Final exam *Introduction to Cryptography VU* (Total: 40 points) 26 January 2024

1) (1 point per correct, −1 per incorrect answer; minimum 0 points) Are the following statements true or false?

a) An unbounded adversary can break a perfectly secret encryption scheme.

b) $f(n) = n^{-\frac{1}{n}}$ is negligible.

c) DES has longer keys than AES.

d) The block-cipher modes of operation ECB, CBC, and CTR are all CPA-secure.

e) The block-cipher modes of operation CBC and CTR are CCA-secure.

f) A deterministic MAC cannot be secure[1].

g) Using a MAC of the sent message, one can prevent replay attacks.

h) A hash function takes an arbitrary-length input and produces a fixed-length output.

i) The integers with multiplication $(\mathbb{Z}, \cdot)$ form a group.

j) For every $N, e \in \mathbb{N}$ with $\gcd(e, \phi(N)) = 1$, we have that $x \mapsto [x^e \bmod N]$ is a permutation on $\mathbb{Z}_N^*$.

k) The discrete logarithm problem is hard in $(\mathbb{Z}_p, +)$, where p is prime.

l) To achieve the same security, NIST recommends longer key lengths for private-key encryption schemes than public-key encryption schemes.

2) (2+4+3+2 points) Private-key encryption:

a) A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CCA-secure if for every p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\varepsilon(\cdot)$ such that $\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1] \leq 1/2 + \varepsilon(n)$, with $\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ defined as follows:

1. A key $k \leftarrow \mathsf{Gen}(1^n)$ is generated. $\mathcal{A}$ is given 1^n and oracle access to $\mathsf{Enc}_k(\cdot)$ and $\mathsf{Dec}_k(\cdot)$.
2. $\mathcal{A}$ outputs a pair of messages m_0, m_1 with $|m_0| = |m_1|$.
3. A bit $b \leftarrow \{0,1\}$ is sampled and the challenge ciphertext $c^* := \mathsf{Enc}_k(m_b)$ is given to $\mathcal{A}$.
4. $\mathcal{A}$ continues to have access to $\mathsf{Enc}_k(\cdot)$ and $\mathsf{Dec}_k(\cdot)$, but is not allowed to query the latter on c^*.
5. $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$. The output of the experiment is 1 iff $b' = b$.

Which modifications to the definition of CCA-security are necessary to obtain CPA-security?

b) Define the one-time pad encryption by specifying the key space, the message space, and all 3 algorithms.

c) Is the one-time pad encryption scheme CPA-secure? Justify your answer.

d) Name one advantage and one disadvantage of private-key encryption compared to public-key encryption.

3) (3 points) MACs and hash functions:

Let $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF) and $H\colon \{0,1\}^* \to \{0,1\}^n$ a hash function. Show that if H is not collision-resistant, then the following MAC scheme for messages from $\{0,1\}^*$ is not secure[1]:

$\mathsf{Gen}(1^n)$: Return $k \leftarrow \{0,1\}^n$. $\mathsf{Mac}_k(m)$: Return $t := F_k(H(m))$. $\mathsf{Vrfy}_k(m,t)$: Return 1 iff $F_k(H(m)) = t$.

4) (2+4 points) Number theory and RSA:

a) Compute $[2^{63} \bmod 11]$.

b) Let (N_1, e_1) and (N_2, e_2) be two RSA public keys, where N_1 and N_2 were generated so they share one of their prime factors. Show how to efficiently obtain the corresponding secret keys.

5) (3+5 points) Public-key encryption:

a) Consider Elgamal encryption using a standardized group $(\mathbb{G}, q, g)$:

$\mathsf{Gen}(1^n)$: Sample $x \leftarrow \mathbb{Z}_q$ and return $pk := g^x$, $sk := x$.
$\mathsf{Enc}_{pk}(m)$: Sample $r \leftarrow \mathbb{Z}_q$ and return $(c_1, c_2) := (g^r, pk^r \cdot m)$.

Show how to decrypt and argue correctness.

b) Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be as in a) and let $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be a CCA-secure private-key encryption scheme with key space $\mathbb{G}$. Show that the following hybrid encryption scheme is not CCA-secure:

$\overline{\mathsf{Gen}}(1^n)$: Return $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$.
$\overline{\mathsf{Enc}}_{pk}(m)$: Sample $k \leftarrow \mathbb{G}$ and return $(c_1, c_2) := \big(\mathsf{Enc}_{pk}(k), \mathsf{Enc}'_k(m)\big)$.
$\overline{\mathsf{Dec}}_{sk}(c_1, c_2)$: Compute $k := \mathsf{Dec}_{sk}(c_1)$ and return $m := \mathsf{Dec}'_k(c_2)$.

[1] in the sense of *existential unforgeability under adaptive chosen-message attacks*