Security

Assignment 3, Wednesday, September 23, 2015

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, October 1, 24:00 (midnight) sharp!

Goals: After completing these exercises successfully you should

- perform a ciphertext-only attack on a transposition ciphers;
- encrypt and decrypt with linear shift feedback registers;
- analyse an incorrectly used one-time pad.

Marks: You can score a total of 100 points.

1. **(30 points)** You are given the following ciphertext encrypted with a transposition cipher:

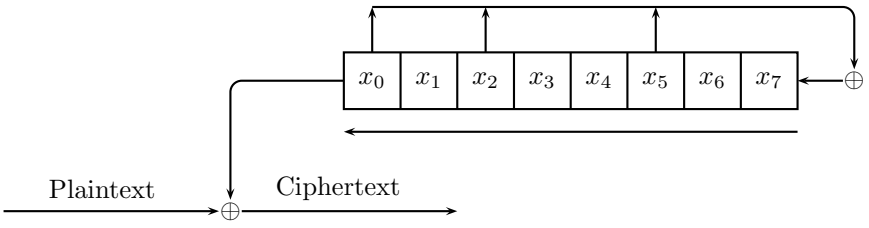
   ```
   SEOTSDNHAELTOENCACYLEDYOTTAFAPLNTLIAMOLANRISULHONODFRSI
   DMOLENFISMLAOEOANINSROSICDSIOORNETTWTOINNITGTXXYXXLXXXX
   ```

   (a) How can you tell that a transposition cipher was used (as opposed to *e.g.* substitution), by only looking at the ciphertext?

   (b) What is the probable block length? How would a simple change of the scheme (no change of the permutation) make it much harder to figure out the block length?

   (c) Use this as a first step to decrypt the ciphertext. Find the plaintext, and explain briefly how you did it.

2. **(30 points)** Consider the following simple Linear Feedback Shift Register (LFSR). The plaintext is bitwise XOR-ed with the output bits of the LFSR which **first computes** $x_0 \oplus x_2 \oplus x_5$ and **then shifts** such that x_0 falls out.



Example:

The initial state	**0**	1	**0**	1	1	**1**	0	1
is followed by	**1**	0	**1**	1	1	**0**	1	1
and outputs	**0**							

   (a) Describe the next five states of the LFSR if it is initialized according to the box above. The first successor state is already given as illustration, so you have to give the four subsequent ones.

(b) Also do a "rollback" and compute the *previous* four states, starting from the initial state.

(c) Assume you know that the LFSR is in the initial state given above. After four shifts you intercept 1111 as resulting ciphertext. Reconstruct the 4 bits of plaintext that were encrypted to this ciphertext.

3. **(40 points)**

The one-time pad scheme is a very secure encryption scheme, but it has one important disadvantage: The pad can only be used *once*.

In this exercise, you get a ciphertext that resulted from a one-time pad encryption, as well as some parts of the plaintext and the key stream. Additionally, there is a weakness you can exploit: The key stream used to create this ciphertext was not used only one time, but a part of it has been used multiple times. Using this knowledge, recover the plaintext. Note that the repetition can start at any point in the pad, and the bits at the start of the pad are not necessarily part of the repeating pattern. Once the repetition has started, it continues forever. In order to be able to perform an XOR operation on the bits, the characters in the plaintext are translated to 7-bit ASCII binary representation[1] (e.g. 'a' becomes `1100001`).

ASCII	d	o	n	'	t	...	r	...	...	...
plain	1100100	1101111	1101110	0100111	...	0100000	...	1100101	...	1100101
pad	1011001	0010101	...	...	...	...	...	...	0101101	...
XOR	0111101	1111010	1000000	1111101	...	...	0111100	0110000	1011101	...
ASCII	=	z	@	}	3	C	<	0	]	x

a	...	...	...	...	...	...	...	...	...	...
1100001	1110100	0100000	...	...	...	...	...	...	1101100	...
...	...	...	...	...	...	...	...	...	...	...
...	1111011	1100111	...	...	0101111	...	...	...	...	...
4	{	g	d	E	/	I	Y	z	b	\

[1] `http://en.wikipedia.org/wiki/ASCII`