Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 1

Out: 04/25/2006 Solution available on: 05/04/2006 Saarland University

Problem 1: Cryptanalysis of the Vigenere Cipher

The following ciphertext was encrypted using the Vigenere-Cipher (The text is available for download on the course web page), where all spaces and punctuation was removed. Decrypt it, using any tool you like.

```
FHJWN XYLWA XTMQS QXJZC USJXU DSZMD IAXBO XEYGO
GAYTE MSYWN OEGZO ISJBH QWJJF ARXWM QKNVD QRLIR
PESKR KPYWT AOQAS QVJZA XOKBH QMFZE MVFQL MBQMA
EYTCS QEFVD BLFGI ZGFZO GNIEI FHYPE YCFVB QAQWT
AFKCN NUYVO IPQMA EEKWR SEYIB AUYBH USFVC UESBS
FUKNF ARYPE DEXBO RTMMC AUWAE
```

Problem 2: Relations between Adversarial Goals

Give separating examples for the following adversarial goals (since we did not give precise definitions for all goals, you do not need any proofs but informal arguments suffice):

(a) Construct an encryption scheme that is resistant against *total break* but not against *universal break* under ciphertext-only attacks. More precisely, let $c \leftarrow \mathsf{E}(K, m)$ denote a ciphertext for some K, m. Then it should not be possible to extract K only given c, but m should be easily extractable from c. This should hold for all values of K and m.

(b) Construct an encryption scheme that is resistant against *universal break*, but not against *selected-plaintext break* under ciphertext-only attacks: There should exist two messages m_1, m_2 such that there is no algorithm that can recover m_1 given $c_1 \leftarrow \mathsf{E}(K, m_1)$ for a random K, but there exists an efficient algorithm that recovers m_2 given only $c_2 \leftarrow \mathsf{E}(K, m_2)$ for a random K.

(c) Construct an encryption scheme that is resistant against *selected-plaintext break*, but not against *loss of partial information* under ciphertext-only attacks: For all messages m there should be no algorithm that can uniquely recover m given only $c \leftarrow \mathsf{E}(K, m)$ for a random key K, but the encryption scheme should not have perfect secrecy.

(**Hint**: Something "stupid" might work. For (b) and (c) it might be convenient to start with an encryption scheme that provides perfect secrecy.)

Problem 3: Encryption Schemes and Perfect Secrecy

Consider the following encryption scheme. Let $\mathcal{M} := \{0, 1\}$ and $\mathcal{K} := \mathcal{C} := \{1, 2, 3\}$ denote the set of plaintexts, keys and ciphertexts, respectively. Let encryption E be defined by the following table:

m	$\mathsf{E}(1, m)$	$\mathsf{E}(2, m)$	$\mathsf{E}(3, m)$
0	1	3	2
1	3	2	1

(a) Give a decryption function D such that (E, D) constitutes an encryption scheme over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$.

(b) Does your scheme have perfect secrecy? Give a proof or a counterexample.

Problem 4: Perfect Secrecy for Two-time Key Use

In class we gave the definition perfect secrecy for the case when the adversary sees the encryption of a single message: namely, for all m_0,m_1, and c, we have

$$\mathsf{Pr}[c = c'; K \leftarrow_R \mathcal{K}, c' \leftarrow \mathsf{E}(K, m_0)] = \mathsf{Pr}[c = c'; K \leftarrow_R \mathcal{K}, c' \leftarrow \mathsf{E}(K, m_1)]$$

(a) Formulate a definition of perfect secrecy for the case when the adversary sees the encryption of two messages (using the same key K).
(**Hint**: you should have messages m_0, m_1, m_0', m_1'.)

(b) Argue that no deterministic encryption scheme can satisfy your definition in part (a). Does it help if we allow encryption to be randomized?
(**Hint**: Consider the case that some messages of m_0, m_1, m_0', m_1' are equal.)

Problem 5: Secret Sharing

Assume that you are given a highly secret document and have two places of medium physical security where it could potentially be deposit.

(a) How could you share the secret document among both places such that both places are jointly able to reconstruct the document but if the attacker only gains access to one of the places, it learns no information at all about the document?

(b) Generalize your solution to n places: All n places are jointly able to reconstruct the secret but an attacker does not learn any information about the secret if only having access to at most $n - 1$ places.

Problem 6*: Spy Games: Encryption with a Deck of Cards

(* This problem is a rather hard one and not relevant for the quizzes.*)

Bob randomly shuffles a deck of 52 cards and deals half of them to himself, and the remaining half to his partner Alice. Later Bob wants to secretly transmit an n-bit message to Alice for the largest possible value of n. Moreover, he wants to achieve perfect secrecy in doing so. Assume Bob is allowed to publicly (i.e., both Alice and the attacker will hear it) announce anything he wants. Show that Bob can achieve $n = 48$, but cannot achieve $n = 49$. For the first part, give an explicit algorithm allowing Bob to secretly "send" 48 bits; for the second part you have to argue why 49 bits are impossible. Optionally, tell the exact maximal number of possibilities (which is between 2^{48} and 2^{49}) that Bob can encode.
(**Hint**: This strongly relies on $n!$ and $\binom{n}{t}$ for appropriate values of t. A scientific calculator might become handy.)