LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: . . . .

First Name: . . . .

Section: . . . .

Security and Cryptography

Final Exam

January 12$^{\text{th}}$, 2009

Duration: 4 hours

This document consists of 16 pages.

Instructions

Electronic comunication devices and documents are *not* allowed.

Other electronic devices are permitted.

Answers must be written on the exercises sheet.

This exam contains 4 *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 Impact of Moore's Law on Massive Bruteforce Projects

We assume that the number of elementary operations per second of an up to date computer sold at time t is $f_0 e^{\frac{t}{\tau}}$ and that its price is a constant c. A spook agency is hiring some new cryptographer to run a massive bruteforce cryptanalysis project. The project starts at time $t = 0$ and is bound to complete at time $t = t_c$. The agency wants to run an exhaustive key search. We assume that a computer needs r elementary operations to try a single key.

The project consists of making all bought computers participate in the exhaustive search. Let M denote the total budget to be spent. Let K be the total number of keys which can be tried during the entire project.

Let $b(t)$ be the number of machines running at time t. We assume that machines can all run until time t_c whenever they start running, so $b(t)$ is increasing and depends on the *strategy* to buy new machines. We will compare the following strategies:

- The "startup funds strategy" consists of using the budget right away. In terms of b this translate into a constant function $b(t) = \alpha$.
- The "sleeping strategy" consists of waiting without spending until time $t = t_1$ then buying all machines. In terms of b this translate into a locally constant function $b(t) = 0$ if $t < t_1$ and $b(t) = \alpha$ if $t \geq t_1$.
- The "continous budget strategy" consists of regularly buying computers. In terms of b this translate into a linear function $b(t) = \lambda t$. (For this strategy we model $b(t)$ by a continuous function.)

For numerical applications we will take the following constants

$$\begin{array}{rrr} \tau = \frac{18}{\ln 2}\mathsf{months} & f_0 = 3\mathsf{GHz} & c = 5\,000\mathsf{CHF} \\ t_c = 30\mathsf{years} & r = 200 & M = 10\,000\,000\,000\mathsf{CHF} \end{array} \qquad (1)$$

1. If we buy a computer at time t and make it run until time t_c, express how many keys K it will be able to try in terms of f_0, τ, t_c, r.

2. For the startup funds strategy, express the optimal parameter α in terms of M and c. Express K in terms of f_0, τ, t_c, r, M. Using (1), do the numerical analysis.

3. For the sleeping strategy, express the optimal parameter α in terms of M and c. Express K in terms of $f_0, \tau, t_c, r, M, t_1$. Find the optimal t_1. Using (1), do the numerical analysis.

4. Assuming that $b(t)$ is now a derivable function such that $b(0) = 0$, show that

$$K = \frac{f_0}{r} \int_0^{t_c} \frac{t - (t_c - \tau)}{\tau} e^{\frac{t}{\tau}} b(t)\, dt \tag{2}$$

5. For the continous budget strategy, express the optimal parameter λ in terms of M and c. Express K in terms of f_0, τ, t_c, r, M. Using (1), do the numerical analysis.

6. Deduce from (2) that $b(t)$ becomes optimal as it tends towards the function b_{opt} defined by $b_{\mathsf{opt}}(t) = 0$ for all $t < t_c - \tau$ and $b(t)_{\mathsf{opt}} = \alpha$ for $t > t_c - \tau$. Further deduce that the sleeping strategy is the best one.

2 Homomorphic Signatures

The purpose of this exercise is to study the security of a digital signature scheme. The scheme is defined as follows:

- **Setup:** Two prime numbers p, q such that $p = 1 \mod q$ and an element $g \in \mathbb{Z}_p^\star$ of order q,
- **Key Generation:** The secret key is a tuple $sk = (x, y)$ and the corresponding public key is $pk = (pk_1, pk_2) = (H(x), H(y))$ where $H(\alpha) = g^\alpha \mod p$.
- **Signature:** Given a message $m \in \mathbb{Z}_q$. The signer computes

$$\sigma = x + m \times y \mod q$$

p, q, g, pk are made public while $sk = (x, y)$ is kept secret by the signer.

1. What is the problem preventing us from inverting H? Is H a trapdoor function?

2. Give a typical size of q in bits.

3. Give an algorithm to find g.

4. Give an algorithm to generate p and q. What is its complexity (heuristically)?

5. How does the signature verification work?

6. Show that if an adversary has access to the signatures of two different messages then he is able to retrieve the secret key.

3 MAC From Hash Functions

In this exercise, we will study the security of some MAC constructions based on hash functions. Through this exercise, we will consider a hash function H based on an iterated hash function H_0 with ℓ-bit block messages and the Merkle-Damgård strenghtening pad. That is, $m \| \mathsf{pad}(m)$ has a length multiple of ℓ and $H(m) = H_0(m \| \mathsf{pad}(m))$. (See fig.1.)

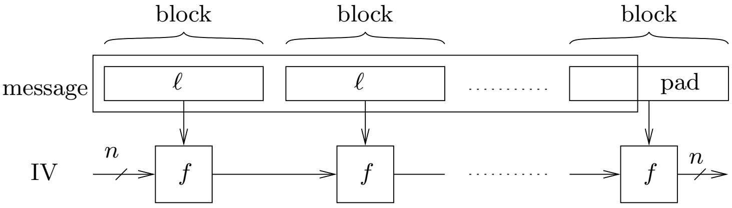

Figure 1: The Merkle-Damgård scheme

1. Recall the standard padding scheme $\mathsf{pad}(m)$ (or an equivalent one).

2. Recall three different security properties of a cryptographic hash function.

3. What is a MAC forgery? Detail the various security models with respect to the Oracles to which the adversary has access.

4. **The Prefix Method**. We consider the MAC algorithm defined given a ℓ-bit secret key K and a message m as

$$\mathsf{MAC}_K(m) = H_0(K\|m\|\mathsf{pad}(m))$$

where $\|$ denotes the concatenation operation.

Show that given the MAC of a known message m the adversary is able to output a forgery on a message $m' \neq m$.

5. **The Suffix Method**. Let us consider another variant defined given a secret key K and a message m as

$$\mathsf{MAC}_K(m) = H_0(m \| \mathsf{pad}(m) \| K)$$

Show that if H is *not* collision-resistant and the adversary has access to an Oracle to which he can submit a *chosen* message m and get $\mathsf{MAC}_K(m)$ then he is able to forge the MAC of a message $m' \neq m$.

4 Broadcast Encryption and Traitor Tracing

This exercise will be graded separately, like the continuous evaluation surveys.

1. The problem of broadcast encryption schemes is that...

□ it uses symmetric encryption only.
□ it is vulnerable to exhaustive search.
□ the content decryption key has to be sent to a precise list of non-revoked receivers.
□ it is not implemented so far.

2. What is the disadvantage of common stateful broadcast encryption schemes?

□ Receiver cannot be revoked.
□ Sender and receiver must be synchronized.
□ They are patented.
□ Content provider cannot monitor receivers.

3. Which one of the following schemes is *not* a broadcast encryptions scheme?

□ SSD (Goodrich, Sun and Tamassia).
□ LSD (Halevi and Shamir).
□ SAS (Pasini and Vaudenay).
□ SD (Naor, Naor and Lotspiech).

4. Tick the *false* statement about the Advanced Access Content System (AACS).

□ BlueRay disks use AACS.
□ AACS is based on the Naor-Naor-Lotspiech scheme.
□ HD-DVDs use AACS.
□ AACS is a stateful broadcast encryption scheme.

5. The purpose of traitor tracing schemes is...

□ to discourage subscribers from giving away their keys.
□ to detect pirate decoders.
□ to send a video signal to a large number of subscribers.
□ to make pirate decoders decrypt a wrong signal.

6. Tick the *correct* statement. A k-collusion resistant traitor tracing scheme...

   □ makes sure that no subset of k subscribers receive the same key.
   □ can identify a coalition of $k-1$ subscribers who released a decryption key.
   □ is such that no subset of k subscribers can decrypt the broadcast signal.
   □ always remains secure if we have $k+1$ traitors.

7. Which of these technologies was not broken so far?

   □ TEA in XBOX. □ Keeloq for cars.
   □ CRYPTO1 in Mifare RFID tag. □ ECDSA in MRTD.

8. Tick the item *unrelated* to SPA in cryptography.

   □ Attacks based on power consumption analysis.
   □ Medication based on water treatment.
   □ Secure password authentication.
   □ Simple power analysis.

9. Tick which item was *not* used for a side-channel attack so far.

   □ Time. □ Color. □ Power. □ Faults.

10. If my quiz has 7 correct and 3 incorrect answers my grade is...

   □ 5 □ 4.5 □ 3.5 □ 3

**Any attempt to look at
the content of these pages
before the signal
will be severly punished.**

Please be patient.