LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Security and Cryptography

Final Exam

January 12$^{\text{th}}$, 2010

Duration: 3 hours

This document consists of 18 pages.

Instructions

Electronic comunication devices and documents are *not* allowed.

A pocket calculator is allowed.

Answers must be written on the exercises sheet.

This exam contains 3 *independent* exercises.

Answers can be either in French or English. Readability and style of writing will be part of the grade.

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 Vigenère Cipher

We formalize the Vigenère Cipher as follows:

- Let $\mathsf{A} = \mathbb{Z}_{26}$ denote the alphabet, A^* denotes the set of all finite sequences (or *strings*) of elements in A. For $s \in \mathsf{A}^*$ we denote by $|s|$ its length and s_i its ith term for $i = 0, 1, \ldots, |s| - 1$.
- The plaintext space, key space, and ciphertext space are A^*.
- We assume that given a random plaintext $X = (X_0, \ldots, X_{n-1})$ of length n, all X_i are independent with distribution p. That is

$$\Pr\left[X = x \,\middle|\, |X| = n\right] = \prod_{i=0}^{n-1} p(x_i)$$

- We assume that given a key $K = (K_0, \ldots, K_{k-1})$ of length k, all K_i are independent and follow a uniform distribution. That is

$$\Pr\left[K = \kappa \,\middle|\, |K| = k\right] = \frac{1}{26^k}$$

- The ciphertext is defined by

$$Y_i = X_i + K_{i \bmod k} \bmod 26$$

  for $i = 0, 1, \ldots, n - 1$.

1. Assuming that the key is of length k, what is the entropy of K in terms of bits?

2. How large should be k to have an equivalent key length of 80 bits?

3. Given a string s, we define the index of coincidence $I_c(s)$ as the probability that two elements of s selected at random at different positions are equal. Given $c \in A$, let $n_s(c)$ be the number of index positions i such that $s_i = c$.

   Show that

$$I_c(s) = \sum_{c \in A} \frac{n_s(c)(n_s(c) - 1)}{|s|(|s| - 1)}$$

4. Let X be a random plaintext of length $n = |X|$. Express the expected value $I_p = E(I_c(X))$ in terms of n and p.

We denote I_u the value of I_p when p is the uniform distribution.
Deduce I_u from the previous question.

5. Let $n = qk + r$ be the Euclidean division of n by k. We pick I and J different with uniform distribution and let $\mathcal{E}$ be the event that $I \bmod k = J \bmod k$.

   Show that $\Pr[Y_I = Y_J | \neg\mathcal{E}] = I_u$.

   Show that $\Pr[Y_I = Y_J | \mathcal{E}] = I_p$.

Show that

$$\Pr[\mathcal{E}] = \frac{q(2n - k(q+1))}{n(n-1)}$$

Deduce the value $E(I_c(Y))$.

Using $n \gg 1$, $q \approx \frac{n}{k}$ and $E(I_c(Y)) \approx I_c(Y)$, deduce a formula to estimate k based on $I_c(Y)$.

2 Secure Channel

1. Assuming that Alice and Bob share a secret key K and want to set up a secure channel, explain what are the properties of

   - message confidentiality
   - message authenticity
   - message integrity
   - message sequentiality

2. The GSM secure channel works by sending $m \oplus \mathsf{A5}(\mathsf{KC}, \mathsf{Count})$ where KC is an encryption key and Count is an implicit message counter.

   Which of the properties of Q. 1 is guaranteed, which is not? Explain precisely your answer. (If the answer is neither a clear *yes* nor a clear *no*, explain why.)

3. The Bluetooth secure channel works by sending $(m \| \mathsf{CRC}(m)) \oplus \mathsf{E0}(K_c, \mathsf{CLK})$ where K_c is an encryption key, CLK is the clock value, and CRC is a cyclic redundancy check function (i.e. a linear mapping).

   Which of the properties in Q. 1 is guaranteed, which is not? Explain precisely your answer. (If the answer is neither a clear *yes* nor a clear *no*, explain why.)

4. The WEP secure channel works by sending $\mathsf{IV}\|((m\|\mathsf{CRC}(m)) \oplus \mathsf{RC4}(K, \mathsf{IV}))$ where K is an encryption key, IV is an asynchronous initial vector, and CRC is a cyclic redundancy check function (i.e. a linear mapping).

   Which of the properties in Q. 1 is guaranteed, which is not? Explain precisely your answer. (If the answer is neither a clear *yes* nor a clear *no*, explain why.)

5. The TLS protocol works by sending $\mathsf{Enc}_{K_1}(m \| \mathsf{MAC}_{K_2}(m \| \mathsf{seq}))$ where K_1 and K_2 are two secret keys and seq is an implicit message counter.

   Which of the properties in Q. 1 is guaranteed, which is not? Explain precisely your answer. (If the answer is neither a clear *yes* nor a clear *no*, explain why.)

6. The biometric passport works by sending $\mathsf{Enc}_{\mathsf{KSenc}}(m)\|\mathsf{MAC}_{\mathsf{KSmac}}(\mathsf{Enc}_{\mathsf{KSenc}}(m))$ where KSenc and KSmac are two secret keys.

   Which of the properties in Q. 1 is guaranteed, which is not? Explain precisely your answer. (If the answer is neither a clear *yes* nor a clear *no*, explain why.)

3 TCHO Encryption

The goal of the exercise is to study the TCHO public-key cryptosystem.

- We consider the usual $+$ and $\times$ operations in $\mathbb{Z}_2$.
- The plaintext space is $\{0,1\}$ (we encrypt a single bit) and the ciphertext space is $\{0,1\}^\ell$ (the ciphertexts are ℓ-bit long).
- The public key is a polynomial of degree d with coefficients in $\mathbb{Z}_2$ denoted $P(z) = P_0 + P_1 z + \cdots + P_d z^d$.
- The secret key is a polynomial of degree d_K with coefficients in $\mathbb{Z}_2$ denoted $K(z) = K_0 + K_1 z + \cdots + K_{d_K} z^{d_K}$.
- These two polynomials are such that:
  - $P(z)$ divides $K(z)$ in $\mathbb{Z}_2[z]$;
  - $K(z)$ has a total number w of nonzero coefficients which is low. We assume that w is odd.
- We define four elementary operations.
  - **Repetition:** Given a plaintext x, we define the ℓ-bit vector $C(x) = (x, \ldots, x)$ (all components of $C(x)$ are equal to x).
  - **LFSR:** Given a d-bit vector $r = (r_0, r_1, \ldots, r_{d-1})$, we define its expansion to an ℓ-bit vector ($\ell > d$) by using the relation

    $$r_{i+d} = \sum_{j=0}^{d-1} r_{i+j} P_j$$

    for $i = 0, \ldots, \ell - 1 - d$ in $\mathbb{Z}_2$.

    Note that this relation is linear. We let $\mathcal{L}_P(r) = (r_0, r_1, \ldots, r_{\ell-1})$.
  - **Biased sequence:** Given a random seed r' we define $\mathcal{S}_\gamma(r')$ as a random ℓ-bit string such that the probability that each bit is 0 is given by $\frac{1+\gamma}{2}$ (its probability of being 1 is thus $\frac{1-\gamma}{2}$).
  - **Cancellation:** Given $y \in \mathbb{Z}_2^\ell$, we define $K \otimes y \in \mathbb{Z}_2^{\ell - d_K}$ by

    $$(K \otimes y)_i = \sum_{j=0}^{d_K} y_{i+j} K_j$$

    for $i = 0, \ldots, \ell - 1 - d$ in $\mathbb{Z}_2$.
- **Encryption:** To encrypt the bit x with randomness r and r', compute:

  $$\mathsf{Enc}_P(x; r, r') = C(x) + \mathcal{L}_P(r) + \mathcal{S}_\gamma(r')$$

  with component-wise addition over $\mathbb{Z}_2$.

1. Show that given $C(x) + \mathcal{S}_\gamma(r')$, the plaintext x can be recovered if γ is not too small. What is the complexity of the attack in terms of ℓ?

2. Show that given $C(x) + \mathcal{L}_P(r)$, the plaintext x can be recovered. What is the complexity of the attack in terms of d?

3. Show that for any $x \in \mathbb{Z}_2$ we have $K \otimes C(x) = (x, x, \ldots, x)$.

4. Show that for any $r \in \mathbb{Z}_2^d$ we have $K \otimes \mathcal{L}_P(r) = 0$.

5. Show that for a random r' all bits of $K \otimes \mathcal{S}_\gamma(r')$ have the same distribution and a probability of being 0 of $\frac{1}{2}(1+\gamma^w)$.
Hint: For any i, $(K \otimes \mathcal{S}_\gamma(r'))_i$ is the XOR of exactly w independent bits of bias γ.

6. Given $\mathsf{Enc}_P(x; r, r')$ and $K(z)$, give an algorithm to recover x. What is its complexity in terms of the parameters d_K and ℓ?

7. To study the security, give an algorithm to recover $K(z)$ given $P(z)$, d_K and w. What is its complexity?
Hint: if $K(z) = 1 + \sum_{j=1}^{w-1} z^{i_j}$, it satisfies a condition which can be written

$$1 + \sum_{j=1}^{\frac{w-1}{2}} z^{i_j} = \sum_{j=\frac{w-1}{2}+1}^{w-1} z^{i_j} \pmod{P(z)}$$

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

Please be patient.