

Soren Madsen
Dr. Houshmand
HW 1 - Applied Cryptography

Homework 1:

1. QZJRJ A ZJRS VX F XARMCO ARFUVAYMC MQ
PT: HERE THERE IS A STRONG TRADITION OF
XAMRI ATTICO FX F RTXNTA MO AZVX GMYA
STORY TELLING AS A RESULT OF THIS MOST
WIMWTS PRJ ARTGTICUMNX WNKTVP XUJFSJRX FCU
PEOPLE ARE TREMENDOUS PUBLIC SPEAKERS AND
AZBRJ VX FTGMYA CM HVAATC XWJTPZ
THERE IS ALMOST NO WRITTEN SPEECH

Top Letters: E T A O Translation: E T S L A ?
 CT Letters: J A X R A X R F } Used code to assist

2. See code submission.

3. Trigrams:

HAL: 5 Distances: (35, 25, 10, 50)
 KUX: 5 Distances: (15, 30, 10, 65)
 Suspected key length: 5
 Col 1: Possible Shift: A=H, T=X, E=J

Col 1:

6	6	0	0	7	2	5	9	0	0	7	3	8	0	3	3	0	3	0	9	0	3	4	1	5	2	2
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	
Shift: 19													Shift: 0													

Col 2:

5	8	9	2	0	1	2	5	1	0	0	1	1	0	3	0	8	1	3	3	7	1	1	8	6	0	0	3
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		
Shift: 14													Shift: 14														

Col 2:

6 0 3 5 0 2 0 7 0 2 3 18 7 0 6 4 0 0 4 1 6 10 0 0 6 7
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
t a e Shift: 7

Shift: 21

Col 3:

2 0 2 0 12 1 1 7 6 5 4 3 4 0 0 5 4 4 7 0 0 6 7 10 0 2
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
a e t Shift: 4

Shift: 18

Col 4:

0 1 3 4 3 4 1 0 7 8 12 0 4 3 0 0 0 6 2 2 3 4 4 1 4 11
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
t a e Shift: 17

Possible keywords:

14 19 7 4 17
0 21 18
D T H E R
A B S

Keyword: ~~OTHER~~ other

Plaintext: Borchhoff discovered his first geometry theorem...