Cryptology

Homework nr 2

Simple substitution ciphers

Encryption/decryption process by means of different tools, especially – Cryptool 2.1 software. The empty tables are slightly oversized in order to have enough space to fill with proper letters in two rows, "like a snake". Before the entering this letters by pen, do the same job with pencil to avoid any corrections, corrections of previous corrections etc.

1.1. Cut out and build a cipher wheel as illustrated in figure below, but with an inner wheel that rotates, and use it to complete the following tasks. Instead of physical model, I encourage you to build a software "virtual" version.

(a) Encrypt the following plaintext using a rotation of 11 clockwise.

`A page of history is worth a volume of logic`

(b) Decrypt the following message, which was encrypted with a rotation of [ ] clockwise.
`AOLYLHYLUVZLJYLAZILAALYAOHUAOLZLJYLALZAOHALCLYFIVKFNBLZZLZ`

 (c) Decrypt the following message, which was encrypted by rotating 1 clockwise for the first letter, then 2 clockwise for the second letter, etc.
`XJHRFTNZHMZGAHIUETXZJNBWNUTRHEPOMDNBJMAUGORFAOIZOCC`

1.2. Decrypt each of the following Caesar encryptions by trying the various possible shifts until you obtain readable text.

(a) `LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH`   shift: [ ]

(b) UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB   shift: ☐

(c) BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX   shift: ☐

1.3. For this exercise, use the simple substitution table given below.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	C	J	A	X	U	F	B	Q	K	T	P	R	W	E	Z	H	V	L	I	G	Y	D	N	M	O

Simple substitution encryption table for exercise 1.3

(a) Encrypt the plaintext message The gold is hidden in the garden

(b) Make a decryption table, that is, make a table in which the ciphertext alphabet is in order from A to Z and the plaintext alphabet is mixed up.

(c) Use your decryption table from (b) to decrypt the following message.

IBXLX JVXIZ SLLDE VAQLL DEVAU QLB

1.4. Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them. Fill the frequency table and a list of the most common bigrams that appear in the ciphertext.

Because of the length of the plaintexts, tables will not be used. Please add only the pictures with Cryptool solutions as separate elements of the report.

(a) "A Piratical Treasure"

```
JNRZR BNIGI BJRGZ IZLQR OTDNJ GRIHT USDKR ZZWLG OIBTM NRGJN IJTZJ
LZISJ NRSBL QVRSI ORIQT QDEKJ JNRQW GLOFN IJTZX QLFQL WBIMJ ITQXT
HHTBL KUHQL JZKMM LZRNT OBIMI EURLW BLQZJ GKBJT QDIQS LWJNR OLGRI
EZJGK ZRBGS MJLDG IMNZT OIHRK MOSOT QHIJL QBRJN IJJNT ZFIZL WIZTO
MURZM RBTRZ ZKBNN LFRVR GIZFL KUHIM MRIGJ LJNRB GKHRT QJRUU RBJLW
JNRZI TULGI EZLUK JRUST QZLUK EURFT JNLKJ JNRXR S
```

The ciphertext contains ⬚ letters.

Letter																									
Freq. ↓																									

Bigram						
Freq. ↓						

(b) "A Botanical Code"

```
KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ BXRME MNKNG BURIX
KJRXR SBUER ISATB UIBNN RTBUM NBIGK EBIGR OCUBR GLUBN JBGRL SJGLN
GJBOR ISLRS BAFFO AZBUN RFAUS AGGBI NGLXM IAZRX RMNVL GEANG CJRUE
KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI NJAWB OBNNO ATBZJ KOBRC JKIRR
NGBUE BRINK XKBAF QBROA LNMRG MALUF BBG
```

The ciphertext contains ⬚ letters.

Letter																									
Freq. ↓																									

Bigram				
Freq. ↓				

(c) In order to make this one a bit more challenging, we have removed all occurrences of the word "the" from the plaintext.

"A Brilliant Detective"

```
GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ BOVUE
SIXCQ NQESX NGEUG AHZQA QHNSP CIPQA OIDLV JXGAK CGJCG SASUB FVQAV
CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG OGOVA XGNVU BAVKX
QZVQD LVJXQ EXCQO VKCQG AMVAX VWXCG OOBOX VZCSO SPPSN VAXUB DVVAX
QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA MVBSZ VOOSH VSAWX QHGMV GWVSX
CSXXC VBSNV ZVNVN SAWQZ ORVXJ CVOQE JCGUW NVA
```

The ciphertext contains ⬚ letters.

Letter																									
Freq. ↓																									

Bigram				
Freq. ↓				