LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Advanced Cryptography

Final Exam

June 24th, 2008

Duration: 4 hours

This document consists of 16 pages.

Instructions

Electronic comunication devices and are *not* allowed.

Other electronic devices and all printed documents are permitted.

Answers must be written on the exercises sheet.

This exam contains 3 *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 Meet in the Middle vs Collision Search

We consider a block cipher E mapping a key $K \in \{0,1\}^{\ell_K}$ and a message block $x \in \{0,1\}^{\ell}$ to $\mathsf{E}(K,x) \in \{0,1\}^{\ell}$. We denote $\mathsf{E}^{-1}(K,y)$ the inverse permutation, i.e. $\forall K,x : \mathsf{E}^{-1}(K,\mathsf{E}(K,x)) = x$.

We consider the double-encryption block cipher $\bar{\mathsf{E}}$ mapping a key $K = (K_1,K_2) \in \{0,1\}^{\ell_K} \times \{0,1\}^{\ell_K}$ and a message block $x \in \{0,1\}^{\ell}$ to

$$\bar{\mathsf{E}}(K_1,K_2,x) = \mathsf{E}(K_2,\mathsf{E}(K_1,x)).$$

We consider a known plaintext attack against $\bar{\mathsf{E}}$ using a sample (x_0,y_0) with $y_0 = \bar{\mathsf{E}}(K,x_0)$. The purpose of the attack is to find K_1 and K_2 given x_0 and y_0 only.

1.1 Preliminaries

We assume that K is random and that $\mathsf{E}(K,\cdot)$ behaves like the perfect cipher, i.e. the uniformly distributed random permutation $\mathsf{C}^\star$ over $\{0,1\}^{\ell}$. We further assume that $\ell_K \ll \frac{\ell}{2}$.

1. Let x and y be two fixed elements of $\{0,1\}^{\ell}$. Depending on ℓ and ℓ_K, what is the *expected* number of K_1 that satisfy $\mathsf{E}(K_1,x) = y$?

2. Given a fixed $x \in \{0,1\}^{\ell}$ and a fixed $K_0 \in \{0,1\}^{\ell_K}$ and depending on ℓ and ℓ_K, what is the *expected* number of K_1 that satisfy $\mathsf{E}(K_1,x) = \mathsf{E}(K_0,x)$?

3. Depending on ℓ and ℓ_K, what is the *expected* number of (K_1, K_2) pairs that satisfy $\bar{\mathsf{E}}(K_1, K_2, x_0) = y_0$?

1.2 Brute-force attacks

4. What would be the time complexity and memory complexity of a brute-force attack against $\bar{\mathsf{E}}$ if it was a regular block cipher (i.e. not using the structure of double encryption)?

5. What would be the time complexity and memory complexity of a generic brute-force attack against the double encryption $\bar{\mathsf{E}}$?

1.3 Towards a collision search problem.

Let g be defined as:

$$g(b, K) = \begin{cases} \mathsf{E}(K, x_0) & \text{if } b = 0 \\ \mathsf{E}^{-1}(K, y_0) & \text{if } b = 1 \end{cases}$$

6. Show that there is a collision on g which is related to the (K_1, K_2) pair we are looking for.

7. By using some expected properties of E from the preliminaries, show that it is likely that there exists a single collision on g.

2 Key Agreement Protocols

E-passports include a contactless chip which can establish a secure communication channel together with *any* reader. We denote icc the chip of the passport and ifd the reader. We consider several protocols and study their security.

2.1 Basic Access Control (BAC)

The BAC protocol enables the chip and the reader to agree on a symmetric key. The reader proves that it is authorized to access to the chip by showing evidence that he knows the passport number. Here, we assume that this passport number is a string w with 48 bits of entropy.

BAC works as follows:

- both devices derive $K_0 = F(w)$ from w and each one of them pick a random number N_i and random key K_i ($i = \mathsf{icc}, \mathsf{ifd}$);
- the chip sends its random number N_{icc} to the reader;
- using a block cipher and a MAC, the reader sends $N_{\mathsf{ifd}} \| N_{\mathsf{icc}} \| K_{\mathsf{ifd}}$ protected by K_0 to the chip;
- the chip decrypts the message and checks the MAC, then verifies that the received N_{icc} is consistent with the sent one. Ahter that, it sends $N_{\mathsf{icc}} \| N_{\mathsf{ifd}} \| K_{\mathsf{icc}}$ protected by K_0 to the reader;
- the reader decrypts the message and checks the MAC, then verifies that N_{icc} and N_{ifd} are correct;
- both devices derive a key $K_1 = G(K_{\mathsf{icc}} \oplus K_{\mathsf{ifd}})$;
- finally, a secure communication channel protected by K_1 is open using a block cipher and a MAC and some handshake messages are exchanged.

First, we study the security of key agreement alone, thus we assume that w is known to the adversary.

1. Consider first a passive attack and study the problem of deriving K_1 from all exchanged messages between the chip and the reader. Does the protocol resist passive attacks? Detail your answer.

2. Does it resist to man-in-the-middle attacks? Detail your answer.

Now, we study the security of access control, thus we assume that w is unknown to the adversary.

3. Consider a passive attack and study the problem of deriving w from all exchanged messages between the chip and the reader. Does the protocol resist passive attacks? Detail your answer.

2.2 Extended Access Control (EAC)

The EAC protocol consists of two separate protocols: Chip authentication and Terminal authentication.

- Chip authentication enables the chip to authenticate itself and to agree on a key. The protocol is a variant of the Diffie-Hellman protocol (based on elliptic curves) with a static key for the chip and an ephemeral one for the reader and derives a symmetric key K_1.
- Terminal authentication enables the reader to prove it is authorized to access to the chip. For this, the reader first provides a certificate from an authority assessing its authorization to read the chip and containing an ECDSA public key. The reader is assumed to possess the corresponding ECDSA secret key. The chip sends to the reader a random challenge x. The reader computes an ECDSA signature of x concatenated with the ephemeral key which was used during the Chip authentication protocol and sends the signature to the chip. The chip verifies that the ECDSA signature is correct. If succeeded, the chip can open read access to the reader through the secure communication channel.

We assume that the static key is authenticated by specific means.

Let us first consider the Chip authentication protocol.

4. Recall how the Diffie-Hellman protocol works, where the static key is used, where the ephemeral key is used, and how K_1 is derived.

5. Consider first a passive attack and study the problem of deriving K_1 from all exchanged messages between the chip and the reader. Does the protocol resist passive attacks? Detail your answer.

6. Does it resist to man-in-the-middle attacks? Detail your answer.

We now consider the Terminal authentication protocol.

7. Consider the problem of accessing the chip with no authorization through active attacks. Does the protocol resist to such attacks? Detail your answer.

3 $p + 1$ Factoring Method

Let n be an integer to factor.

3.1 Reminders

1. Recall how the $p - 1$ method works and when it applies.

3.2 Ring constructions

Let p be a prime factor of n and let θ be an invertible element in $\mathbf{Z}_n$. We define $R = \mathbf{Z}_n^2$ with the following operations:

$$\begin{aligned} (a, b) + (c, d) &= ((a + c) \bmod n, (b + d) \bmod n) \\ (a, b) \times (c, d) &= ((ac - bd\theta) \bmod n, (bc + ad) \bmod n) \end{aligned}$$

2. Show that R is a ring.

We define $F = \mathbf{Z}_p^2$ with the following operations:

$$\begin{aligned}(a,b)+(c,d) &= ((a+c) \bmod p, (b+d) \bmod p)\\ (a,b)\times(c,d) &= ((ac-bd\theta) \bmod p, (bc+ad) \bmod p)\end{aligned}$$

3. Show that F is a field when θ is a non-quadratic residue in $\mathbf{Z}_p^*$.

4. If θ is selected at random in $\mathbf{Z}_n^*$, what is the probability that it is a non-quadratic residue in $\mathbf{Z}_p^*$?

Let $\varphi : R \longrightarrow F$ be defined by

$$\varphi(a, b) = (a \bmod p, b \bmod p)$$

5. Show that φ is a surjective ring homomorphism.

6. Let $G \subset R$ be the set of all $(a, b) \in R$ s.t. $a^2 - \theta b^2 = 1$. Show that $\varphi(G)$ is a subgroup of F of order $p + 1$.

3.3 Factoring method

From now on we assume that there exists a prime factor p of n such that $p + 1$ is smooth. The purpose of the method is to find p given n. We use the ring R of the previous questions and the function φ.

7. Show that given a random $x \in G$ and an integer B such that $B!$ is a factor of $p + 1$, then $\varphi(x^{B!}) = (1, 0)$.

   Reminder: $x^\alpha = x \times x \cdots \times x$ (α times).

8. Given a random y such that $\varphi(y) = (1, 0)$, find an algorithm to compute p with high probability.
Note: Observe that φ cannot be computed since p is unknown.

9. Inspired by the previous questions, detail an algorithm to factor n.
   Hint: θ can be chosen *after* choosing $x \in R$

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

Please be patient.