Cryptography and Networked Systems Security

Prof. Dr.-Ing. Volker Roth
Freie Universität Berlin

Homework 1

Academic Integrity

Hereby I certify that I have neither received nor given help in answering the questions in this homework assignment.

_____

Date, signature, name in block letters

Question 1 (5 pts.)

Provide a formal definition of the Gen, Enc, and Dec algorithms for both the mono-alphabetic substitution and Vigenère ciphers. Remark: a permutation is typically denoted π.

Question 2 (10 pts.)

In an attempt to prevent Kasiski's attack on the Vigenère cipher, the following modification has been proposed. Given the period t of the cipher, the plaintext is broken up into blocks of size t. Recall that within each block, the Vigenère cipher works by encrypting the ith character with the ith key (using a shift cipher). Letting the key be $k_1, \ldots, k_t$, this means the ith character in each block is encrypted by adding k_i to it, modulo 26. The proposed modification is to encrypt the ith character in the jth block by adding $k_i + j \mod 26$.

1. Show that decryption can be carried out.

2. Describe the effect of the above modification on Kasiski's attack.
3. Devise an alternate way to determine the period for this scheme.

Question 3 (10 pts.)

Show that the shift, substitution, and Vigenère 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?

Question 4 (5 pts.)

Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext must be encrypted in order for the adversary to completely recover the key? Compare to the amount of plaintext necessary for a known-plaintext attack.

Question 5 (10 pts.)

Decrypt the following ciphertext. What is the decryption key?

```
MKKBPNRBPVNNKGBMKKMFUOKFBVTOFQZD
DPPSZKOHNYHOBFELUEURGFGRKORLMRVK
FSFKOANYHOPHNUFIBZWKGMKKLFOJPEGO
JCAFTNHSIAVOUZQYHOIXFKAAREKWTUGV
LTMZZEARMNHTDHGAGRYOAAFJBECNKOPF
JQUZTDRTOCSKAHPJKKBPNDCOFSNUAPCY
AQIXFNSGCPXSXUYABPNYJBFTKGASBZKZ
AXEINPFAWKBBNVLPDRDHZNDBLLNZAYIM
KKPLNRZDPFAGFNURWZFAKGGTSOANMXZX
SRBZVSCKRVKFSZDKHRKQOTOZOMFMNBZM
RXWSGCTKSCN
```

The ciphertext was generated with a Beauford cipher. The encryption function of the Beauford cipher is defined as follows:

Gen: Let t be the period. For $i = 0, \ldots, t-1$ set k_i to be a random number in $\{0, \ldots, 25\}$. Output the key $k = k_0, \ldots, k_{t-1}$.

Enc: Given plaintext $p = p_0, \ldots, p_n$ set $c_i = k_{(i \mod t)} - p_i \mod 26$. Output $c = c_0, \ldots, c_n$.