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 sessions 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: 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: What is the signature of $m = \tilde{m}^e$ for some $\tilde{m}$?

Problem 2: One-time secure signature scheme?

Let f be a one-way permutation. Consider the following signature scheme for messages in the set $\{1, \cdot, n\}$:

- 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 $i \in \{1, \dots, n\}$, output $f^{(ni)}(x)$.
- To verify signature σ on message i with respect to public key y, check whether $y = f^{(i)}(\sigma)$.

1. 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?
2. Prove that no ppt adversary given a signature on i can output a forgery on any message $j > i$ except with negligible probability.
3. Suggest how to modify the scheme so as to obtain a one-time-secure signature scheme.

   Hint: Include two values y, y' in the public key.

Problem 3: 3

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 $m \in \{1, \dots, p\}$ with $p = p(n)$ polynomial in n.

$\mathsf{Gen}(1^n)$: Choose $\mathsf{sk}_1, \mathsf{sk}_2 \in_R \{0,1\}^n$, $\mathsf{pk}_1 := f^p(\mathsf{sk}_1)$ and $\mathsf{pk}_2 := f^p(\mathsf{sk}_2)$.
Set $\mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2)$ and $\mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2)$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Compute $\sigma_1 := f^{p-m}(\mathsf{sk}_1)$ and $\sigma_2 := f^{m-1}(\mathsf{sk}_2)$. Return $\sigma := (\sigma_1, \sigma_2)$

$\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma)$: If $\mathsf{pk}_1 = f^m(\sigma_1)$ and $\mathsf{pk}_2 = f^{p-m+1}(\sigma_2)$ return 1, else return 0.

1. Show that Π is correct.
2. Prove that Π is a one-time-secure signature scheme, if f is a one-way permutation.