Cryptography (SS2006) Prof. Michael Backes

Solutions for Exercise Sheet 1

Out: 05/05/2006 Saarland University

Problem 1: Cryptanalysis of the Vigenere Cipher

This solution was meant to demonstrate how weak these historic ciphers are and to show you how much crypto-related stuff can be found in the Internet. Consequently, the encrypted message was the following:

> The only goal this exercise pursued was to let you at least once browse the web for some kindergarden crypto tools. Several of them are available as you see, and playing around with them can be a lot of fun. But now please forget about this ancient stuff for the rest of this course.

My favorite tool for breaking Vigenere Ciphers is

`http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html`,

but several others are available. The first step always consists in identifying the length of the key. This is usually done as follows: for every key-length n, calculate letter frequencies. If these look like the (shifted) letter frequencies of normal text, then we are likely to have found the correct keysize. The actual key is then computed by simple frequency analysis.

Be aware that the key "A" might either represent a shift by *zero* or by *one* position, depending on the implementation. The above implementation uses $A = 0$ and the key used to encrypt the example was MAFIA.

Problem 2: Relations between Adversarial Goals

The following examples should provide a deeper understanding of the different adversarial goals. The constructed schemes are artificial, but they provide insights into the differences of these notions. For all schemes let us fix $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^k$ for some $k \geq 2$.

(a) A scheme resistant against *total break* which is *universally breakable* is the following: Let $\mathsf{E}(K, m) := m$, and $\mathsf{D}(K, c) := c$. It can easily be verified that this is indeed an encryption scheme. It is resistant against total break, as the ciphertext c is completely independent of K, so no adversary can ever learn K from c. On the other hand, it is obviously universally breakable, as the encryption clearly leaks the plaintext.

(b) The following scheme is not *universally breakable*, however, selected plaintexts can be retrieved. Fix some plaintext $a \in \mathcal{M}$. Let $\mathsf{E}(K, m) := (K \oplus m) \mid\mid b$ where $b = \begin{cases} 1 & \text{if } m = a \\ 0 & \text{otherwise.} \end{cases}$. Decryption is given by splitting a given ciphertext c into $c' \in \{0,1\}^k$ and $b \in \{0,1\}$, i.e., $c' \mid\mid b = c$, and calculating $\mathsf{D}(K, c) = K \oplus c'$. Obviously this scheme is *partially breakable* as the message a can be extracted from the ciphertext by checking if the bit equals 1. However, the cipher is not *totally breakable*, as an adversary cannot decide which message is inside a given ciphertext. The only information available is whether or not the plaintext is a.

(c) For the last scheme no plaintext can be retrieved from a given ciphertext. However, it leaks *partial information* about the plaintexts. Let $\mathsf{E}(K, m) := K \oplus m \mid\mid m^{(0)}$ where $m^{(0)}$ is the last bit of m. This does not allow the adversary to retrieve any plaintext, but obviously leaks one bit of the message.

Problem 3: Encryption Schemes and Perfect Secrecy

(a) One possible decryption function is the following:

c	$\mathsf{D}(1,c)$	$\mathsf{D}(2,c)$	$\mathsf{D}(3,c)$
1	0	1 $(*)$	1
2	1 $(*)$	1	0
3	1	0	1 $(*)$

Notice that the entries marked with a star $(*)$ are not fixed by the correctness property of encryption. However, decryption is defined as a function from $\mathcal{C}$ to $\mathcal{M}$, so one needs to specify these values to get a function.

(b) To prove that this scheme provides perfect secrecy, one simply checks that, for any $c \in \mathcal{C}, m \in \mathcal{M}$, the following holds:

$$\mathsf{P}\left[c = c'; K \leftarrow_{\mathcal{R}} \mathcal{K}, c' \leftarrow \mathsf{E}(K,m)\right] = \frac{1}{|\mathcal{K}|} = \frac{1}{3}.$$

Since this value does not depend on m, we have that for all $m_0, m_1 \in \mathcal{M}$ and for all $c \in \mathcal{C}$

$$\mathsf{P}\left[c = c'; K \leftarrow_{\mathcal{R}} \mathcal{K}, c' \leftarrow \mathsf{E}(K,m_0)\right] = \mathsf{P}\left[c = c'; K \leftarrow_{\mathcal{R}} \mathcal{K}, c' \leftarrow \mathsf{E}(K,m_1)\right].$$

As desired, this is the definition of perfect secrecy.

Problem 4: Perfect Secrecy for Two-time Key Use

(a) A cipher (E, D) provides perfect secrecy for two-time key use iff for all $m_0, m_1, m_0', m_1' \in \mathcal{M}$ and for all $c_0, c_1 \in \mathcal{C}$ the following holds:

$$\begin{aligned} & P\left[c_0 = c_0' \wedge c_1 = c_1'; K \leftarrow_{\mathcal{R}} \mathcal{K},\ c_0' \leftarrow \mathsf{E}(K,m_0),\ c_1' \leftarrow \mathsf{E}(K,m_1)\right] \\ = \quad & P\left[c_0 = c_0' \wedge c_1 = c_1'; K \leftarrow_{\mathcal{R}} \mathcal{K},\ c_0' \leftarrow \mathsf{E}(K,m_0'),\ c_1' \leftarrow \mathsf{E}(K,m_1')\right] \end{aligned}$$

Intuitively, this means that no adversary can tell which two plaintexts have been encrypted, seeing the two ciphertexts.

(b) If encryption is deterministic, i.e., for all $K \in \mathcal{K}$ the function $\mathsf{E}(K,\cdot)$ is deterministic, then for every randomly choosen key $K \leftarrow_{\mathcal{R}} \mathcal{K}$ and messages $m_0 = m_0' = m_1 \neq m_1'$, the following holds, where $c_0 = c_1 = \mathsf{E}(K,m_0)$:

$$P\left[c_0 = c_0' \wedge c_1 = c_1'; K \leftarrow_{\mathcal{R}} \mathcal{K},\ c_0' \leftarrow \mathsf{E}(K,m_0),\ c_1' \leftarrow \mathsf{E}(K,m_1)\right] \geq \frac{1}{|\mathcal{K}|} > 0,$$

but

$$P\left[c_0 = c_0' \wedge c_1 = c_1'; K \leftarrow_{\mathcal{R}} \mathcal{K},\ c_0' \leftarrow \mathsf{E}(K,m_0'),\ c_1' \leftarrow \mathsf{E}(K,m_1')\right] = 0.$$

This violates the definition given in (a).

In fact, even probabilistic encryption does not solve this problem. If encryption is correct, i.e., for all $K \in \mathcal{K}$ and for all $m \in \mathcal{K}:\ \mathsf{D}(K, \mathsf{E}(K,m)) = m$, then the following holds: Given $m_0, m_1 \in \mathcal{M}$, with $m_0 \neq m_1$, and $K' \in \mathcal{K}$, let $c := \mathsf{E}(K', m_0)$. Then for all $K \in \mathcal{K}$ it holds that $\mathsf{E}(K,m_1) \neq c$. Using the same argument as above one sees that this does not provide perfect secrecy.

Problem 5: Secret Sharing

There are, of course, several solutions to this exercise but the simplest one is the following. Let the secret S be encoded into a bitstring of length m.

(a) Choose a random bitstring r of length m. Store r in one place, and store $r \oplus S$ in the other place. Then one can easily reconstruct the secret S knowing both r and $r \oplus S$. However, r itself contains no information about S, at is was chosen randomly, and even $r \oplus S$ alone contains no information about S, as it is uniformly distributed in the set of all bit-strings of length m (being a one-time pad encryption).

(b) This construction can easily be generalized to n places: Choose $n-1$ random strings r_i of length m, store them in different places, and store $r_1 \oplus \ldots \oplus r_{n-1} \oplus S$ in the last place. The same argument as above shows that every subset of $n-1$ places contains no information about S, while it can easily be reconstructed from the information in all n places.

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

Shannons theorem says that $|\mathcal{K}| \geq |\mathcal{C}|$ has to hold to achieve perfect secrecy, and we always have $|\mathcal{C}| \geq |\mathcal{M}|$ as encryption is injective. So we can encrypt at most $|\mathcal{K}|$ plaintexts providing perfect secrecy. The number of keys $|\mathcal{K}|$ can easily be calculated as

$$|\mathcal{K}| = \binom{52}{26} = \frac{52!}{26! \cdot 26!} = 495918532948104 \approx 2^{48.4}.$$

This proves that at most 48 bits can be secrectly transmitted. We omit the description of an algorithm that indeed securely transmits 48 bits, i.e., achieves this upper bound. Reading a lot of spy novels will eventually tell you some ways how this can be done. :-) Alternatively, please ask one of our teaching assistants.