Security

Assignment 3, Friday, September 29, 2017

Handing in your answers:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Bart or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, October 9, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- use the Vigenère cipher and one-time pad, and understand their relation.

Marks: You can score a total of 100 points.

1. **(45 points)** During the lecture, the Vigenère was introduced. For more background information, see e.g. `http://en.wikipedia.org/wiki/Vigenere_cipher`.

   (a) Decrypt the following Vigenère ciphertext using the key '`elephant`'.

   ```
   xtqtmlvxwwmzlaatvcslmrhbxqpxlsybopeqhnnge
   ```

   (b) The idea of book cipher encryption is that a certain clause of a book, or more generally a certain piece of text is used as key to the Vigenère cipher: Instead of specifying a single word as key, one gives a starting point in a piece of text, such as "The third word in the second line in the movie 'The Big Lebowski' from 1998". The key consists of continuous text starting from the specified word and is *as long as the message to encrypt*.
   Encrypt the following text with this method (The opening text of The Big Lebowski is available at `http://www.imdb.com/title/tt0118715/quotes`, the key thus starts with "the name of Jeff..."):

   ```
   That rug I had, really tied the room together.
   ```

   Remove all spaces and punctuation in both the key and the plaintext and convert all upper-case characters to lower case.

   (c) Book cipher encryption is stronger than Vigenère with a short, repeating, key. However, it is still not secure for sufficiently long messages. Why? How would the strength of the encryption scheme change if a non-English key is utilized?

2. **(55 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 and the rest of the table. 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	r	e	p	...	...	...		...
plain	1110010	1100101	...	...	1100001	...	0100000	1101001
pad	1011011	...	...	1011101	...	0101011	...	...
XOR	0101001	0100100	1001100	...	...	1011111	...	1011111
ASCII	)	$	L	8	9	_	;	_

t	...	...	...	...	...	...	...	...
...	...	...	...	...	...	1101111	...	...
...	...	...	...	...	...	...	...	...
1011010	...	1111010	...	...	...	1011001	1111110	...
Z	L	z	?	{	y	Y	~	Y

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