Carl Cortez

CIS 628

Lab 2

1.1

Part 1 - Going off of the relative letter frequency, I tried using E as the most common letter. T just happened to follow that up as the second most used letter. A worked out nicely as the third most used letter. From there, I did a mix of guess and check.

R	84	1	E
B	68	0	T
M	62	0	A
K	49	0	N
J	48	0	O
W	47	0	I
I	41	0	S
P	30	0	H
U	24	0	R
D	23	0	D
H	23	0	
V	22	0	
X	20	0	F
Y	19	0	
N	17	0	
S	17	0	
T	13	0	Y
L	8	0	
O	7	0	
Q	7	0	
A	5	0	
C	5	0	
E	5	0	
F	1	0	
G	1	0	
Z	0	0	

Excel sheet found here.

Part 2

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

Part 3

Shoshin Nagamine wrote this text.

1.2

A-5 L J-2 U S-1 D
B- M K-1 V T-10 E ← most frequent!
C 1 N L-5 W U-1 F
D-2 O M- X V-1 G
E P N Y W-4 H
F Q O Z X-6 I
G-5 R P-5 A Y- J
H-4 S Q-1 B Z K
I-9 T R-1 C

1 letter

1) Only the most frequent letter had to be identified by frequency count. Luckily, the most frequent letter used ended up being in place of 'e.'

Cleartext is:

If we all unite we will cause the rivers to stain the great waters with their blood.

2. Tecumseh wrote this message.

1.4

Task 1

8 spots with 128 options for each spot.
128^8 is the key space.

Task 2

8 letters * 7 bits = 56 bits for the key space.

Task 3

With 26 options for 8 spots, our key space is 26^8.
In bits, 2 to some power will equal 26^8. Since 26 isn't a power of 2, using logs will be needed. See below for work.

task 3 work

$26^8 = 2^?$

$\log_2(26^8) = 8\cdot\log_2(26) \approx 37.6$ bits

=

task 4

A) $128^{\text{spots}} = (2^7)^{\text{spots}} = 2^{7\cdot\text{spots}} = 2^{128}$

#of spots = $128/7 \approx 18.3$ spots/characters

B) 26 letters

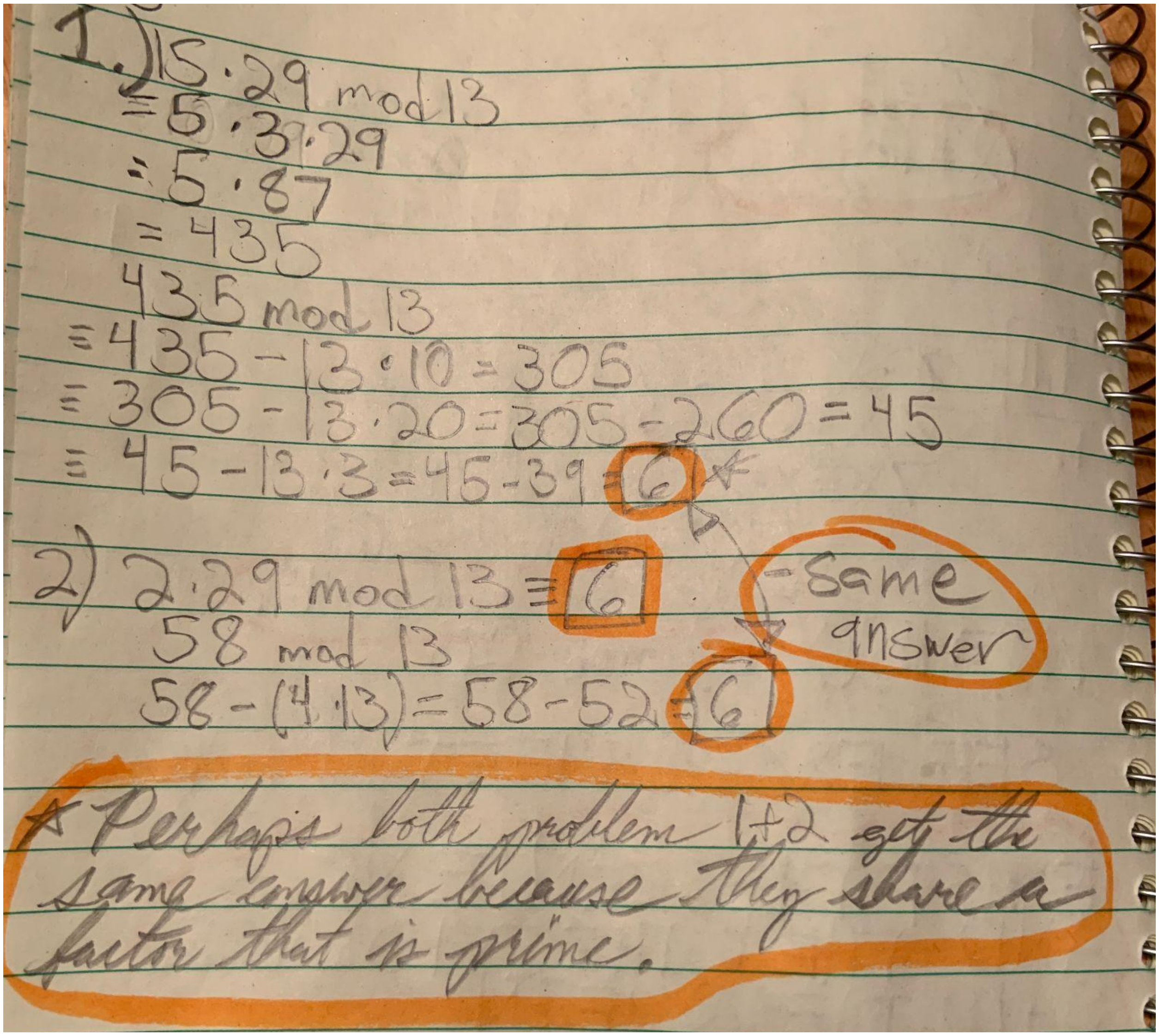
$26^{\text{spots}} = 2^{128}$

* 26 can't be rewritten just with base 2; using logs.

spots $= \log_{26}(2^{128})$

$= 128\cdot\log_{26}(2) \approx 27.23$ lowercase letters

1.5



1.) $15 \cdot 29 \bmod 13$
$= 5 \cdot 3 \cdot 29$
$= 5 \cdot 87$
$= 435$
$435 \bmod 13$
$\equiv 435 - 13 \cdot 10 = 305$
$\equiv 305 - 13 \cdot 20 = 305 - 260 = 45$
$\equiv 45 - 13 \cdot 3 = 45 - 39 = \boxed{6}$ ☆

2) $2 \cdot 29 \bmod 13 \equiv \boxed{6}$
$58 \bmod 13$
$58 - (4 \cdot 13) = 58 - 52 = \boxed{6}$

same answer

☆ Perhaps both problem 1+2 get the same answer because they share a factor that is prime.

Part 3. $2 \cdot 3 \bmod 13 \approx 6$
Part 4. $-11 \cdot 3 \bmod 13$ simplifies to (-33) mod 13 which is 6.
13(-3)=-39 which is 6 away from -33.

Again, we get the same answer of 6 because a prime factor is shared; I think.
Part 4 gets a negative number initially.
Part 3 is the most straightforward.
Part 1 has the most work to show.

1.6

Task 1-3

A)

$1/5 \bmod 13$

$1 \div 5 = 1 \cdot 5^{-1}$

☆ $1 \cdot 5^{-1} \bmod 13 = ?$

from definition $a \cdot a^{-1} \bmod 13 \equiv 1$

$5 \cdot 8 \equiv_{\bmod 13} 1$ ✓

$5^{-1} = 8$

back to ☆

$1 \cdot 8 \bmod 13 \equiv \boxed{8}$

B)

$1/5 \bmod 7$

$1 \cdot 5^{-1} \bmod 7$ $\qquad$ $5(\underbrace{3}_{5^{-1}}) \equiv_{\bmod 7} 1$ ✓

$1 \cdot 3 \equiv_{\bmod 13} \boxed{3}$

C)

$3 \cdot 2/5 \equiv \bmod 7$ $\qquad$ $5(\underbrace{3}_{5^{-1}}) \equiv 1 \bmod 7$ ✓

$3 \cdot \frac{2}{5} = 6/5 = 6 \cdot 5^{-1} \bmod 7$

$= 6 \cdot 3 \bmod 7$

$= 18 \bmod 7 \equiv \boxed{4}$

<u>*1.7*</u>

task 1.7

#1

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2)

+	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)

+	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	6	6	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) $\mathbb{Z}_4$

$0 \cdot \boxed{} \equiv 1$

$1 \cdot 1 \equiv 1$

$\boxed{2} \cdot \quad \equiv 1$

$\boxed{3} \cdot \quad \equiv 1$

*for Z_4, 2, 0, and 3 don't have multiplicative inverses.

$\mathbb{Z}_6$

$0 \cdot \quad \equiv 1$

$1 \cdot 1 \equiv 1$

$2 \cdot \_ \equiv 1$

$3 \cdot \_ \equiv 1$

$4 \cdot \quad \equiv 1$

$5 \cdot 5 \equiv 1$

*for Z_6, 2, 3, 0, and 4 don't have multiplicative inverses.

$\mathbb{Z}_5$

$1 \cdot 1 \equiv 1$

$2 \cdot 3 \equiv 1$

$3 \cdot 2 \equiv 1$

$4 \cdot 4 \equiv 1$

*A multiplicative inverse works for all nonzero elements in $\mathbb{Z}_5$ because each element can multiply by some term and be simplified to 1 using mod 5. Also helps that 5 is prime.

1.8

1.8

a) $\mathbb{Z}_{11}$ 5, 10, 15, 20, 25, 30, 35, 40, 45

$5 \cdot \boxed{9} = 45$ $45 \bmod_{11} = 1$

$45 - (11 \cdot 4) = 1$

* In $\mathbb{Z}_{11}$, 5's multiplicative inverse is 9.

b) $\mathbb{Z}_{12}$

$5 \cdot \boxed{5} = 25$ $25 \bmod_{12} = 1$

$25 - (2 \cdot 12) = 1$ ✓

* In $\mathbb{Z}_{12}$, 5's multiplicative inverse is 5.

c) $\mathbb{Z}_{13}$ 1, 14, 27, 40

$5 \cdot \boxed{8} = 40$ $40 \bmod_{13} = 1$

$40 - (3 \cdot 13) = 1$ ✓

* In $\mathbb{Z}_{13}$, 5's multiplicative inverse is 8.

1.9

1.9

3,000
6500
40
2

Mod 13

A) $X = 3^2 = 3^1 \cdot 3^1 = \boxed{9} \bmod 13$

B) $X = 7^2 = 7 \cdot 7 = 49$

$49 - (13 \cdot 3) = \boxed{10}$

C) $3^{10} = 3^4 \cdot 3^4 \cdot 3^2$ $\quad 81 = 13 \cdot 6 + 3$

$= 81 \cdot 81 \cdot 9$

$= (13 \cdot 6 + 3)(13 \cdot 6 + 3)\, 9$

$\equiv 3 \cdot 3 \cdot 9 = 81$

$= (13 \cdot 6 + 3) \equiv \boxed{3}$

D) $7^{100} = (7^2)^{50}$ $\quad 49 = 13 \cdot 3 + 10$

$(13 \cdot 3 + 10)^{50}$

$\equiv 10^{50} = (10^2)^{25}$ $\quad 100 = 13 \cdot 7 + 9$

$= 100^{25}$

$= (13 \cdot 7 + 9)^{25}$ $\quad 81 = 13 \cdot 6 + 3$

$\equiv 9^{25} = (9^2)^{12} \cdot 9$

$= (13 \cdot 6 + 3)^{12} \cdot 9$

$3^{12} \cdot 9 = (3^4)^3 \cdot 9$

$\equiv 3^3 (9) = 3^5$

$= 9 \cdot 9 \cdot 3$

$= (13 \cdot 6 + 3) \cdot 3$

$\equiv 3 \cdot 3 = \boxed{9}$

E)

1.9 and 1.11

5. $7^x = 11 \mod 13$ $\quad 1 < x < 2$

$x = \log_7(11)$ $\quad 0 < x < 13$

1.11

1. $a \cdot x + b \equiv y \mod 26$

$7x + 22 \equiv y \mod 26$

$7x \equiv y - 22 \mod 26$

$x \equiv 7^{-1}(y-b) \mod 26$

thanks for slide 49.

$x \equiv 15(y-b) \mod 26$

SEE EXCEL SHEET for work

FIRST THE SENTENCE
AND THEN THE EVIDENCE
SAID THE QUEEN

2. Written by Lewis Carroll

[Excel sheet with work]

1.12

1) Encryption: $e_k(x) = y \equiv a \cdot x + b \mod 30$

Decryption: $d_k(y) = x \equiv a^{-1} \cdot (y - b) \mod 30$

with Key: $K = (a,b)$ and restriction $\gcd(a,30) = 1$.

2) $8 \times 30 - 1 = 239$ Keys

\# of desirable characters — options — (1,0) option we don't want.

3) $x \equiv a^{-1} \cdot (y - b) \mod 30$ — Not 29

$17^{-1} \equiv \boxed{23}$ so $x \equiv 23(y-1) \mod 30$

F — $x \equiv 23(26-1)$ mod "

R — $x \equiv 23(20-1)$ mod "

O — $x \equiv 23(29-1)$ mod "

D — $x \equiv 23(22-1)$ mod "

O — $x \equiv 23(29-1)$ mod "

4) "FRODO" comes from the Shire