Criptografia i Seguretat [104355]

Exercises Classical Cryptography

1. We have an encrypted message "VRBXQSHSLQLOOR", which has been encrypted using a simple substitution (mono-alphabetic) cipher, as $c_i = m_i + k \pmod{n}$ with an unkown k and $n = 26$. The alphabet used is:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

   Find the value for k and the original message.

2. If now the encrypted message is "EHFJEQZHEKTPEXH", use the same program to find the worst time to find the original message. Can we find the k used? Is this cryptographic method secure?

3. Supose that we have a *cleartext* where the relative frequency of the symbol "a" is 0.1. We also know that the digram "ny" appears with a frequency of 0.02.
   (a) If we use a transposition cipher, will the letter "a" and the digram "ny" keep the same frequency in the *ciphertext*?
   (b) What happens if we use a simple or monoaphabetic substitution? Will the substituted symbols keep the same frequency in both cases?

4. The Vigenère method is a polyalphabetic substituion cipher with a variable length key.
   - We consider the key of length r as $k = (k_0, k_1, \ldots, k_{r-1})$
   - If the message M is greater than r, then the message is divided into blocks of size r. Given a block of r symbols: $m_0, m_1, \ldots, m_{r-1}$, each symbol is encrypted as: $c_i = m_i + k_i \pmod{n}$ for $0 \leq i \leq r-1$, and n is the size of the alphabet.

   Using the Vigenère cipher with the alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

   (a) If $n = 26$ and $r = 5$, what is the size of the key space?
   (b) Encrypt the message "VOLANDO VOY VOLANDO VENGO" (without spaces) with the key "CAMARON" using the Vigenère cipher and the previous alphabet of size $n = 26$.
   (c) We know that the cleartext "COMELVALLESNOHIHARES" has been encrypted as the ciphertext "OCXEXJLLXSDNAVTHMFPS". We also know that the key length is $r = 4$. Can you find the key?

5. The Hill cipher is a substitution cipher based on the use of matrices. We provide a broad description here:

- The key is an invertible square matrix $K_{r\times r}$ with elements in $\mathbb{Z}_n$ (the alphabet).
- The plaintext is encoded as a matrix $M_{r\times c}$.
- The encryption is computed as the matrix product, $C_{r\times c} = K \cdot M \pmod{n}$
- The decryption is computed using the key matrix inverse in $\mathbb{Z}_n$, $M = K^{-1} \cdot C \pmod{n}$

As an example, if we have the alphabet with 26 symbols, so $n = 26$ and the key:

$$K = \begin{pmatrix} 2 & 18 & 3 \\ 5 & 7 & 11 \\ 9 & 14 & 20 \end{pmatrix}$$

we can encrypt the message "CRIPTOGRAFIA", which in matrix form is:

$$M = \begin{pmatrix} 2 & 15 & 6 & 5 \\ 17 & 19 & 17 & 8 \\ 8 & 14 & 0 & 0 \end{pmatrix}$$

so the encryption is given by:

$$C = K \cdot M \pmod{26} = \begin{pmatrix} 22 & 24 & 6 & 24 \\ 9 & 24 & 9 & 3 \\ 0 & 5 & 6 & 1 \end{pmatrix}$$

which corresponds to the ciphertext "WJAYYFGJGYDB".

The Hill cipher (1929) is an example of a polygraphic substitution cipher, which performs a uniform substitution on blocks of letters. Note that this idea is slightly different as the monoalphabetic and polyalphabetic substitution that we have seen in class. It is usually considered as one of the first block ciphers in history.

(a) Encrypt the message "BARCELONA" using the Hill cipher with the same key K as the previous example.

(b) Using also the same key, can you decrypt the message "XELOEKSVVRQXAMQSZIEGCMGSULBYZYQDRKYEQKKUQEIEH"? (note: you need to compute K^{-1})

6. In a Hill cipher using matrices, Alice wants to use the key "POOL" while Bob wants to use "SWIM". Who should we trust?