SECURITY

Assignment 2, Friday, September 22, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant

Assignment 1

(10 points) Imagine that you are given a fragment of ciphertext based on some (sufficiently long) English plaintext. Assume it's the output of either a substitution or a transposition cipher. How can you tell which cipher was used, without breaking the code?

Solution 1

A possible way could be to analyze the letter frequencies. If the letter frequencies are close to the frequencies in a language, then it's a transposition. Transposition doesn't change letter frequencies so they remain the same. Substitution changes letters, so the letter frequency wouldn't be almost the same as in language.

Assignment 2

(30 points) Consider the following ciphertext output of a mono-alphabetic substitution:

> Dko hxyyxr goxglo gbct jxb bcnr, kocldkt hknlabor, cra c spyyob dkcd rovob oras. Nd ns rx ycddob dx dkoy nj dko knwk lxbas glct dkonb wcyo xj dkbxros, sx lxrw cs dkot cbo lojd nr gocho. Dkot rovob cbo.

A. Find the matching plaintext by breaking the substitution cipher. Describe your method.
B. How many keys are possible for a substitution cipher using the (lowercase) English alphabet? Keys that leave some or all characters unchanged are also allowed.

Solution 2

A. *"The common people pray for rain, healthy children, and a summer that never ends. It is no matter to them if the high lords play their game of thrones, so long as they are left in peace. They never are"*

   In order to decipher the text, we searched for words that we possibly know. For example there is a loose c, by assuming that this has to be an 'a' to form a sentence we already discovered one substitution. By analyzing the frequencies of the characters, we found out that o has the most occurrences, so this should probably be 'e'. This is followed by 'd' for probably 't', Etc. By comparing this frequencies with the frequencies of letters used in the English alphabet we came up with the following substitution table:

B. $26! \approx 2^{88.4}$, or about 88 bits.

Assignment 3

(35 points) Consider the following ciphertext, which is the result of a columnar transposition cipher:
aeiycnwcmrneedvrt#irsgitaoear#peaos#rfsiegselnsh

A. Which two properties of transposition ciphers can be observed from the ciphertext?
B. What is the most likely key size? Explain your answer.
C. Find the plaintext. Explain and show your approach.
D. Sticking with the same key size, how could you make the scheme harder to break?

Solution 3

A. The following properties can be observed:
    a. That there is used a hashtag as padding to fill up empty spaces
    b. That the block size is 6
B. The column size is 6 which you can see by counting chars until the # signs. The total length of the ciphertext is 48 chars. You can see 3 # signs. The key length has to at least be 3 and a divisible of 48. 6 is the only solution where the # signs are constantly at the bottom of the columns (last row).
C. "*War is peace freedom is slavery ignorance is strength*"
When you break the text apart in blocks of 6 you will get : "*aeiycn wcmrne edvrt# irsgit aoear# peaos# rfsieg selnsh"*. At this point i reshuffled to get the hashes to the back and saw the word "war" on the first line. Then i reshuffled the columns bit more and got the following table as seen below resulting in the discovery of the sentence described above.
D. We can increase the difficulty by simply removing the padding element #. This helped to easily discover the key size which helped decrypting the cipher. If the padding would be done with a random char, it would be way harder to resolve the key size.

	Keysize: 8							
Column Size: 6	w	a	r	i	s	p	e	a
	c	e	f	r	e	e	d	o
	m	i	s	s	l	a	v	e
	r	y	i	g	n	o	r	a
	n	c	e	i	s	s	t	r
	e	n	g	t	h	#	#	#

Assignment 4

(25 points) Read about the Playfair cipher: https://en.wikipedia.org/wiki/Playfair_cipher. In this exercise, we will use the variant that uses 'I' for both 'I' and 'J'.

A. Using the key 'Albus Dumbledore', write down the 5x5 key grid.
B. Briefly explain how decryption works (i.e. how it differs from encryption)
C. Use the grid to decrypt the following ciphertext:
   CU XB TG PM BZ AI LK EG HM LQ MO XD TF PK GO CD DT RB QR IN FR RB CG MQ OR WM ZO OE OE EG IR QR QS MT MQ QI MB CH IQ

Solution 4

A. The 5 x 5 grid with the key ‘Albus Dumbledore’ will look like this:

A	L	B	U	S
D	M	E	O	R
C	F	G	H	I(I = J)
K	N	P	Q	T
V	W	X	Y	Z

B. Decryption works by comparing all pairs of letters in the grid. If the two letters aren’t in the same row or column we can make a rectangle and take the other edge of the rectangle on the same row for both values. If the letters are on the same row, we can take one letter on the left of both to decipher, because we take one letter on the right to encrypt we now have to go to the opposite direction. When both letters are in the same column, we take one letter above for both. In encryption one letter below is taken, so to decrypt we have to go in the opposite direction. If we apply this rules for all pairs of letters, this will result a sequence. In this sequence we need to remove the X between two of the same letters, because this is put in between to split same letters.

C. To decipher the text we will decipher all pairs of two characters step-by-step:

a. CU: forms a grid, we can replace them by the other corners, so this will be HA
b. XB: are in the same column, so we pick the items above each letter: PX
c. TG: forms a rectangle: PI
d. PM: rectangle NE
e. BZ: rectangle SX
f. AI: rectangle SC
g. LK: rectangle AN
h. EG: same column, so letters above BE
i. HM: rectangle FO
j. LQ: rectangle: UN
k. MO: same row, so letter to the right: DE
l. XD: rectangle VE
m. TF: rectangle: NI
n. PK: letters on the left: NT
o. GO: rectangle: HE
p. CD: same column, so item above: DA
q. DT: rectangle: RK
r. RB: rectangle ES
s. QR: rectangle TO
t. IN: rectangle: FT
u. FR: rectangle: IM
v. RB: rectangle: ES
w. CG: letter left IF
x. MQ: rectangle ON
y. OR: letter left EO
z. WM: item above: NL
aa. ZO: rectangle YR
bb. OE: letters left: EM
cc. OE: letters left: EM
dd. EG: letters above: BE
ee. IR: letters above: RS
ff. QR: rectangle: TO
gg. QS: rectangle: TU
hh. MT: rectangle: RN
ii. MQ: rectangle: ON
jj. QI: rectangle: TH
kk. MB: rectangle: EL
ll. CH: same row, so letters left: IG
mm. IQ: rectangle: HT

Message:

HAPXPINESXSCANBEFOUNDEVENINTHEDARKESTOFTIMESIFONEONLYREMEMBERST
OTURNONTHELIGHT

After removing the X that are used to split same letters, the following sentence appears:

HAPPINESS CAN BE FOUND EVEN IN THE DARKEST OF TIMES IF ONE ONLY
REMEMBERS TO TURN ON THE LIGHT