Homework 3: Chapter 1 Questions

Mudit Vats
mpvats@syr.edu
4/29/2020

Table of Contents

Overview

This lab report presents observations and explanations for the exercises described in Professor Weissman's HW3 assignment.

NOTE: As part of this learning, I understood the value of relative prime / coprime and gcd as I went along. As such, several of my trials for the inverse could have been eliminated since those trial numbers are not relative prime / coprime. Good learning experience, however. I left the "extra work" in the homework to show my work even though some of those steps were not necessary.

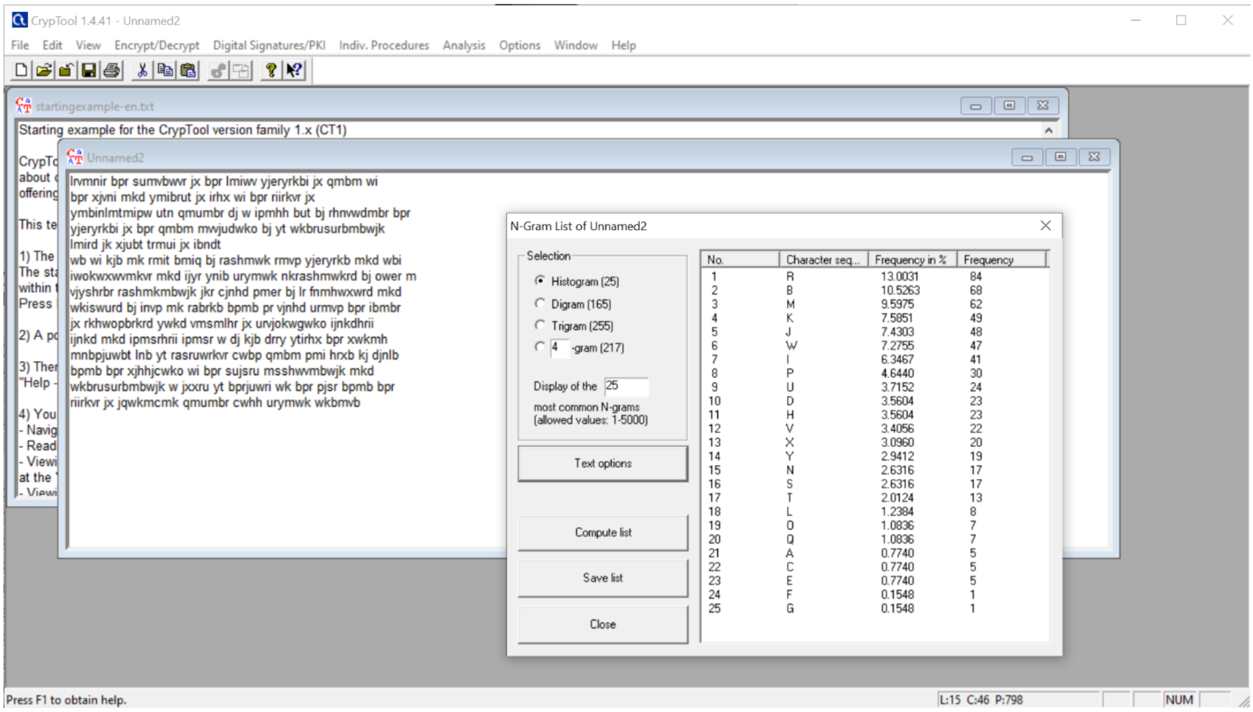
Problem 1.1

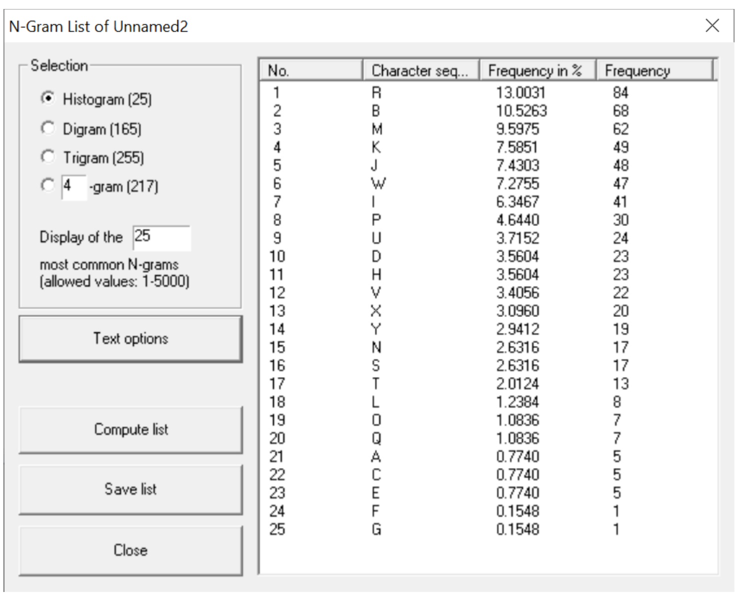
Decode the ciphertext:

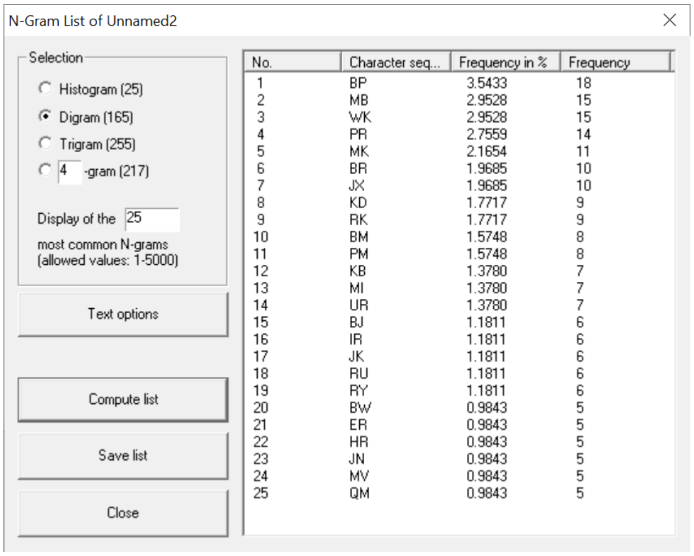
lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

Using CrypTool to get the frequency of the letters

Crypt tool screen shot and a larger view of the letter frequency shown. I also generation single, digram, trigram, 4-gram and 5-gram.


CrypTool 1.4.41 - Unnamed2
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Starting example for the CrypTool version family 1.x (CT1)
Unnamed2
lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
N-Gram List of Unnamed2
Press F1 to obtain help.
L:15 C:46 P:798
NUM


N-Gram List of Unnamed2
Selection
Histogram (25)
Digram (165)
Trigram (255)
4 -gram (217)
Display of the 25
most common N-grams
(allowed values: 1-5000)
Text options
Compute list
Save list
Close
No. Character seq... Frequency in % Frequency
1 R 13.0031 84
2 B 10.5263 68
3 M 9.5975 62
4 K 7.5851 49
5 J 7.4303 48
6 W 7.2755 47
7 I 6.3467 41
8 P 4.6440 30
9 U 3.7152 24
10 D 3.5604 23
11 H 3.5604 23
12 V 3.4056 22
13 X 3.0960 20
14 Y 2.9412 19
15 N 2.6316 17
16 S 2.6316 17
17 T 2.0124 13
18 L 1.2384 8
19 O 1.0836 7
20 Q 1.0836 7
21 A 0.7740 5
22 C 0.7740 5
23 E 0.7740 5
24 F 0.1548 1
25 G 0.1548 1



N-Gram List of Unnamed2

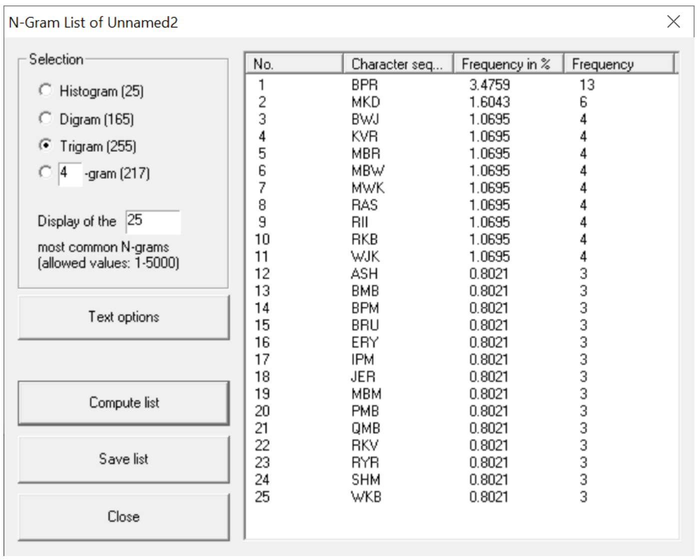
Selection

- Histogram (25)
- Digram (165) (selected)
- Trigram (255)
- 4 -gram (217)

Display of the 25 most common N-grams (allowed values: 1-5000)

Text options | Compute list | Save list | Close

No.	Character seq...	Frequency in %	Frequency
1	BP	3.5433	18
2	MB	2.9528	15
3	WK	2.9528	15
4	PR	2.7559	14
5	MK	2.1654	11
6	BR	1.9685	10
7	JX	1.9685	10
8	KD	1.7717	9
9	RK	1.7717	9
10	BM	1.5748	8
11	PM	1.5748	8
12	KB	1.3780	7
13	MI	1.3780	7
14	UR	1.3780	7
15	BJ	1.1811	6
16	IR	1.1811	6
17	JK	1.1811	6
18	RU	1.1811	6
19	RY	1.1811	6
20	BW	0.9843	5
21	ER	0.9843	5
22	HR	0.9843	5
23	JN	0.9843	5
24	MV	0.9843	5
25	QM	0.9843	5



N-Gram List of Unnamed2

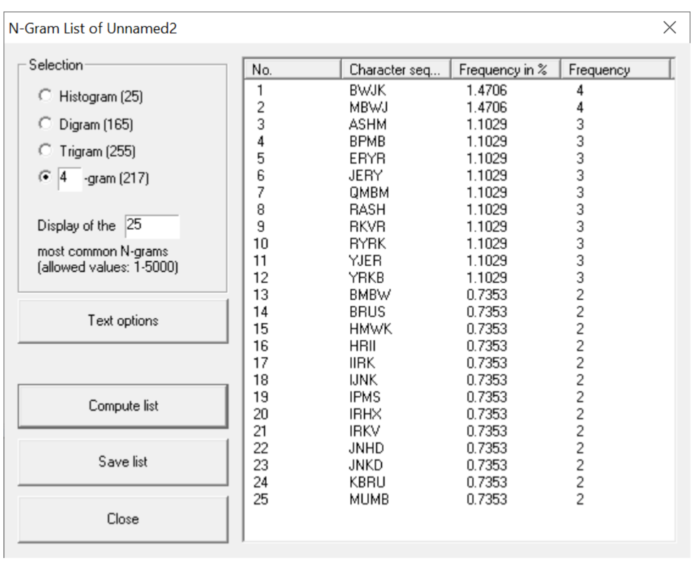
Selection

- Histogram (25)
- Digram (165)
- Trigram (255) (selected)
- 4 -gram (217)

Display of the 25 most common N-grams (allowed values: 1-5000)

Text options | Compute list | Save list | Close

No.	Character seq...	Frequency in %	Frequency
1	BPR	3.4759	13
2	MKD	1.6043	6
3	BWJ	1.0695	4
4	KVR	1.0695	4
5	MBR	1.0695	4
6	MBW	1.0695	4
7	MWK	1.0695	4
8	RAS	1.0695	4
9	RII	1.0695	4
10	RKB	1.0695	4
11	WJK	1.0695	4
12	ASH	0.8021	3
13	BMB	0.8021	3
14	BPM	0.8021	3
15	BRU	0.8021	3
16	ERY	0.8021	3
17	IPM	0.8021	3
18	JER	0.8021	3
19	MBM	0.8021	3
20	PMB	0.8021	3
21	QMB	0.8021	3
22	RKV	0.8021	3
23	RYR	0.8021	3
24	SHM	0.8021	3
25	WKB	0.8021	3



N-Gram List of Unnamed2

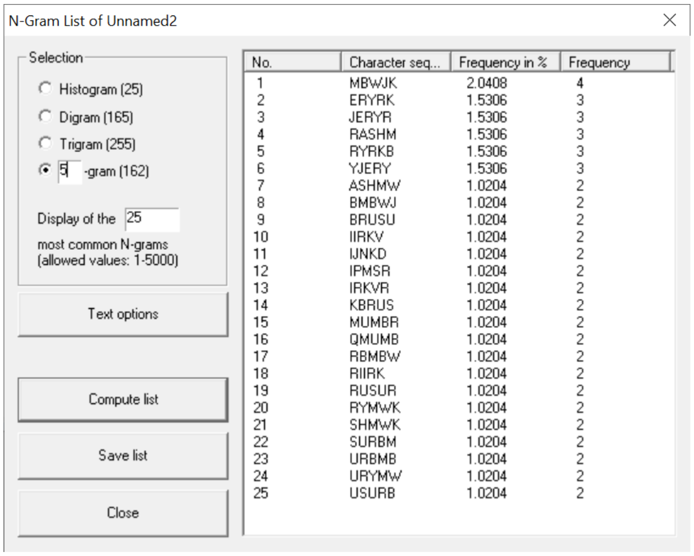
Selection

- Histogram (25)
- Digram (165)
- Trigram (255)
- 4 -gram (217) (selected)

Display of the 25 most common N-grams (allowed values: 1-5000)

Text options | Compute list | Save list | Close

No.	Character seq...	Frequency in %	Frequency
1	BWJK	1.4706	4
2	MBWJ	1.4706	4
3	ASHM	1.1029	3
4	BPMB	1.1029	3
5	ERYR	1.1029	3
6	JERY	1.1029	3
7	QMBM	1.1029	3
8	RASH	1.1029	3
9	RKVR	1.1029	3
10	RYRK	1.1029	3
11	YJER	1.1029	3
12	YRKB	1.1029	3
13	BMBW	0.7353	2
14	BRUS	0.7353	2
15	HMWK	0.7353	2
16	HRII	0.7353	2
17	IIRK	0.7353	2
18	IJNK	0.7353	2
19	IPMS	0.7353	2
20	IRHX	0.7353	2
21	IRKV	0.7353	2
22	JNHD	0.7353	2
23	JNKD	0.7353	2
24	KBRU	0.7353	2
25	MUMB	0.7353	2



No.	Character seq...	Frequency in %	Frequency
1	MBWJK	2.0408	4
2	ERYRK	1.5306	3
3	JERYR	1.5306	3
4	RASHM	1.5306	3
5	RYRKB	1.5306	3
6	YJERY	1.5306	3
7	ASHMW	1.0204	2
8	BMBWJ	1.0204	2
9	BRUSU	1.0204	2
10	IIRKV	1.0204	2
11	IJNKD	1.0204	2
12	IPMSR	1.0204	2
13	IRKVR	1.0204	2
14	KBRUS	1.0204	2
15	MUMBR	1.0204	2
16	QMUMB	1.0204	2
17	RBMBW	1.0204	2
18	RIIRK	1.0204	2
19	RUSUR	1.0204	2
20	RYMWK	1.0204	2
21	SHMWK	1.0204	2
22	SURBM	1.0204	2
23	URBMB	1.0204	2
24	URYMW	1.0204	2
25	USURB	1.0204	2

Letter frequency Tables

This is table 1.1 from Understanding Cryptography by Christof Paar.

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

I also used these frequency tables as to help with the >1-grams.

- http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/english-letter-frequencies/

Decoding

Using the Letter Frequency Tables I started with larger to smaller substitutions. Some substitution I did no use since there were frequency with the same values so it wasn't clear which substitution to use; this was the case with the four-gram.

```
mbwjk->ation
```

Irvmnir bpr sumvbwvr jx bpr Imiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbATION
Imird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m

vjyshrbr rashmkATION jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvATION mkd
wkbrusurbATION w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

bpr->the, mkd->and

lrvmnir THE sumvbwvr jx THE lmiwv yjeryrkbi jx qmbm wi
THE xjvni AND ymibrut jx irhx wi THE riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr THE
yjeryrkbi jx THE qmbm mvvjudwko bj yt wkbrusurbATION
lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb AND wbi
iwokwxwvmkvr AND ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkATION jkr cjnhd pmer bj lr fnmhwxwrd AND
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp THE ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd AND ipmsrhrii ipmsr w dj kjb drry ytirhx THE xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb THE xjhhjcwko wi THE sujsru msshwvATION AND
wkbrusurbATION w jxxru yt THEjuwri wk THE pjsr bpmb THE
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

Single Letter Replacements

Since some of letters were decodes, I went through and substituted single letter matches.

lEvAniE THE suAvTIvE Ox THE lAiIv yOeEyENTi Ox qATA Ii
THE xOvni AND yAiTEut Ox iEhx Ii THE EiiENvE Ox
yATinlAtAiHI utn qAuATE DO I iHAhh Tut TO EhnvIDATE THE
yOeEyENTi Ox THE qATA AvvOuDINo TO yt INTEusuETATION
lAiED ON xOuTt tEAui Ox iTnDt
IT Ii NOT AN EAit TAiq TO EashAIN EAvH yOeEyENT AND ITi
iIoNIxIvANvE AND iOyE yniT uEyAIN nNEashAINED TO oIeE A
vOyshETE EashANATION ONE cOnhD HAeE TO lE fnAhIxIED AND
INisIuED TO invH AN EaTENT THAT HE vOnhD uEAvH THE iTATE
Ox ENhIoHTENED yIND vAsAlhE Ox uEvOoNIgINo iOnNDhEii
iOnND AND iHAsEhEii iHAsE I DO NOT DEEy ytiEhx THE xINAh
AnTHOuITt lnT yt EasEuIENvE cITH qATA HAi hExT NO DOnlT
THAT THE xOhhOcINo Ii THE suOsEu AsshIvATION AND
INTEusuETATION I OxxEu yt THEOuIEi IN THE HOsE THAT THE
EiiENvE Ox OqINAcAN qAuATE cIhh uEyAIN INTAvT

Observations
At this point, I can pick out words to discover more matches. This is because the larger gram and single gram substitutions uncovered enough of the key that words that are only one or two letters off are easy to decipher.

ENhIoHTENED h->L, o->G
lEvAniE THE suAvTIvE Ox THE lAiIv yOeEyENTi Ox qATA Ii
THE xOvni AND yAiTEut Ox iELx Ii THE EiiENvE Ox
yATinlAtAiHI utn qAuATE DO I iHALL Tut TO ELnvIDATE THE
yOeEyENTi Ox THE qATA AvvOuDING TO yt INTEusuETATION
lAiED ON xOuTt tEAui Ox iTnDt
IT Ii NOT AN EAit TAiq TO EasLAIN EAvH yOeEyENT AND ITi
iIGNIxIvANvE AND iOyE yniT uEyAIN nNEasLAINED TO GIeE A
vOysLETE EasLANATION ONE cOnLD HAeE TO lE fnALIxIED AND
INisIuED TO invH AN EaTENT THAT HE vOnLD uEAvH THE iTATE
Ox ENLIGHTENED yIND vAsAlLE Ox uEvOGNIgING iOnNDLEii
iOnND AND iHAsELEii iHAsE I DO NOT DEEy ytiELx THE xINAL
AnTHOuITt lnT yt EasEuIENvE cITH qATA HAi LExT NO DOnlT
THAT THE xOLLOcING Ii THE suOsEu AssLIvATION AND
INTEusuETATION I OxxEu yt THEOuIEi IN THE HOsE THAT THE
EiiENvE Ox OqINAcAN qAuATE cILL uEyAIN INTAvT

xOLLOcING x->F, c->W
lEvAniE THE suAvTIvE OF THE lAiIv yOeEyENTi OF qATA Ii
THE FOvni AND yAiTEut OF iELF Ii THE EiiENvE OF
yATinlAtAiHI utn qAuATE DO I iHALL Tut TO ELnvIDATE THE
yOeEyENTi OF THE qATA AvvOuDING TO yt INTEusuETATION
lAiED ON FOuTt tEAui OF iTnDt
IT Ii NOT AN EAit TAiq TO EasLAIN EAvH yOeEyENT AND ITi
iIGNIFIvANvE AND iOyE yniT uEyAIN nNEasLAINED TO GIeE A
vOysLETE EasLANATION ONE WOnLD HAeE TO lE fnALIFIED AND
INisIuED TO invH AN EaTENT THAT HE vOnLD uEAvH THE iTATE
OF ENLIGHTENED yIND vAsAlLE OF uEvOGNIgING iOnNDLEii
iOnND AND iHAsELEii iHAsE I DO NOT DEEy ytiELF THE FINAL
AnTHOuITt lnT yt EasEuIENvE WITH qATA HAi LEFT NO DOnlT
THAT THE FOLLOWING Ii THE suOsEu AssLIvATION AND
INTEusuETATION I OFFEu yt THEOuIEi IN THE HOsE THAT THE
EiiENvE OF OqINAWAN qAuATE WILL uEyAIN INTAvT

iELF i->S
lEvAnSE THE suAvTIvE OF THE lASIv yOeEyENTS OF qATA IS
THE FOvnS AND yASTEut OF SELF IS THE ESSENvE OF
yATSnlAtASHI utn qAuATE DO I SHALL Tut TO ELnvIDATE THE
yOeEyENTS OF THE qATA AvvOuDING TO yt INTEusuETATION
lASED ON FOuTt tEAuS OF STnDt
IT IS NOT AN EASt TASq TO EasLAIN EAvH yOeEyENT AND ITS
SIGNIFIvANvE AND SOyE ynST uEyAIN nNEasLAINED TO GIeE A
vOysLETE EasLANATION ONE WOnLD HAeE TO lE fnALIFIED AND
INSsIuED TO SnvH AN EaTENT THAT HE vOnLD uEAvH THE STATE

OF ENLIGHTENED yIND vAsAlLE OF uEvOGNIgING SOnNDLESS
SOnND AND SHAsELESS SHAsE I DO NOT DEEy ytSELF THE FINAL
AnTHOuITt lnT yt EasEuIENvE WITH qATA HAS LEFT NO DOnlT
THAT THE FOLLOWING IS THE suOsEu AssLIvATION AND
INTEusuETATION I OFFEu yt THEOuIES IN THE HOsE THAT THE
ESSENvE OF OqINAWAN qAuATE WILL uEyAIN INTAvT

ESSENvE v->C

lECAnSE THE suACTICE OF THE lASIC yOeEyENTS OF qATA IS
THE FOCnS AND yASTEut OF SELF IS THE ESSENCE OF
yATSnlAtASHI utn qAuATE DO I SHALL Tut TO ELnCIDATE THE
yOeEyENTS OF THE qATA ACCOuDING TO yt INTEusuETATION
lASED ON FOuTt tEAuS OF STnDt
IT IS NOT AN EASt TASq TO EasLAIN EACH yOeEyENT AND ITS
SIGNIFICANCE AND SOyE ynST uEyAIN nNEasLAINED TO GIeE A
COysLETE EasLANATION ONE WOnLD HAeE TO lE fnALIFIED AND
INSsIuED TO SnCH AN EaTENT THAT HE COnLD uEACH THE STATE
OF ENLIGHTENED yIND CAsAlLE OF uECOGNIgING SOnNDLESS
SOnND AND SHAsELESS SHAsE I DO NOT DEEy ytSELF THE FINAL
AnTHOuITt lnT yt EasEuIENCE WITH qATA HAS LEFT NO DOnlT
THAT THE FOLLOWING IS THE suOsEu AssLICATION AND
INTEusuETATION I OFFEu yt THEOuIES IN THE HOsE THAT THE
ESSENCE OF OqINAWAN qAuATE WILL uEyAIN INTACT

FOCnS n->U

lECAUSE THE suACTICE OF THE lASIC yOeEyENTS OF qATA IS
THE FOCUS AND yASTEut OF SELF IS THE ESSENCE OF
yATSUlAtASHI utU qAuATE DO I SHALL Tut TO ELUCIDATE THE
yOeEyENTS OF THE qATA ACCOuDING TO yt INTEusuETATION
lASED ON FOuTt tEAuS OF STUDt
IT IS NOT AN EASt TASq TO EasLAIN EACH yOeEyENT AND ITS
SIGNIFICANCE AND SOyE yUST uEyAIN UNEasLAINED TO GIeE A
COysLETE EasLANATION ONE WOULD HAeE TO lE fUALIFIED AND
INSsIuED TO SUCH AN EaTENT THAT HE COULD uEACH THE STATE
OF ENLIGHTENED yIND CAsAlLE OF uECOGNIgING SOUNDLESS
SOUND AND SHAsELESS SHAsE I DO NOT DEEy ytSELF THE FINAL
AUTHOuITt lUT yt EasEuIENCE WITH qATA HAS LEFT NO DOUlT
THAT THE FOLLOWING IS THE suOsEu AssLICATION AND
INTEusuETATION I OFFEu yt THEOuIES IN THE HOsE THAT THE
ESSENCE OF OqINAWAN qAuATE WILL uEyAIN INTACT

lECAUSE l->B

BECAUSE THE suACTICE OF THE BASIC yOeEyENTS OF qATA IS
THE FOCUS AND yASTEut OF SELF IS THE ESSENCE OF
yATSUBAtASHI utU qAuATE DO I SHALL Tut TO ELUCIDATE THE
yOeEyENTS OF THE qATA ACCOuDING TO yt INTEusuETATION
BASED ON FOuTt tEAuS OF STUDt
IT IS NOT AN EASt TASq TO EasLAIN EACH yOeEyENT AND ITS

SIGNIFICANCE AND SOyE yUST uEyAIN UNEasLAINED TO GIeE A COysLETE EasLANATION ONE WOULD HAeE TO BE fUALIFIED AND INSsIuED TO SUCH AN EaTENT THAT HE COULD uEACH THE STATE OF ENLIGHTENED yIND CAsABLE OF uECOGNIgING SOUNDLESS SOUND AND SHAsELESS SHAsE I DO NOT DEEy ytSELF THE FINAL AUTHOuITt BUT yt EasEuIENCE WITH qATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE suOsEu AssLICATION AND INTEusuETATION I OFFEu yt THEOuIES IN THE HOsE THAT THE ESSENCE OF OqINAWAN qAuATE WILL uEyAIN INTACT

ACCOuDING u->R

BECAUSE THE sRACTICE OF THE BASIC yOeEyENTS OF qATA IS THE FOCUS AND yASTERt OF SELF IS THE ESSENCE OF yATSUBAtASHI RtU qARATE DO I SHALL TRt TO ELUCIDATE THE yOeEyENTS OF THE qATA ACCORDING TO yt INTERsRETATION BASED ON FORTt tEARS OF STUDt
IT IS NOT AN EASt TASq TO EasLAIN EACH yOeEyENT AND ITS SIGNIFICANCE AND SOyE yUST REyAIN UNEasLAINED TO GIeE A COysLETE EasLANATION ONE WOULD HAeE TO BE fUALIFIED AND INSsIRED TO SUCH AN EaTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED yIND CAsABLE OF RECOGNIgING SOUNDLESS SOUND AND SHAsELESS SHAsE I DO NOT DEEy ytSELF THE FINAL AUTHORITt BUT yt EasERIENCE WITH qATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE sROsER AssLICATION AND INTERsRETATION I OFFER yt THEORIES IN THE HOsE THAT THE ESSENCE OF OqINAWAN qARATE WILL REyAIN INTACT

EASt t->Y, RECOGNIgING g->Z, GIeE e->V, fUALIFIED f->Q

BECAUSE THE sRACTICE OF THE BASIC yOVEyENTS OF qATA IS THE FOCUS AND yASTERY OF SELF IS THE ESSENCE OF yATSUBAYASHI RYU qARATE DO I SHALL TRY TO ELUCIDATE THE yOVEyENTS OF THE qATA ACCORDING TO yY INTERsRETATION BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASq TO EasLAIN EACH yOVEyENT AND ITS SIGNIFICANCE AND SOyE yUST REyAIN UNEasLAINED TO GIVE A COysLETE EasLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSsIRED TO SUCH AN EaTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED yIND CAsABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAsELESS SHAsE I DO NOT DEEy yYSELF THE FINAL AUTHORITY BUT yY EasERIENCE WITH qATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE sROsER AssLICATION AND INTERsRETATION I OFFER yY THEORIES IN THE HOsE THAT THE ESSENCE OF OqINAWAN qARATE WILL REyAIN INTACT

sRACTICE s->P, yASTERY y->M

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF qATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU qARATE DO I SHALL TRY TO ELUCIDATE THE

MOVEMENTS OF THE qATA ACCORDING TO MY INTERPRETATION
BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASq TO EaPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEaPLAINED TO GIVE A COMPLETE EaPLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EaTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EaPERIENCE WITH qATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OqINAWAN qARATE WILL REMAIN INTACT

Final Decode - TASq q->K, EaPLAIN a->X

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION
BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A COMPLETE EXPLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

Final Key

This is the final key.

Cipher	Plain
A	X
B	T
C	W
D	D
E	V
F	Q
G	Z
H	L
I	S
J	O
K	N
L	B
M	A

N	U
O	G
P	H
Q	K
R	E
S	P
T	Y
U	R
V	C
W	I
X	F
Y	M
Z	J

Answers

1. The frequency was computed using CrypTool shown above.
2. Final decode text is –

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A COMPLETE EXPLANATION ONE WOULD HAVE TO BE QUALIFIED AND INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT THAT THE FOLLOWING IS THE PROPER APPLICATION AND INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

3. I believe Shoshin Nagamine wrote the book The Essance of Okinawan Karate-Do. While the passage above doesn't explicitly come up, this is the first link when searching for the decrypted text.

https://www.amazon.com/Essence-Okinawan-Karate-Do-Shoshin-Nagamine/dp/0804821100

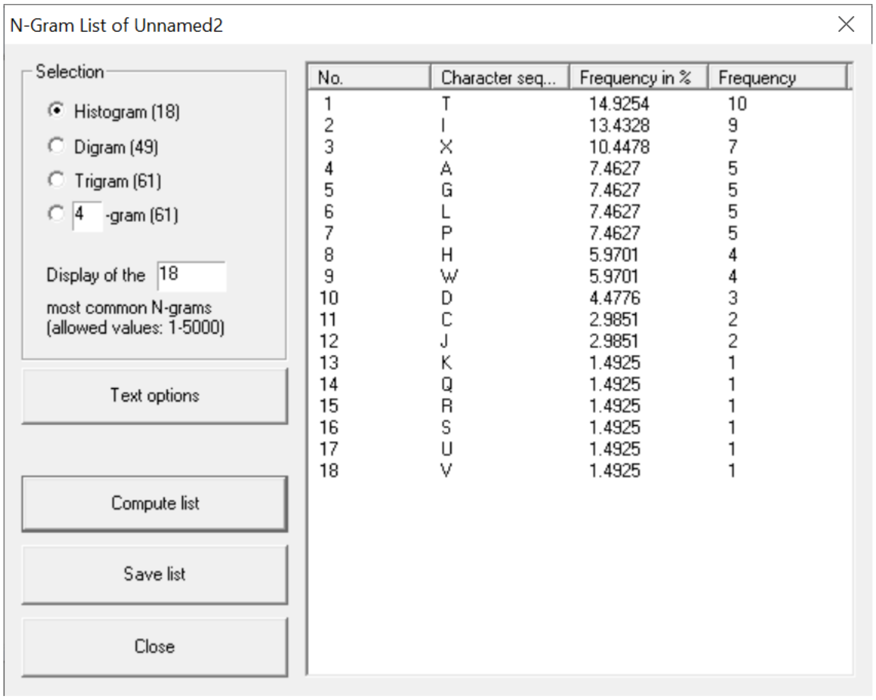
Problem 1.2

Decode the ciphertext which was encoded with a shift cipher.

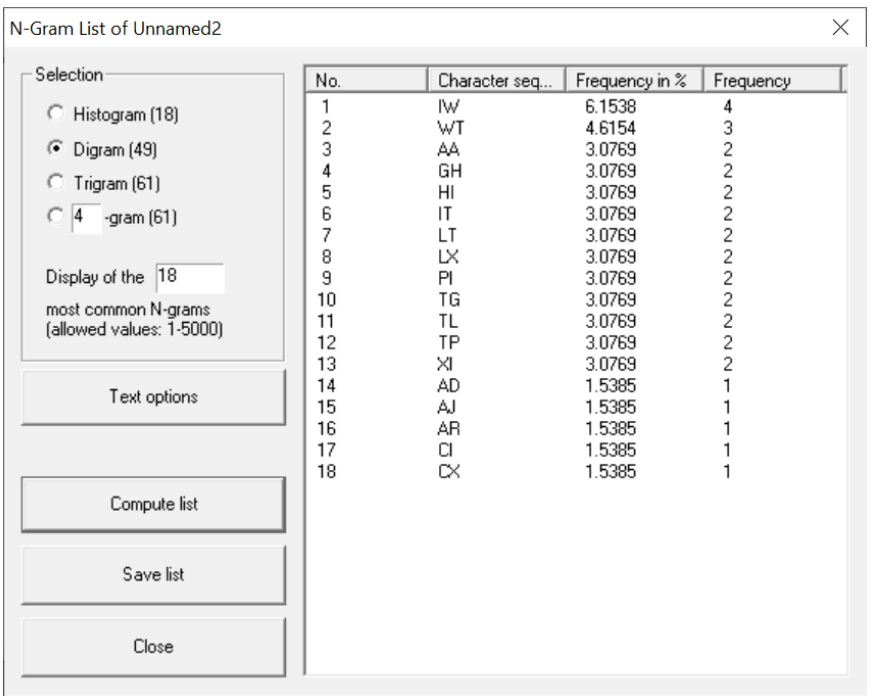
xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpit

ghlxiwiwtxgqadds

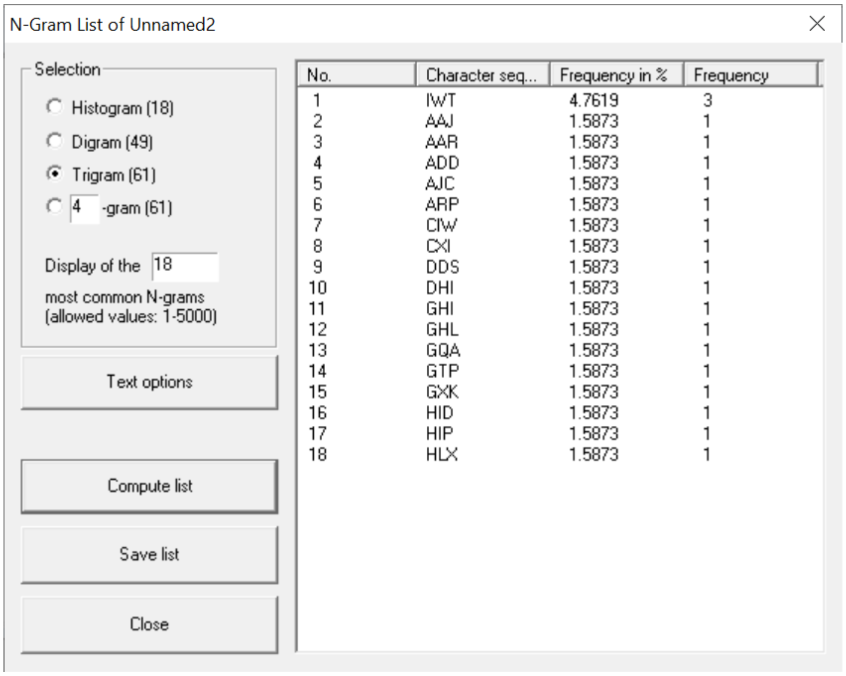
Using letter frequency and CrytpTool, we see the following letter frequencies tables –



No.	Character seq...	Frequency in %	Frequency
1	T	14.9254	10
2	I	13.4328	9
3	X	10.4478	7
4	A	7.4627	5
5	G	7.4627	5
6	L	7.4627	5
7	P	7.4627	5
8	H	5.9701	4
9	W	5.9701	4
10	D	4.4776	3
11	C	2.9851	2
12	J	2.9851	2
13	K	1.4925	1
14	Q	1.4925	1
15	R	1.4925	1
16	S	1.4925	1
17	U	1.4925	1
18	V	1.4925	1



No.	Character seq...	Frequency in %	Frequency
1	IW	6.1538	4
2	WT	4.6154	3
3	AA	3.0769	2
4	GH	3.0769	2
5	HI	3.0769	2
6	IT	3.0769	2
7	LT	3.0769	2
8	LX	3.0769	2
9	PI	3.0769	2
10	TG	3.0769	2
11	TL	3.0769	2
12	TP	3.0769	2
13	XI	3.0769	2
14	AD	1.5385	1
15	AJ	1.5385	1
16	AR	1.5385	1
17	CI	1.5385	1
18	CX	1.5385	1



No.	Character seq...	Frequency in %	Frequency
1	IWT	4.7619	3
2	AAJ	1.5873	1
3	AAR	1.5873	1
4	ADD	1.5873	1
5	AJC	1.5873	1
6	ARP	1.5873	1
7	CIW	1.5873	1
8	CXI	1.5873	1
9	DDS	1.5873	1
10	DHI	1.5873	1
11	GHI	1.5873	1
12	GHL	1.5873	1
13	GQA	1.5873	1
14	GTP	1.5873	1
15	GXK	1.5873	1
16	HID	1.5873	1
17	HIP	1.5873	1
18	HLX	1.5873	1

Using the frequency table and the English letter frequencies

iwt->the

xultpaajcxitltlxaarpjhtTHEgxktghidhipxcTHEvgtpilpitghlxiwTHExgqadds

letter substitutions

xulEpaajcxTElElxaarpjhETHEgxkEghTdhTpxcTHEvgEpTlpTEghlxTHTHExgqadds

Finding the Key

Just using the trigram and three letters, we see this mapping –

Chiper	Xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds
Plain Substit	xulEpaajcxTElElxaarpjhETHEgxkEghTdhTpxcTHEvgEpTlpTEghlxTHTHExgqadds

If we look at the t->E, i->T, w->H, we can see that the substituted text is 15 characters shifted for all three characters. So, the formula is –

- ek(x) congruent to x + 15 mod 26
- dk(y) congruent to y - 15 mod 26

Applying these equations, we get a key of –

Plain	Cipher
A	P
B	Q
C	R
D	S
E	T

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

Decoding the Cipher text

xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds

IFWEALLUNITEWEWILLCAUSETHERIVERSTOSTAINTHEGREATWATERSWITHTHEIRBLOOD

"IF WE ALL UNITE WE WILL CAUSE THE RIVERS TO STAIN THE GREAT WATERS WITH THEIR BLOOD"

Answers

1. I identified three letters "THE" using the trigram. Knowing that it was a shift cipher, I calculated the deltas between the cipher text and substituted text. From there it was easy to get the key (shown above).
2. After Googling, it looks like Tecumseh wrote the message: https://en.wikipedia.org/wiki/Tecumseh

Problem 1.4

Passwords and key sizes.

1. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?

    a. 128 ^ 8 since there are 128 possible characters per password letter. Since each letter is independent, this is an exponential computation, so it become 128 * 128 * 128 * 128 * 128 * 128 * 128 * 128 which is 128 ^ 8.

2. What is the corresponding key length in bits?
    a. 7 bits per character * 8 characters = 56 bits.

3. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?
    a. 26 letters would take 5 bits to represent, so 5 bits * 8 characters would be 40 bits.

4. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of
    a. 7-bit characters? 128 bit key length / 7 bits per character => 18.285 = ~19 characters.
    b. 26 lowercase letters from the alphabet? 128 bit key length / 5 bits per character => 25.6 = ~26 characters.

Problem 1.5

Compute the results.

1. $15 \cdot 29 \bmod 13$
    a. 435 mod 13
    b. 6 mod 13

2. $2 \cdot 29 \bmod 13$
    a. 58 mod 13
    b. 6 mod 13

3. $2 \cdot 3 \bmod 13$
    a. 6 mod 13

4. $-11 \cdot 3 \bmod 13$
    a. -33 mod 13
    b. -7 mod 13
    c. We add the modulus 13 to -7, since we can't have a negative number.
        i. Alternatively, we could add modulus first to make -11 positive, which would be 2 * 3 mod 13. The result is the same 6 mod 13.
    d. 6 mod 13

Relationship between different parts of the problem.

- Equivalency tables can be used to reduce the problem. All of the problems are modulus 13, so the digits before the mod are all part of "some" equivalency class. Each digit in this equivalency class differs by the next digit by 13 (the modulus). Since this is modulus 13, there are 13 equivalency classes.
- These numbers are -11, 2, 3, 15, 29.
- If we know the equivalency class for a number, we can reduce the problem to the smallest number >0, thus making the problem much easier.
- Looking at the numbers, we can easily pick out these patterns –
    - {… -11, 2, 15, 28, … } ← One equivalency class.
    - { … 3, 16, 29 … } ← Another equivalency class.
    - There are more equivalency classes, but the numbers we're interested in all fall into these two tables, so we stop here.

Using Equivalency Tables

1. If we reconsider 15 * 29 mod 13, we can use equivalency classes to reduce the problem. So, for 15 we can substitute 2. For 29, we can substitute 3. Thus, we have 2 * 3 mod 13, which yields the same answer: 6 mod 13.
2. If we reconsider 2 * 29 mod 13, we can substitute 29 with 3 and get 2 *3 mod 13, which yields the same answer: 6 mod 13.
3. The third problem is already reduced as much as it can be, so no substitution is performed. The problem and final result is the same: 2 * 3 mod 13, which is 6 mod 13.
4. For the fourth problem, -11 * 3 mod 13, we can do the same. So, -11 can be substituted with 2, so we get 2 * 3 mod 13, which once again, yields 6 mod 13.

Bottom-line, we can use equivalency classes to substitute larger numbers in order to simplify the problem. This is valuable since it's less computationally intensive from a computer's perspective and a human's perspective!

Problem 1.6

The basic steps I used to solve these problems are:

1. Transform the division problem into a multiplication problem.
2. Find the modular multiplicative inverse using the property a * a^-1 ≡ 1 mod m.
3. Substitute the inverse into the multiplication problem from step #1.

1/5 mod 13

Steps below.

1. Transform the problem:
    a. 1 / 5 mod 13 transforms to 1 * INVERSE mod 13
2. Find the inverse:
    a. 5 * ? mod 13 ≡ 1 mod 13
    b. Trying 1 yields 5 * 1 mod 13 = 5. Nope.
    c. Trying 2 yields 5 * 2 mod 13 = 10. Nope.
    d. Trying 3 yields 5 * 3 mod 13 = 2. Nope.
    e. Trying 4 yields 5 * 4 mod 13 = 7 Nope.

f. Trying 5 yields 5 * 5 mod 13 = 12 Nope.
g. Trying 6 yields 5 * 6 mod 13 = 4 Nope.
h. Trying 7 yields 5 * 7 mod 13 = 9 Nope.
i. Trying 8 yields 5 * 8 mod 13 = 1 YES since 1 = 1 mod 13.
j. Inverse is 8.

3. Substitute:
    a. 1 / 5 mod 13 transforms to 1 * INVERSE mod 13
    b. 1 * 8 mod 13
    c. 8 mod 13 => 8.

1/5 mod 7

Steps below.

1. Transform the problem:
    a. 1 / 5 mod 7 transforms to 1 * INVERSE mod 7
2. Find the inverse:
    a. 5 * ? mod 7 ≡ 1 mod 7
    b. Trying 1 yields 5 * 1 mod 7 = 5. Nope.
    c. Trying 2 yields 5 * 2 mod 7 = 3. Nope.
    d. Trying 3 yields 5 * 3 mod 7 = 1. YES since 1 = 1 mod 13.
    e. Inverse is 3.
3. Substitute:
    a. 1 / 5 mod 7 transforms to 1 * INVERSE mod 7
    b. 1 * 3 mod 7
    c. 3 mod 7 => 3.

3 · 2/5 mod 7

Steps below.

1. Transform the problem:
    a. 3 * 2 / 5 mod 7 transforms to 3 * 2 * INVERSE mod 7
2. Find the inverse:
    a. 5 * ? mod 7 ≡ 1 mod 7
    b. From the previous problem we know that the inverse is 3.
    c. Inverse is 3.
3. Substitute:
    a. 3 * 2 / 5 mod 7 transforms to 3 * 2 * INVERSE mod 7
    b. 3 * 2 * 3 mod 7
    c. 18 mod 7 => 4.

Problem 1.7

This section describes / shows each step performed per the exercise in Step 1.

1. Construct the multiplication table for Z4.

*	0	1	2	3
0	0	0	0	0
1	0	1	2	4
2	0	2	0	2
3	0	3	2	1

2. Construct the addition and multiplication tables for Z5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. Construct the addition and multiplication tables for Z6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2

4	4	5	0	1	2	3
5	5	0	1	2	3	4

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. There are elements in Z4 and Z6 without a multiplicative inverse.

Which elements are these?
For Z4

1. Elements in Z4 that HAVE a multiplicative inverse are gcd(a, 4) are { 1, 3 }.
2. Because of this, the elements that DO NOT HAVE a multiplicative inverse for Z4 are { 0, 2 }.

For Z6

1. Elements in Z6 that HAVE a multiplicative inverse are gcd(a, 6) are { 1, 5 }.
2. Because of this, the elements that DO NOT HAVE a multiplicative inverse for Z6 are { 0, 2, 3, 4 }.

Why does a multiplicative inverse exist for all nonzero elements in Z5?
Elements in Z5 that have a multiplicative inverse are gcd(a, 5) are { 1, 2, 3, 4 }. Five is prime, so fundamentally nothing can divide into it except for 1. So in terms of GCD, there is no GCD (other then 1) that can divide into 5, so all number <5 are relative prime.

Problem 1.8

Calculate modular multiplicative inverse of 5.

For Z11

1. 5 * 5^-1 mod 11 = 1 mod 11
2. 5 * INVERSE mod 11 = 1 mod 11
    a. Try 1, 5 * 1 mod 11 = 5. Nope.
    b. Try 2, 5 * 2 mod 11 = 10. Nope.
    c. Try 3, 5 * 3 mod 11 = 4. Nope.
    d. Try 4, 5 * 4 mod 11 = 9. Nope.
    e. Try 5, 5 * 5 mod 11 = 14. Nope.
    f. Try 6, 5 * 6 mod 11 = 8. Nope.
    g. Try 7, 5 * 7 mod 11 = 2. Nope.
    h. Try 8, 5 * 8 mod 11 = 7. Nope.
    i. Try 9, 5 * 9 mod 11 = 1 mod 11. YES.
3. The modular inverse for 5 mod 11 is 9 mod 11.

For Z12

1. 5 * 5^-1 mod 12 = 1 mod 12
2. Calculating gcd(a, 12) = { 1, 5, 7, 11 }
    a. As mentioned later, I learned as I went, so for Z12 and Z13 we calculate gcd to narrow down the range of the relative prices that may fit.
3. 5 * INVERSE mod 11 = 1 mod 11
    a. Try 1, 5 * 1 mod 12 = 5. Nope.
    b. Try 5, 5 * 5 mod 12 = 1. Yes.
4. The modular inverse for 5 mod 12 is 5 mod 11.

For Z13

1. 5 * 5^-1 mod 13 = 1 mod 13
2. Calculating gcd(a, 13) = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 }
    a. This is interesting since 13 is prime, so all digits <13 are relatively prime. So, try them all!
3. 5 * INVERSE mod 13 = 1 mod 13
    a. Try 1, 5 * 1 mod 13 = 5. Nope.
    b. Try 2, 5 * 2 mod 13 = 10. Nope.
    c. Try 3, 5 * 2 mod 13 = 2. Nope.
    d. Try 4, 5 * 4 mod 13 = 7. Nope.
    e. Try 5, 5 * 5 mod 13 = 12. Nope.
    f. Try 6, 5 * 6 mod 13 = 4. Nope.
    g. Try 7, 5 * 7 mod 13 = 9. Nope.
    h. Try 8, 5 * 8 mod 13 = 1. Yes.
4. The modular inverse for 5 mod 14 is 8 mod 13.

Problem 1.9

Compute x as far as possible without a calculator. Problems 1-3 were straight forward. The key to problem 3 and 4 were creating the equivalency tables which can then be used to reduce the problem.

1. x = 3^2 mod 13

a. x = 9 mod 13

2. x = 7^2 mod 13
   a. x = 49 mod 13
   b. x = 10 mod 13

3. x = 3^10 mod 13
   a. Equiv Table 0, 13, 26, 39, 52, 65, 78, 91…
   b. Equiv Table 1, 14, 27, 40, 53, 66, 79, 92…
   c. Equiv Table 2, 15, 28, 41, 54, 67, 80, 93…
   d. Equiv Table 3, 16, 29, 42, 55, 68, 81, 94…
   e. x = 3^4 * 3^4 * 3^2 mod 13
   f. x = 81 * 81 * 9 mod 13
   g. Using Equivalency Table d and replacing 81 with 3, we have: x = 3 * 3 * 9 mod 13
   h. x = 81 mod 13
   i. x = 3 mod 13

4. x = 7^100 mod 13
   a. Equiv Table 0, 13, 26, 39, 52, 65, 78, 91…
   b. Equiv Table 1, 14, 27, 40, 53, 66, 79, 92…
   c. Equiv Table 2, 15, 28, 41, 54, 67, 80, 93…
   d. Equiv Table 3, 16, 29, 42, 55, 68, 81, 94…
   e. Equiv Table 4, 17, 30, 43, 56, 69, 82, 95…
   f. Equiv Table 5, 18, 31, 44, 57, 70, 83, 96…
   g. Equiv Table 6, 19, 32, 45, 58, 71, 84, 97…
   h. Equiv Table 7, 20, 33, 46, 59, 72, 85, 98…
   i. Equiv Table 8, 21, 34, 47, 60, 73, 86, 99…
   j. Equiv Table 9, 22, 35, 48, 61, 74, 87, 100…
   k. Equiv Table 10, 23, 36, 49, 62, 75, 88, 101…
   l. x = (7^2)^50 mod 13
   m. Using Equivalency Table k and replacing 49 (7^2) with 10, we have: x = 10^50 mod 13.
   n. x = (10^2)^25 mod 13
   o. Using Equivalency Table j and replacing 100 (10^2) with 9, we have: x = 9^25 mod 13.
   p. x = (9^2)^12 * 9 mod 13.
   q. Using Equivalency Table d and replacing 81 (9^2) with 3, we have: x = 3^12 * 9 mod 13.
   r. x = (3^4)^3 * 9 mod 13.
   s. Using Equivalency Table d and replacing 81 (3^4) with 3, we have: x = 3^3 * 9 mod 13.
   t. x = (3^3) * (3^2) mod 13.
   u. x = (3^4) * 3 mod 13.
   v. Using Equivalency Table d and replacing 81 (3^4) with 3, we have: x = 3 * 3 mod 13.

w. x = 9 mod 13.

5. 7^x = 11 mod 13
    a. Trying 1, yields 7 mod 13 = 7 mod 13. Nope.
    b. Trying 2, yields 49 mod 13 = 10 mod 13. Nope.
    c. Trying 3, yields 343 mod 13 = 5 mod 13. Nope.
    d. Trying 4, yields 2401 mod 13 = 9 mod 13. Nope.
    e. Trying 5, yields 16807 mod 13 = 11 mod 13. Yes, this works!
    f. x = 5

Problem 1.11

Decrypt using Affine Cipher.

Decrypt the text:

Text: falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

Formulas

k = (a, b)

ek(x) = y

= a * x + b mod 26

dk(y) = x

= a^1 * (y - b) mod 26

Get Modular Multiplicative Inverse

Key to decryption is getting the modular multiplicative inverse.

k = (a=7, b=22)

ek(x) = y

= 7 * x + 22 mod 26

dk(y) = x

= 7^-1 * (y - 22) mod 26

1. Get the inverse:
    a. 7 * 7^-1 mod 26 = 1 mod 26
    b. 7 * INVERSE mod 26 = 1 mod 26

i. Try 1, 7 * 1 mod 26 = 7. Nope.
ii. Try 2, 7 * 2 mod 26 = 14. Nope.
iii. Try 3, 7 * 3 mod 26 = 21. Nope.
iv. Try 4, 7 * 4 mod 26 = 2. Nope.
v. Try 5, 7 * 5 mod 26 = 9. Nope.
vi. Try 6, 7 * 6 mod 26 = 16. Nope.
vii. Try 7, 7 * 7 mod 26 = 23. Nope.
viii. Try 8, 7 * 8 mod 26 = 4. Nope.
ix. Try 9, 7 * 9 mod 26 = 11. Nope.
x. Try 10, 7 * 10 mod 26 = 18. Nope.
xi. Try 11, 7 * 11 mod 26 = 25. Nope.
xii. Try 12, 7 * 12 mod 26 = 6. Nope.
xiii. Try 13, 7 * 13 mod 26 = 13. Nope.
xiv. Try 14, 7 * 14 mod 26 = 20. Nope.
xv. Try 15, 7 * 15 mod 26 = 1 mod 26. YES.

2. Decryption formula:
    a. dk(y) = x
    b. = 7^-1 * (y - 22) mod 26
    c. = INVERSE * (y - 22) mod 26
    d. = 15 * (y - 22) mod 26

We use the formula in 2d to decrypt encrypted letter to plain text letter. Please note, as mentioned above, the key was to get the inverse. The inverse is 15, so knowing that, using the formula to decrypt the cipher letters is simple (although I manually calculated each letter in the key!).

	Cipher	Plain
0	A	I
1	B	X
2	C	P
3	D	B
4	E	Q
5	F	F
6	G	U
7	H	J
8	I	Y
9	J	N
10	K	C
11	L	R
12	M	G
13	N	V
14	O	K
15	P	Z
16	Q	O
17	R	D

18	S	S
19	T	H
20	U	W
21	V	L
22	W	A
23	X	P
24	Y	E
25	Z	T

Applying the key above:

Cipher: falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

Decode: firstthesentenceandthentheevidencesaidthequeen

Final: "first the sentence and then the evidence said the queen"

Who wrote the line?

According to Google, this is from Alice's Adventures Under Ground – Chapter 4, by Lewis Carroll.

http://www.alice-in-wonderland.net/resources/chapters-script/alices-adventures-under-ground/chapter-4/

Problem 1.12

Questions below.

1. What are the encryption and decryption equations for the cipher?

k = (a, b)

ek(x) = y

= a * x + b mod 30

dk(y) = x

= a^-1 * (y - b) mod 30

2. How large is the key space of the affine cipher for this alphabet?

Key is (a, b), with the restriction that gcd(a, 30) = 1 (inverse must exist). 30 is the set of key values (m). a must be in relative prime/co-prime with 30, so those values for a are: { 1, 7, 11, 13, 17, 19, 23, 29 } = 8 possible values for inverse.

Now, we have 8 values for a and 30 for m. So, we have 8 * 30 => 240 possible keys.

NOTE: As part of this learning, I just now understood the value of relative prime / coprime and gcd. As such, several of my trials for the inverse could have been eliminated since those trial numbers are not relative prime / coprime. Good learning experience, however. I left the "extra work" in the homework to show my work even though some of those steps were not necessary.

3. The following ciphertext was encrypted using the key (a = 17,b = 1). What is the corresponding plaintext?

dk(y) = x

= 17^1 * (y - b) mod 30

= INVERSE * (y - 1) mod 30

1. Get the inverse:
    a. 17 * 17^-1 mod 30 = 1 mod 30
    b. 17 * INVERSE mod 30 = 1 mod 30
        i. Try 1, 17 * 1 mod 30 = 17. Nope.
        ii. Try 2, 17 * 2 mod 30 = 4. Nope.
        iii. Try 3, 17 * 3 mod 30 = 21. Nope.
        iv. Try 4, 17 * 4 mod 30 = 8. Nope.
        v. Try 5, 17 * 5 mod 30 = 25. Nope.
        vi. Try 6, 17 * 6 mod 30 = 12. Nope.
        vii. Try 7, 17 * 7 mod 30 = 29. Nope.
        viii. Try 8, 17 * 8 mod 30 = 17. Nope.
        ix. Try 9, 17 * 9 mod 30 = 3. Nope.
        x. Try 10, 17 * 10 mod 30 = 20. Nope.
        xi. Try 11, 17 * 11 mod 30 = 7. Nope.
        xii. Try 12, 17 * 12 mod 30 = 24. Nope.
        xiii. Try 13, 17 * 13 mod 30 = 11. Nope.
        xiv. Try 14, 17 * 14 mod 30 = 28. Nope.
        xv. Try 15, 17 * 15 mod 30 = 15. Nope.
        xvi. Try 16, 17 * 16 mod 30 = 2. Nope.
        xvii. Try 17, 17 * 17 mod 30 = 19. Nope.
        xviii. Try 18, 17 * 18 mod 30 = 6. Nope.
        xix. Try 19, 17 * 19 mod 30 = 23. Nope.
        xx. Try 20, 17 * 20 mod 30 = 10. Nope.
        xxi. Try 21, 17 * 21 mod 30 = 17. Nope.
        xxii. Try 22, 17 * 22 mod 30 = 14. Nope.
        xxiii. Try 23, 17 * 23 mod 30 = 1 mod 30. YES!!!
2. Decryption formula:

a. dk(y) = x
b. = 17^-1 * (y - 1) mod 30
c. = INVERSE * (y - 1) mod 30
d. = 23 * (y - 1) mod 30

Using the formula in 2d and substituting the letter to integer mapping, we can decrypt the text:

Cipher:	a	u	ß	w	ß
Mapping:	26	20	29	22	29
Decrypt:	5	17	14	3	14
Plain:	F	R	O	D	O

3. From which village does the plaintext come?

Frodo comes from Bag End / The Shire.

https://en.wikipedia.org/wiki/Frodo_Baggins