Information Security 2018

Exercise session 1

Historical ciphers, perfect security, computational security

Exercise 1 (historical ciphers)

Encrypt the plaintext “INFORMATION SECURITY” using the following ciphers:

1. **Shift cipher** using the last 2 digits of you Student ID mod 26. For example, if your Student ID is 05-981-234, the key is 34 mod 26 = 8.
2. **Vigenere cipher** using “ETH” as the key.

Exercise 2 (historical ciphers)

Suppose that the following is the output of a **substitution cipher**:
“SIAA ZQ LKBA. VA ZOA RFPBLUAOAR”.
Assume the cleartext to be in English. What is the **most likely** ciphertext letter corresponding to the plaintext letter “E”?

Exercise 3 (historical ciphers)

Show that the **shift**, **substitution**, and **Vigenere ciphers** are all trivial to break using a known-plaintext attack.

How much known plaintext is needed to completely recover the key for each of the ciphers?

Exercise 4 (historical ciphers)

The lecture slides describe an **attack** by Kasiski et al. on the **Vigenere cipher**. To prevent the attack, the following **modification** has been proposed:

Given the period t of the cipher (i.e., the encryption key k has length t), the plaintext is broken up into blocks of size t. We encrypt the ith character in the jth block by adding $k_i + j \bmod 26$.

(a) Describe the effect of the above modification on Kasiski's attack.

(b) Explain a way to determine the period t for this scheme, and that way attack the modified scheme.

Exercise 5 (perfect security)

When using the **one-time pad** with the key $k = 0^l$, it follows that $\mathrm{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^l$.

- Is this an improvement? In particular, is it still perfectly secret? Prove your answer.
- If your answer is positive, explain why the one-time pad is not described in this way.
- If your answer is negative, reconcile this with the fact that encrypting with 0^l does not change the plaintext.

Exercise 6 (perfect security)

Prove or refute the following claim:

Every **encryption scheme**, for which the size of the **key space** equals the size of the **message space**, and for which the key is chosen uniformly from the key space, is perfectly secret.

Exercise 7 (perfect security)

Prove or refute the following claim:

For every encryption scheme that is **perfectly secret** it holds that for **every distribution** over the message space M, every m, $m' \in M$, and every $c \in C$:

$$Pr[M = m | C = c] = Pr[M = m' | C = c].$$

Exercise 8 (computational security)

We say that an encryption scheme (*Enc*, *Dec*) is **CPA-secure** if every randomized **polynomial time** adversary guesses b correctly with **probability at most** $0.5 + \epsilon(n)$, where ϵ is negligible.

Prove that this definition of CPA-secure encryption cannot be satisfied, if the oracle can encrypt **arbitrary-length messages** and the adversary is not restricted to output equal-length messages.

Exercise 9 (1/2) (Cryptanalysis)

- Download the file "cipher" from the course webpage. It contains a single line of 151,530 ascii characters.
- All characters are lower case letters between ‘a’ and ‘z’ inclusive. No other special characters, spaces, or digits.
- The file is a Vigenere Cipher of a passage written in English.
- The key is a randomly chosen string of lower-case ascii characters between ‘a’ and ‘z’ inclusive, and has a randomly-chosen length (between 1 and 80 characters).
- Use whatever programming language you prefer to decrypt the file.

Exercise 9 (2/2) (Cryptanalysis)

- Hint 1: copy this string of English letter frequency from the lecture to use in your code: "etiaonsrhcldpyumfbgwvkxqzj".
- Hint 2: you can use the sum of a 1-dimensional Euclidean Distances (ED) to measure the deviation between candidate plaintext character frequency and the English pattern.
  - Example: total ED between "iemhd" and "himed" is 1+2+0+3+0 = 6.
  - Example: total ED between "etiaonsrhcldpyumfbgwvkxqzj" and "teiaonsrhcldpyumfbgwvkxqzj" is 2 .
- Hint 3: first assume a fixed key length (e.g., 10) and guess the key character by character.