1$.

Alternative solutions:

(1) $5 \equiv_{191} 5 + 191 = 196 = (14)^2$.

(2) As $191 \equiv_4 3$, so **if** $5 \in \mathbb{QR}_{191}$, then $5^{\frac{p+1}{4}} \bmod 191$ should be a square root of 5 modulo 191, i.e. $5^{\frac{p+1}{2}} \equiv_{191} 5$ should hold.

Note that you do not know whether 5 is a quadratic residue, so simply computing $5^{\frac{p+1}{4}} \bmod 191$ does not prove anything.

Exercise 6 **3P+3P = 6P**

Let G be a PRG of stretch $l(n) = 2n$. Further, let F be a PRF of block length n and key length $2n$.

We build from G and F a keyed function H which has key and block length n:

For every $n \in \mathbb{N}$**, for all** $x, k \in \{0,1\}^n$ **let** $H_k(x) := F_{G(k)}(x)$**.**

We define the following oracles:

$\mathcal{O}_H$	$\mathcal{O}_F$	$\mathcal{O}_R$ (random function oracle)
on init:	**on init:**	**on init:**
$k \overset{u}{\in} \{0,1\}^n$	$k \overset{u}{\in} \{0,1\}^{2n}$	T : empty map
on query x**:**	**on query** x**:**	**on query** x**:**
return $H_k(x)$	return $F_k(x)$	if $T[x]$ is undefined : $T[x] := y \overset{u}{\in} \{0,1\}^n$ **return** $T[x]$

(a) Let $\mathcal{D}$ be any PPT-distinguisher for the following "F-or-H"-experiment:

- Choose $b \overset{u}{\in} \{0,1\}$.
- If $b = 0$, set $\mathcal{O} := \mathcal{O}_F$; else set $\mathcal{O} := \mathcal{O}_H$.
- $r \overset{r}{:=} \mathcal{D}^{\mathcal{O}}(1^n)$

▷ $\mathcal{D}$ wins if $r = b$

Show that any such $\mathcal{D}$ can only succeed with negligible advantage (over simply guessing).

Hint: Let $\mathcal{D}$ be a distinguisher for the "F-or-H"-experiment. Construct from it the distinguisher $\mathcal{D}_G$ for the PRG G:

- Get input $y \in \{0,1\}^{2n}$.
- Compute $r \overset{r}{:=} \mathcal{D}(1^n)$ by answering any oracle query x by $F_y(x)$.
- return r

(b) Show that H is a PRF of key and block length n (under above assumptions on F and G), i.e. show that

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H}(1^n) = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_R}(1^n) = 1\right]\right|$$

is negligible for any PPT-distinguisher $\mathcal{D}$.

Solution:

(a) In the PRG experiment, $\mathcal{D}$ is either given $y \overset{u}{\in} \{0,1\}^{2n}$ (if $b' = 0$) or $G(k)$ for $k \overset{u}{\in} \{0,1\}^n$ (if $b' = 1$).

Consider the case $b' = 0$:

In this case, all queries of $\mathcal{D}_{H,F}$ are answered via $F_y(x)$ with $y \overset{u}{\in} \{0,1\}^{2n}$, i.e. $\mathcal{D}_{1,2}$ interacts with $\mathcal{O}_F$.

So: $\mathcal{D}$ wins in the case $b' = 0$ of the PRG game iff $\mathcal{D}_{H,F}^{\mathcal{O}_F}$ outputs $r = 0$ iff $\mathcal{D}_{H,F}$ wins in the case $b = 0$ in the experiment X.

Analogously for $b' = 1$:

Now, $\mathcal{D}_{H,F}$ gets all queries answered by $F_y(x)$ for $y = G(k)$ with $k \overset{u}{\in} \{0,1\}^n$, i.e. $\mathcal{D}_{H,F}$ interacts with $\mathcal{O}_H$.

So: $\mathcal{D}$ wins in the case $b' = 1$ of the PRG game iff $\mathcal{D}_{H,F}^{\mathcal{O}_H}$ outputs $r = 1$ iff $\mathcal{D}_{H,F}$ wins in the case $b = 1$ in the experiment X.

In total, $\mathcal{D}$ wins in the PRG game exactly with the same probability as $\mathcal{D}_{H,F}$ wins in X.

Hence, the advantage of $\mathcal{D}_{H,F}$ in X can only be negligibly better than $1/2$.

(b) Let $\mathcal{D}$ be a distinguisher for H in the PRF game. We have to show that the advantage

$$\frac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_R} = 1\right]\right|$$

is negligible. From (a) we know that

$$\frac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_F} = 1\right]\right|$$

is negligible.

As F is a PRF, also

$$\frac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_F}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_R}=1\right]\right|$$

is negligble. Hence, as the sum of two negligible functions is negeligible, also

$$\begin{aligned}\tfrac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_R}=1\right]\right| &= \tfrac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_F}=1\right]+\Pr\left[\mathcal{D}^{\mathcal{O}_F}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_R}=1\right]\right|\\ &\leq \tfrac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_F}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_R}=1\right]\right|+\tfrac{1}{2}\left|\Pr\left[\mathcal{D}^{\mathcal{O}_H}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_F}=1\right]\right|\end{aligned}$$

is also negligible.

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
- ES = (PPT) private-key encryption scheme
- PKES = (PPT) public-key encryption scheme
- $\oplus$ = bitwise XOR
- 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
- CBC = cipher block chaining
- PPT = probabilistic polynomial time
- DPT = deterministic polynomial time