ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: ______________________

First Name: ______________________

Section: ______________________

Cryptography and Security Course (Cryptography Part)

Final Exam

February 23rd, 2007

This document consists of 11 pages.

Instructions

Books and lecture notes are *not allowed.*

Electronic devices are *not allowed.*

Answers must be written on the exercises sheet.

Answers can be written either in French or in English.

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

Part 1: Collision within the Merkle-Damgård Construction

Let N and n be two positive integers such that $N \gg n$. Let $H : \{0,1\}^N \rightarrow \{0,1\}^n$ be a uniformly distributed random function.

1. Compute the probability that two *distinct* fixed inputs produce a collision on the function H, i.e., compute $\Pr_H[H(x) = H(x')]$, where x and x' are two given elements of $\{0,1\}^N$ such that $x \neq x'$.

We now consider that the function H is based on a variant of the Merkle-Damgård construction (see Figure 1). The message is decomposed in blocks of ℓ bits. For the sake of simplicity, we assume that the message has a size which is a multiple of blocks. The number of blocks is denoted by d and we have $N = d \cdot \ell$. In this variant, the compression functions $h_1, \ldots, h_{d+1} : \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^n$ are *independent random* functions. To hash a message $x \in \{0,1\}^N$, the message is first padded and we obtain $x \| \text{pad} \in \{0,1\}^{N+\ell}$ where pad is a bitstring of size ℓ which only depends on the length of x, i.e., we can write pad $= cst(N)$ as a constant, once N is fixed. We set $x_{d+1} :=$ pad.

Then, $x \| \text{pad}$ is processed as shown on Figure 1, where the output of the last compression function h_{d+1} is the hash of the message.

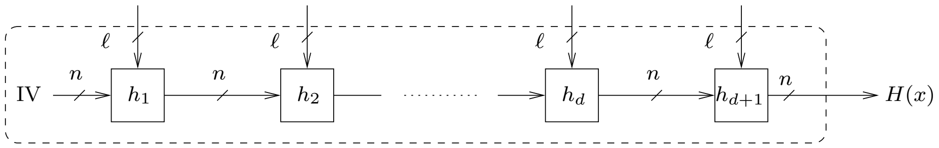

Figure 1: The function H based on a variant of the Merkle-Damgård construction

We consider the case where $d = 1$ and consider two distinct fixed one-block messages $x = x_1$ and $x' = x'_1$ of the *same length* ℓ.

2. Compute $\Pr[h_1(\mathrm{IV}, x_1) = h_1(\mathrm{IV}, x'_1)]$.

3. In the case where $h_1(\mathrm{IV}, x_1) \neq h_1(\mathrm{IV}, x'_1)$, compute the probability that $H(x) = H(x')$, i.e., compute

$$\Pr[H(x) = H(x') \mid h_1(\mathrm{IV}, x_1) \neq h_1(\mathrm{IV}, x'_1)].$$

4. Deduce from the two previous question the value of

$$\Pr[H(x) = H(x')]$$

when H follows the variant of the Merkle-Damgård construction.

We now consider the general case where $d \geq 1$ and consider two fixed messages (of the same length) $x = x_1 \| \cdots \| x_d$ and $x' = x'_1 \| \cdots \| x'_d$ such that $x_1 \neq x'_1$ and $x_i = x'_i$ for all $i > 1$.

5. Using the previous question, show that

$$\Pr[H(x) = H(x')] = 2^{-n} \sum_{i=0}^{d} (1 - 2^{-n})^i$$

for all $d \geq 1$. Compute the limit of this sum when $d \to \infty$. What kind of cryptographic conclusion about Merkle-Damgård construction can you deduce from this?
Hint: Note that "pad" can be seen as another block x_{d+1} such that $x_{d+1} = x'_{d+1}$. Using induction for this proof may be useful!

6. Here, we consider two fixed messages (of the same length) $x = x_1 \| \cdots \| x_d$ and $x' = x'_1 \| \cdots \| x'_d$ such that $x_1 \neq x'_1$, $x_2 \neq x'_2$, and $x_i = x'_i$ for all $i > 2$. Compute

$$\Pr[H(x) = H(x')]$$

for any $d \geq 2$.

7. Finally, let us consider the very general case with two distinct fixed messages $x = x_1 \| \cdots \| x_d$ and $x' = x'_1 \| \cdots \| x'_d$. Find a general formula for

$$\Pr[H(x) = H(x')]$$

depending on some characterization of x and x'.
Hint: Look at the largest j such that $x_j \neq x'_j$.

Part 2: RSA Variants with CRT Decryption

We first recall classical RSA with the decryption variant based on the Chinese Remainder Theorem. Let p and q be two primes of same size and $n = pq$. We then select the public exponent e such that $\gcd(e, (p-1)(q-1)) = 1$.

8. Explain how the decryption exponent d is computed.

In this CRT decryption variant, the primes p and q are known to the decrypter and the main computational task consists of some operations in $\mathbf{Z}_p$ and in $\mathbf{Z}_q$.

9. Explain carefully how we decrypt a given ciphertext $c \in \mathbf{Z}_n$ using this decryption variant.

Multi-Prime RSA

From now on, we consider an RSA variant with a modulus of the form $n = pqr$, where p, q, and r are prime integers of same size. Let s be the size in bits of n. We also assume that if a plaintext is taken randomly in $x \in_U \mathbf{Z}_n$, then this one should lie in $\mathbf{Z}_n^*$.

10. Justify the last assumption when s is large enough by computing the probability that an element $x \in_U \mathbf{Z}_n$ picked uniformly at random also lies in $\mathbf{Z}_n^*$.

We want to encrypt as in the classical RSA variant using an integer e as exponent.

11. What condition on e is necessary and sufficient for the encryption to be invertible? How do we compute the decryption exponent?

Again, we want to decrypt using the Chinese Remainder Theorem. So, from a ciphertext $c \in \mathbf{Z}_n^*$, we first compute $c_p = c \bmod p$, $c_q = c \bmod q$, $c_r = c \bmod r$.

12. Assume here that you know how to invert the CRT transform, i.e., you are able to invert $\Psi : x \mapsto (x \bmod p, x \bmod q, x \bmod r)$. Explain carefully how the corresponding plaintext m is retrieved with this CRT decryption variant.

13. Exhibit a formula for inverting Ψ.
Hint: First you need to find three elements e_p, e_q, and e_r such that $\Psi(e_p) = (1, 0, 0)$, $\Psi(e_q) = (0, 1, 0)$, and $\Psi(e_q) = (0, 0, 1)$. Then, everything works like in linear algebra!

14. Analyze the asymptotic complexity of the decryption with the two moduli variants $n = pq$ and $n = pqr$ when both moduli are of size s. Compare both complexities and express the gain of one variant over the other with a multiplicative factor.

Multi-Power RSA

Here, we focus on another RSA variant with a modulus of the form $n = p^2q$, where p and q have the same size.

15. Explain how RSA with a modulus of this type works. More precisely, describe the key generation, the encryption, and the decryption.
Remark: For the moment, we do not consider a CRT variant for the decryption!

Note that a classical CRT variant of the decryption would require to retrieve the plaintext modulo p^2 and modulo q. However, this is not the fastest way to retrieve the plaintext. We look at another algorithm in what follows.

16. Let e be a positive integer and y be an integer such that $1 \leq y \leq p^2 - 1$. Assume we know an integer $1 \leq x_1 \leq p - 1$ such that $x_1^e \equiv y \pmod{p}$. Find a method to compute an integer x such that $x^e \equiv y \pmod{p^2}$.
Hint: First set $y_1 := x_1^e \bmod p$ and write $x = x_1 + k \cdot p$ for an integer k. Then, write $y = y_1 + \ell \cdot p$ for an integer ℓ and solve an equation to retrieve k.

17. Explain now how you decrypt efficiently using the Chinese Remainder Theorem.

18. Compare the asymptotic complexity of the decryption with CRT of the classical RSA variant and the above decryption method for RSA with a modulus $n = p^2q$, when both moduli have the same size s. What is the asymptotic multiplicative factor gained by the second method?

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

Please be patient.