SECURITY

Assignment 3, Friday, September 29, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

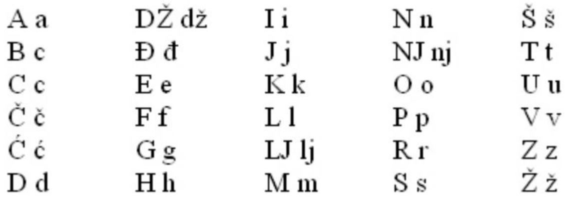
Teaching assistant: Joost Rijneveld

Assignment 1

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 lowercase.
    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?

Solution 1

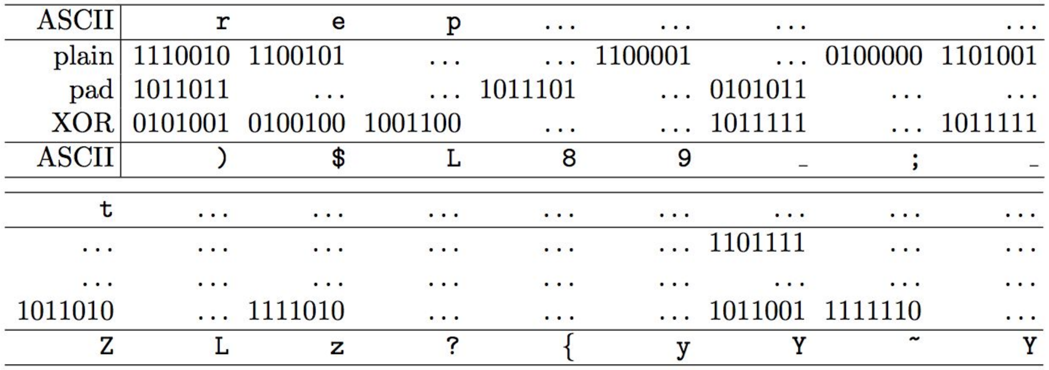
1. Solutions to the first assignment
    a. “Timeflieslikeanarrowfruitflieslikeabanana”
    b. Plaintext: “thatrugihadreallytiedtheroomtogether”
    Key: “fellabythenameofjefflebowski”
    Cipher: “yllerveboeqrqezqhxnjoxisngyuysrptick”
    c. To the second statement: It’s more difficult as it takes longer to brute-force. Given the english language it takes n time to brute-force. Changing to every language makes it inherently more difficult to decrypt. It would also be significantly harder to for instance use the croatian alphabet because of the extra characters involved. The croatian alphabet would include a lot more characters further strengthening the encryption.



A a	DŽ dž	I i	N n	Š š
B c	Đ đ	J j	NJ nj	T t
C c	E e	K k	O o	U u
Č č	F f	L l	P p	V v
Ć ć	G g	LJ lj	R r	Z z
D d	H h	M m	S s	Ž ž

Assignment 2

A. (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

Solution 2

We've made a copy of the table above and recovered the plaintext by completing the rest of the table. The PAD section of our table has two colors, blue and green, which mark the repeating part in the pad. The first blue section consists the first repeating section. The following green section marks the next repetition. This repetition keeps on going forever.

ASCII	r	e	p	e	a	t	space	i	
PLAIN	1110010	1100101	1110000	1100101	1100001	1110100	0100000	1101001	
PAD	1011011	1000001	0111**100**	**1011101**	**1011000**	**0101011**	**0011011**	**0110110**	
XOR	0101001	0100100	1001100	0111000	0111001	1011111	0111011	1011111	
ASCII	)	$	L	8	9	_	;	_	
ASCII	t	space	o	r	space	n	o	t	?
PLAIN	1110100	0100000	1101111	1110010	0100000	1101110	1101111	1110100	0111111
PAD	**0101110**	**1101100**	**0010101**	**0001101**	**1011011**	**0010111**	**0110110**	**0001010**	**1100110**
XOR	1011010	1001100	1111010	0111111	1111011	1111001	1011001	1111110	1011001
ASCII	Z	L	z	?	{	y	Y	~	Y

After completing the table we found the plaintext and identified the repeating section in the PAD section of the table.
Plaintext: "repeat it or not?"
Repeating section: "100 1011101 1011000 0101011 0011011 01101**"**