Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2017/18
TEACHER: Christian Schaffner, TA: Jan Czajkowski, Christian Majenz

Problem Set 12

We will work on the following exercises together during the work session on Friday, 20 October 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: Plain RSA Signatures

Say the public key is $\langle N, e\rangle = \langle 91, 11\rangle$.

(a) Verify that $(43, 36)$ is a valid message-signature pair.

(b) Compute $\phi(N)$.

(c) Calculate the private key d.

(d) Sign the message $m = 28$.

Problem 2: Insecurity of plain RSA Signatures

In Section 12.4.1 we showed an attack on the plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a *single* signing query.

Hint: Use the no-query and the two-query attacks.

Problem 3: Plain RSA Signatures, weaker definition

Assume the RSA problem is hard. Show that the plain RSA signature scheme satisfies the following weak definition of security: an attacker is given the public key $\langle N, e\rangle$ and a uniform message $m \in \mathbb{Z}_N^*$. The adversary succeeds if it can output a valid signature on m without making any signing queries.

Problem 4: One-time-secure signature scheme?

A signature scheme is one-time-secure if no PPT adversary making a *single* query can output a valid forgery.

Let f be a one-way permutation (it is hard to calculate the inverse of f). Consider the following signature scheme for messages in the set $\{1, \ldots, n\}$:

- To generate keys, choose uniform $x \in \{0,1\}^n$ and set $y := f^{(n)}(x)$ (where $f^{(i)}(.)$ refers to i-fold iteration of f, and $f^{(0)}(x) = x$). The public key is y and the private key is x.
- To sign message $i \in \{1, \ldots, n\}$, output $f^{(n-i)}(x)$.
- To verify signature σ on message i with respect to public key y, check whether $y = f^{(i)}(\sigma)$.

(a) Show that the verification procedure will output 1 for every legal message-signature pair.

(b) Show that the above is not a one-time-secure signature scheme. Given a signature on a message i, for what messages j can an adversary output a forgery?

(c) Prove that no PPT adversary given a signature on i can output a forgery on any message $j > i$ except with negligible probability.

★ Problem 5: Another one-time secure signature scheme

Let f be a permutation and $f^{(i)}(x)$ the i-fold iteration of f, and $f^{(0)}(x) := x$. Let us consider the following signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ for messages $m \in \{1, \ldots, p\}$ with $p = p(n)$ polynomial in n.

$$
\begin{array}{rcl}
\mathsf{Gen}(1^n) & : & \text{Choose } \mathsf{sk}_1, \mathsf{sk}_2 \in_R \{0,1\}^n,\ \mathsf{pk}_1 := f^p(\mathsf{sk}_1) \text{ and } \mathsf{pk}_2 := f^p(\mathsf{sk}_2). \\
 & & \text{Set } \mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2) \text{ and } \mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2). \\
\mathsf{Sign}_{\mathsf{sk}}(m) & : & \text{Compute } \sigma_1 := f^{(p-m)}(\mathsf{sk}_1) \text{ and } \sigma_2 := f^{(m-1)}(\mathsf{sk}_2). \\
 & & \text{Return } \sigma := (\sigma_1, \sigma_2). \\
\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma) & : & \text{If } \mathsf{pk}_1 = f^{(m)}(\sigma_1) \text{ and } \mathsf{pk}_2 = f^{(p-m+1)}(\sigma_2) \text{ return } 1, \text{ else return } 0.
\end{array}
$$

(a) Show that Π is correct.

(b) Prove that Π is a one-time-secure signature scheme, if f is a one-way permutation.

★ Problem 6: Hash-based signatures

Read Section 12.6 in [KL] to learn about hash-based signatures, one of the prime candidates for a signature scheme which remains secure against quantum attackers.