1.

a. From: https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html

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

b. From: https://www.dcode.fr/monoalphabetic-substitution

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

c. Shoshin Nagamine

2.

a. 15 * 29 mod 13 = (15 mod 13)(29 mod 13) = (2)(3) = **6**
b. 2 * 29 mod 13 =(2 mod 13)(29 mod 13) = (2)(3) = **6**
c. 2 * 3 mod 13 = (2 mod 13)(3 mod 13) = (2)(3) = **6**
d. -11 * 3 mod 13

-11 = (13 *x) + y 3 mod 13
-11 = (13 * 1) + 2 3
-11 mod 13 = 2
(2)(3) = **6**

Since remainders are not unique, each problem is an equivalence class/relation of mod 13. Each "a" in these problems will always have a remainder of 6 when divided by 13.

3. For the first block, the encryption is $y = E_k$ (x XOR IV), so the decryption is $x = D_k$ (y) XOR IV. Since you have the key, you can decrypt the ciphertext (D_k(y)) and you know the plaintext result is 0xFF. Therefore, x XOR D_k(y) will give you the IV.

4.

a. a=7, m=26
gcd(26, 7) = gcd(13*2, 7) = 1

i	q	t
1	3	
2	1	-3
3	2	4
4	2	-11

a^{-1} = t mod m = -11 mod 26 = **15**

b. a=19, m=999

i	q	t
1	52	
2	1	-52
3	1	53
4	2	-105
5	1	263
6	1	-368

a^{-1} = t mod m = 3 mod 999 = **631**

5. m=6
O(theta) = (3 – 1)(2 – 1) =2
Euler's Theorem holds if a^2 = 1 mod 6 and if the gcd of a and m=6 equals 1 for all elements a.

$0^2 = 0 \bmod 6$
$1^2 = 1 \bmod 6$
$2^2 = 4 \bmod 6$
$3^2 = 3 \bmod 6$
$4^2 = 4 \bmod 6$
$5^2 = 1 \bmod 6$

m=9
O(theta) = 9 – 3 = 6
Euler's Theorem holds if $a^6 = 1 \bmod 9$ and if the gcd of a and m=9 equals 1 for all elements a.
$0^6 = 0 \bmod 9$
$1^6 = 1 \bmod 9$
$2^6 = 1 \bmod 9$
$3^6 = 0 \bmod 9$
$4^6 = 1 \bmod 9$
$5^6 = 1 \bmod 9$
$6^6 = 0 \bmod 9$
$7^6 = 1 \bmod 9$
$8^6 = 1 \bmod 9$

6.

a. 49, only gcd(49, 640) will equal 1 and therefore have a modular inverse. 640 is (p-1)*(q-1). Gcd(640, 49) = gcd(8*8*5*2, 7*7)=1 while gcd(32,640) = gcd(2*2*2*2*2, 8*8*5*2) = 2.

b.

n=pq
n=697
O(theta)=(p-1)(q-1)=640
e=49
$d = e^{-1} = 1 \bmod O(\text{theta})$
gcd(640, 49) = 1
1 = 49 – 16 * 3
= 49 – 16 * (640 – 13 *49)
= 209 * 49 – 16 * 640
= 209 * 49 mod 640
d= 209, p=41, q=17

7.

a.

$B = 2^{105} \bmod 467 = 444$
$K_{eph} = 2^{213} \bmod 467 =$ **29**
$Y = 33 * 444^{213} \bmod 467 =$ **296**
Encrypt is (**29, 296**)

Decrypt is $x = y * k_M^{-1} \bmod p$
$k_M = k_e^{d} \bmod p$

$k_M = 29^{105} \bmod 467 = 292$
$k_M^{-1} = 8$

$x = 296 * 8 \bmod 467 = \mathbf{33}$

b. $B = 2^{105} \bmod 467 = 444$
$K_{eph} = 2^{123} \bmod 467 = 125$
$Y = 33 * 444^{123} \bmod 467 = 301$
Encrypt is (**125, 301**)
$k_M = 125^{105} \bmod 467 = 278$
$k_M^{-1} = 42$

$x = 301 * 42 \bmod 467 = \mathbf{33}$

c. $B = 2^{300} \bmod 467 = 317$
$K_{eph} = 2^{45} \bmod 467 = \mathbf{80}$
$Y = 248 * 317^{45} \bmod 467 = \mathbf{174}$
Encrypt is (**80, 174**)
$k_M = 80^{300} \bmod 467 = 12$
$k_M^{-1} = 39$

$x = 174 * 39 \bmod 467 = \mathbf{248}$

d. $B = 2^{300} \bmod 467 = 317$
$K_{eph} = 2^{47} \bmod 467 = \mathbf{320}$
$Y = 248 * 317^{47} \bmod 467 = \mathbf{139}$
Encrypt is (**320, 139**)
$k_M = 320^{300} \bmod 467 = 74$
$k_M^{-1} = 284$

$x = 139 * 284 \bmod 467 = \mathbf{248}$