LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Advanced Cryptography

Final Exam

July 20$^{\text{th}}$, 2007

Duration: 3 hours 45 minutes

This document consists of 9 pages.

Instructions

Electronic devices are *not* allowed.

Answers must be written on the exercises sheet.

This exam contains 2 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 RSA with a counter

In this exercise, we consider the plain RSA protocol, i.e.

Setup Let $N = pq$ and $\varphi(N) = (p-1)(q-1)$ where p, q are two random $\frac{\ell}{2}$-bit primes.
Pick a random e such that $\mathsf{gcd}(e, \varphi(N)) = 1$ and let $d = e^{-1} \bmod \varphi(N)$
The public key is $K_p = (e, N)$ and the private key is $K_s = (d, N)$.

Encryption On input message $m \in \{0, \ldots, N-1\}$, the ciphertext is $c = m^e \bmod N$.

Decryption On input ciphertext c, the message is recovered computing $m = c^d \bmod N$.

We assume a protocol in which every messages are RSA-encrypted with exponent $e = 3$. To protect the sequentiality of protocol messages, messages are concatenated with a 32-bit counter before encryption. Hence, if Alice wants to send a i^{th} message equal to m to Bob, she sends $(\mathsf{format}(m) \cdot 2^{32} + i)^e \bmod N_B$ where N_B is Bob's RSA modulus and $\mathsf{format}(m)$ is a formatted string consisting of m concatenated with an integrity check $H(m)$. Uppon reception, Bob decrypts, checks that the index number i is as expected, checks the redundancy in the formatted string, and finally extracts m. Messages from Bob to Alice use another counter and Alice's RSA modulus N_A.

1. Which security property is protected by this protocol? Which security property is not? (Confidentiality? Authentication? Integrity?) Explain why.

2. After Alice sends some $a = x^e \bmod N_B$ to Bob, an adversary impersonates the response "could you repeat please" from Bob to Alice. Alice repeats the same message by sending some $b = y^e \bmod N_B$.

   (a) What is the relation between x and y?

   (b) In the ring $\mathbb{Z}_{N_B}[z]$ of polynomials with unknown z and coefficients in $\mathbb{Z}_{N_B}$, show that $z - x$ is a factor of $z^3 - a$ and $(z+1)^3 - b$.

   (c) Deduce that $z - x$ is the gcd of $z^3 - a$ and $(z+1)^3 - b$ in this ring.

(d) From the previous question, apply the Euclid algorithm to find a rational expression for x in terms of a and b.

3. Can this extend to $e = 65537$?

2 RSA Forgeries

We consider the plain RSA signature scheme, i.e.

Setup. Let $N = pq$ and $\varphi(N) = (p-1)(q-1)$ where p, q are two random $\frac{\ell}{2}$-bit primes.
Pick a random e such that $\mathsf{gcd}(e, \varphi(N)) = 1$ and let $d = e^{-1} \bmod \varphi(N)$
The public key is $K_p = (e, N)$ and the private key is $K_s = (d, N)$.

Signature. On input message $m \in \{0, \ldots, N-1\}$, the sign algorithm $\mathsf{sign}_{K_s}(m)$ outputs $\sigma = m^d \bmod N$.

Verification. On input message-signature pair (m, σ), the verify algorithm $\mathsf{verify}_{K_p}(m, \sigma)$ outputs 1 when $m = \sigma^e \bmod N$ and 0 otherwise.

1. Recall what is an *existential* forgery.

2. Without any sample of valid message-signature pair, explain how you can build *existential* forgeries.

3. Recall what is an *universal* forgery.

4. In a chosen adversarial model, the adversary can query a sign oracle. On input m, the sign oracle outputs a signature σ such that $\mathsf{verify}(m, \sigma) = 1$.

   You can query the sign oracle once, explain how you can build *universal* forgeries.

5. The above attack is done in the chosen message adversarial (CMA) model. Is this forgery still possible in the known message adversarial (KMA) model? Explain your answer.

The plain RSA signature is defined only on input messages belonging $\{0, \ldots, N-1\}$. In order to sign longer messages, such as a file, we introduce a hash function. Let $F : \{0,1\}^* \to \{0,1\}^\ell$ be the hash function used as preprocessing where $\ell = \lfloor \log_2(n) \rfloor$. The new signature scheme works as follows:

Setup. No change.

Signature. On input $m \in \{0,1\}^*$, the new sign algorithm $\mathsf{sign}^*_{K_s}(m)$ outputs $\sigma^* = \mathsf{sign}_{K_s}(F(m))$.

6. Express the signature σ^* of m in terms of F,m,n and d.
   Describe the new verify algorithm $\mathsf{verify}^*(m, \sigma^*)$.

Consider that $m = m_1 \| m_2 \| \ldots \| m_t$ where the m_i are ℓ-bit blocks. We define the hash function F by

$$
\begin{aligned}
F: \quad & m & \mapsto \quad & f = F(m) \\
& m_1 \| m_2 \| \ldots \| m_t & \to \quad & f = m_1 \cdot m_2 \cdot \ldots \cdot m_t \bmod n
\end{aligned}
$$

7. Is this preprocessing solving the existential forgery of question 2? If no, describe the new attack.

8. Is this preprocessing solving the unviersal forgery of question 4? If no, describe the new attack.

9. Which assumption(s) on F is (are) necessary to obtain a secure signature scheme?