Introduction to cryptology practical: symmetric cryptography

M1-MOSIG

Further information can be found on the web page : `http://membres-liglab.imag.fr/pernet/M1MOSIG_Crypto.html`

We consider the alphabet of 37 symbols formed by the 26 lower case letters of the alphabet, the most frequent punctuation signs, the space and the End Of Line symbol (EOL). The are mapped to integers modulo 37 according to table 1.

a	0	i	8	q	16	y	24	!	33
b	1	j	9	r	17	z	25	’	34
c	2	k	10	s	18	.	26	”	35
d	3	l	11	t	19	,	27	-	36
e	4	m	12	u	20	EOL	28		
f	5	n	13	v	21		29		
g	6	o	14	w	22	;	31		
h	7	p	15	x	23	?	32		

TABLE 1 – Encoding of the text symbols as integers

Exercice 1. Entropy

a. Write a function that computes the entropy of a message encoded as a vector of `int`.

b. Report experiments with several type of texts (uniform random, english, french, ...).

Exercice 2. Symmetric stream cipher

a. Write the encoding and decoding functions of a stream cipher where each symbol of the cipher-text is the sum modulo 37 of the corresponding symbols in the plain-text and the key.

b. Write two functions `LFSRFibo` and `LFSRGalois` taking as input a connecting polynomial (given as an array of coefficients), an initial state, and an integer n and returning the first n values of the output of the corresponding LFSR. Try to compute the result as efficiently as you can.

c. Compare the computation time of the two methods.

d. Write a program `Encode` that converts a file containing a plain-text into a file containing the corresponding cipher text, and a program `Decode` converting a cipher-text file into a plain-text file. Both programs will read the key (connecting polynomial and initial state) in a file.

Exercice 3. Attacks

In the following, we denote by d the length of the LFSR and by n the length of the message.

Attack of the cipher viewed as a Vigenere cipher

a. Explain why the cipher that you implemented in the previous exercise can be viewed as a Vigenere Cipher. What condition on d and n should be verified.

b. Implement the computation of the length of the key by the method of Friedmann.

c. For plain texts in a natural language (english, french, ...), of length sufficiently large, compute the entropy of the plain text, the cipher-text and the key. Experiment with several lengths of LFSR. Comment on your results.

Attack of the LFSR by a known sub-sequence

d. We now suppose that a contiguous sequence of $k \geq d$ symbols of the plain-text is known. Write the linear system of equations that the coefficients of the connecting polynomial of the LFSR must satisfy. What is a necessary condition on k to find a unique solution to this system ?

e. From the previous question describe an attack that makes it possible to decipher the whole message. What is its complexity ?

f. Implement this attack with a function `LFSRBreak` taking as input, a cipher-text, the sequence of k consecutive symbols in the plain-text and its position, and returns the whole plain-text or FAILURE (if the condition on k is not met).