CIS 3362 Homework #2 Solutions
By Justin King

Part A: Code Break Questions

1) Decode the following message, which was encrypted using the substitution cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

```
fzpgtofucfukqmzvftfuktofgzftouqmfmtosopvfupenopajttoptzqjedu
qtzqvcgqolvlpvlgqrllggqvvifmtolzlfvdkvprrpvtovlziqjqmmfopdtq
dqfttqopyluqlgptmfvgttolulbttzqrlggpklgfmdlsqdldzfeeelpdiqjt
qpnvfxlajtqueitolmfvgtnlvgquzoqdqlgftzfeeklttolnvfxlalspjglp
giqjcuqzpgptlpsolvfpruqtgqvfsofmiqjgqeylhjlgtfqutzqmfvgtiqjz
feekltpmvllsqniqmtolsqdlaqqcfmiqjgqeylhjlgtfqutvollmfvgtiqjz
feeklttludqeepvgkqqdejsc
```

Solution

Cryptool.html was used for this question, as well as the formula sheet.
Pasting in the ciphertext, we get the following frequency breakdown:

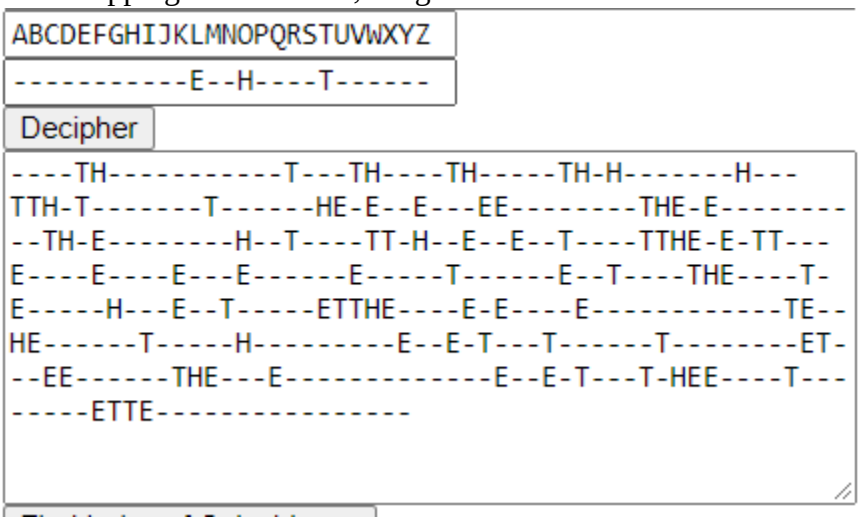
A 1.0% N 1.3%
B 0.3% O 5.2%
C 1.3% P 5.7%
D 3.1% **Q 11.2%**
E 4.4% R 1.3%
F 8.1% S 2.1%
G 6.5% **T 9.9%**
H 0.5% U 3.9%
I 2.6% V 6.0%
J 3.6% W 0.0%
K 2.1% X 0.5%
L 10.7% Y 0.8%
M 3.9% Z 3.9%

English	Average		
E	12.7%	M	2.4%
T	9.1%	W	2.3%
A	8.2%	F	2.2%
O	7.5%	Y	2.0%
I	7.0%	G	2.0%
N	6.7%	P	1.9%
S	6.3%	B	1.5%
H	6.1%	V	1.0%
R	6.0%	K	0.8%
D	4.3%	J	0.2%
L	4.0%	Q	0.1%
U	2.8%	X	0.1%
C	2.8%	Z	0.1%

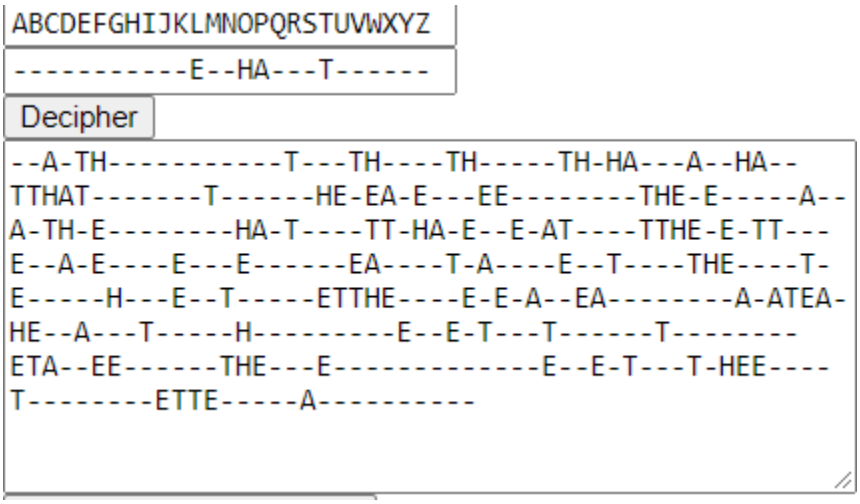
Seeing that T, Q , and L have the highest frequency in the cipher text, the next step is to try to create THE by looking at the common trigrams that are made with T, Q, and L. Since in English,

E and T are the most common letters, we look for a trigram that has 2 common letters on the 1st and 3rd letter of it.

TOL is the most common trigram that uses 2 of either T,Q, or L on the 1st and 3rd letter of them. After mapping TOL to THE, we get



We see a TH-T which could be THAT



We see a TEA-H which is probably TEACH, so we map S to C and get

ABCDEFGHIJKLMNOPQRSTUVWXYZ

----------E--HA--CT------

Decipher

```
--A-TH----------T---TH----TH-----THCHA---A--HA--
TTHAT-------T------HE-EA-E---EE--------THE-E-----A--
A-TH-E--------HA-T----TT-HA-E--E-AT----TTHE-E-TT---
E--A-E----EC--E------EA----T-A----E--T----THE----T-
E-----H---E--T-----ETTHE----E-ECA--EA--------A-
ATEACHE--A---T----CH---------E--E-T---T------T------
--ETA--EEC-----THEC--E-------------E--E-T---T-HEE---
-T--------ETTE-----A--------C-
```

The most common twin bigram by far that wasn't mapped was EE, so it could be LL

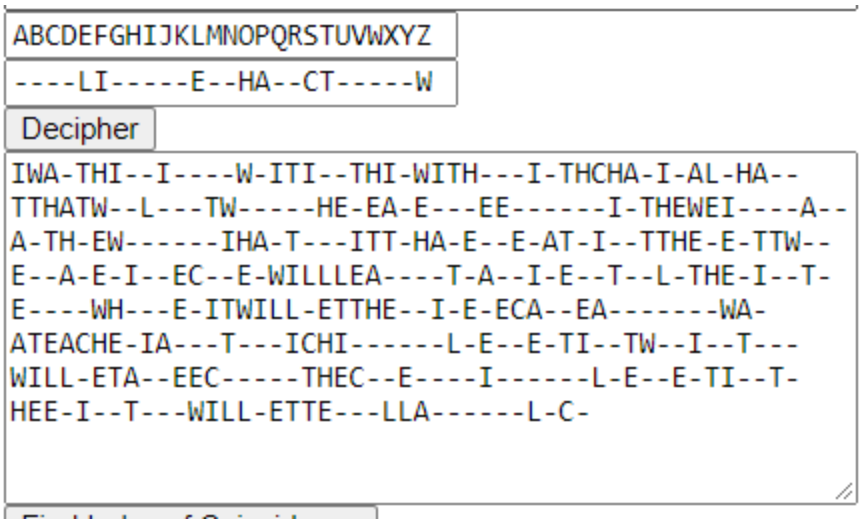
ABCDEFGHIJKLMNOPQRSTUVWXYZ

----L------E--HA--CT------

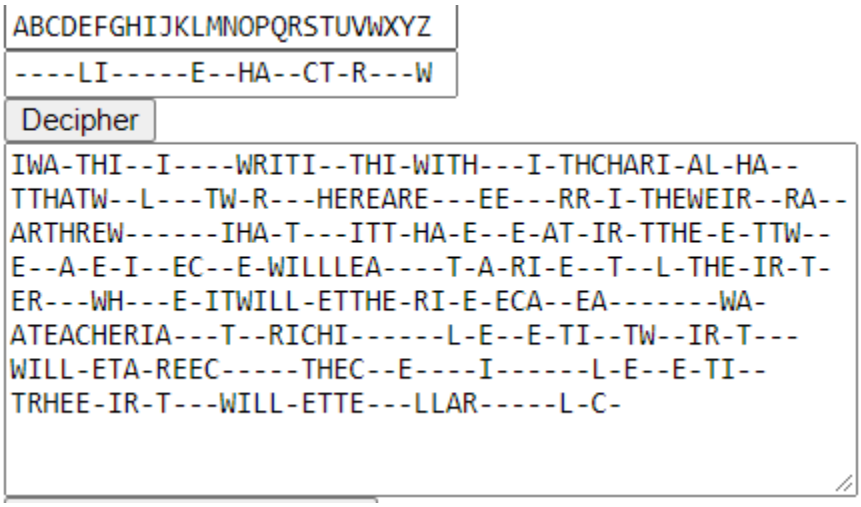
Decipher

```
--A-TH----------T---TH----TH-----THCHA---AL-HA--
TTHAT---L---T------HE-EA-E---EE--------THE-E-----A--
A-TH-E--------HA-T----TT-HA-E--E-AT----TTHE-E-TT---
E--A-E----EC--E---LLLEA----T-A----E--T--L-THE----T-
E-----H---E--T--LL-ETTHE----E-ECA--EA--------A-
ATEACHE--A---T----CH-------L-E--E-T---T------T-----
LL-ETA--EEC-----THEC--E----------L-E--E-T---T-HEE--
--T-----LL-ETTE---LLA------L-C-
```

ZFEE appears 4 times in the ciphertext and since we know it ends with LL, we can guess that the word is WILL because it's the most common word that ends with double L's.



ATEACH- is probably A TEACHER



WRITI—THI- WITH is probably “Writing this with”

ABCDEFGHIJKLMNOPQRSTUVWXYZ

----LIS---GE--HA--CTNR---W

Decipher

```
IWASTHIN-ING--WRITINGTHISWITHN--I-THCHARINAL-HA--
TTHATW--L-N-TW-R-S-HEREARES--EESS-RR-I-THEWEIR-GRA--
ARTHREW------IHA-T---ITT-HA-EN-ESAT-IRSTTHENE-TTW--
ESSAGESI--EC--E-WILLLEA----T-A-RI-E--T-NL-THE-IRST-
ERS-NWH---ESITWILLGETTHE-RI-E-ECA-SEAS----N-
WASATEACHERIA-N-TS-RICHI----S-L-E--ESTI-NTW--IRST---
WILLGETA-REEC-----THEC--E----I----S-L-E--ESTI-
NTRHEE-IRST---WILLGETTEN--LLARSG---L-C-
```

THIN-ING is probably THINKING and -ESSAGES is probably MESSAGES

ABCDEFGHIJKLMNOPQRSTUVWXYZ

--K-LIS---GE--HA-MCTNR---W

Decipher

```
IWASTHINKING--WRITINGTHISWITHN--I-THCHARINAL-HA--
TTHATW--L-N-TW-RKS-HEREARES-MEESS-RR-I-THEWEIR-
GRAMMARTHREW------IHA-T---ITT-HA-EN-ESAT-IRSTTHENE-
TTW-MESSAGESI--EC--E-WILLLEA----T-A-RI-E--T-NL-THE-
IRST-ERS-NWH---ESITWILLGETTHE-RI-E-ECA-SEAS---KN-
WASATEACHERIAMN-TS-RICHI----S-L-E--ESTI-NTW--IRST---
WILLGETA-REEC-----THEC--E---KI----S-L-E--ESTI-
NTRHEE-IRST---WILLGETTEN--LLARSG---L-CK
```

WILLGETTEN—LLARS is “will get ten dollars”

ABCDEFGHIJKLMNOPQRSTUVWXYZ

--KDLIS---GE--HAOMCTNR---W

Decipher

```
IWASTHINKINGO-WRITINGTHISWITHNO-I-THCHARINAL-HA--
TTHATWO-LDNOTWORKSOHEREARESOMEESSORR-I-
THEWEIRDGRAMMARTHREW-O-O--IHADTODOITTOHA-ENOESAT-
IRSTTHENE-TTWOMESSAGESI-DECODEDWILLLEAD-O-TOA-RI-E--
TONL-THE-IRST-ERSONWHODOESITWILLGETTHE-RI-E-ECA-
SEAS-O-KNOWASATEACHERIAMNOTSORICHI--O-SOL-E--
ESTIONTWO-IRST-O-WILLGETA-REECO--O-THECODE-OOKI--O-
SOL-E--ESTIONTRHEE-IRST-O-WILLGETTENDOLLARSGOODL-CK
```

--ESTIONTWO and --ESTIONTRHEE is Question two and Question three

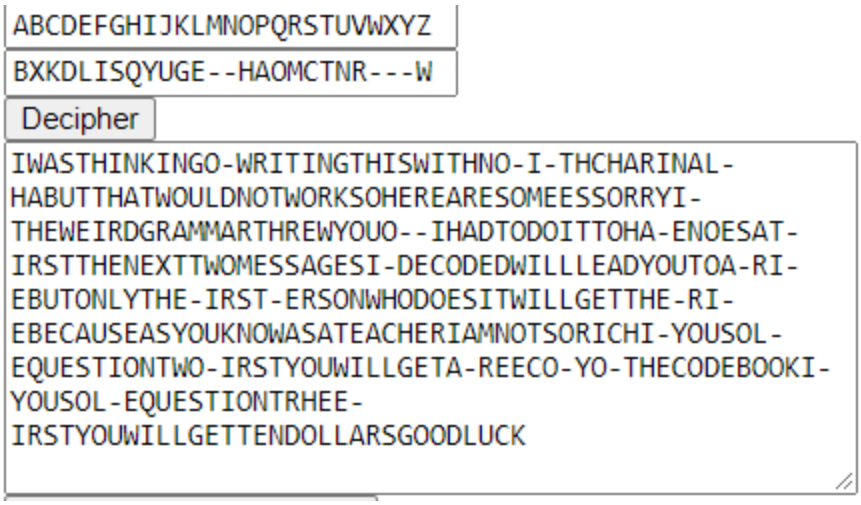
ABCDEFGHIJKLMNOPQRSTUVWXYZ

--KDLISQ-UGE--HAOMCTNR---W

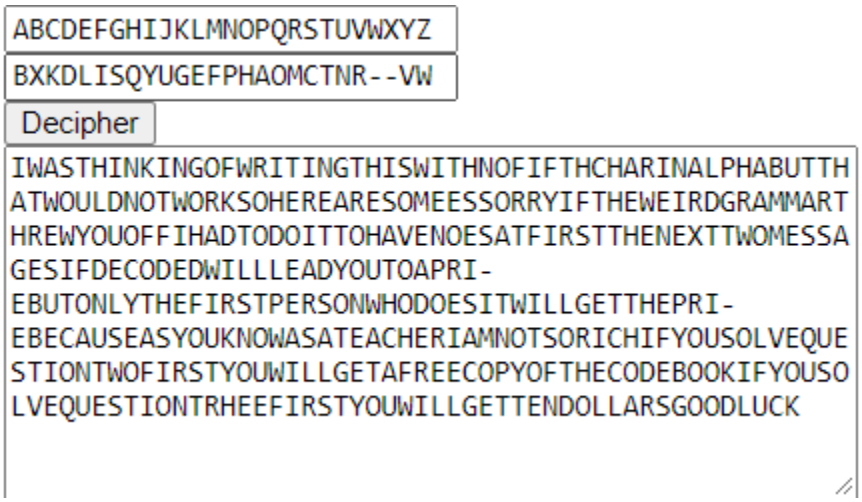
Decipher

```
IWASTHINKINGO-WRITINGTHISWITHNO-I-THCHARINAL-HA-
UTTHATWOULDNOTWORKSOHEREARESOMEESSORR-I-
THEWEIRDGRAMMARTHREW-OUO--IHADTODOITTOHA-ENOESAT-
IRSTTHENE-TTWOMESSAGESI-DECODEDWILLLEAD-OUTOA-RI-E-
UTONL-THE-IRST-ERSONWHODOESITWILLGETTHE-RI-E-
ECAUSEAS-OUKNOWASATEACHERIAMNOTSORICHI--OUSOL-
EQUESTIONTWO-IRST-OUWILLGETA-REECO--O-THECODE-OOKI--
OUSOL-EQUESTIONTRHEE-IRST-
OUWILLGETTENDOLLARSGOODLUCK
```

NE-TTWOMESSAGES is “next two messages” and -ECAUSEAS-OUKNOW is “because as you know”



THE-IRST-ERSON is “The first person” and SOL-E is “Solve”



That leaves PRI-E being Prize and by process of elimination, W maps to J because it’s the only unused letter.

The plain text **is I WAS THINKING OF WRITING THIS WITH NO FIFTH CHAR IN ALPHA BUT THAT WOULD NOT WORK SO HERE ARE SOME ES SORRY IF THE WEIRD GRAMMAR THREW YOU OFF I HAD TO DO IT TO HAVE NO ES AT FIRST THE NEXT TWO MESSAGES IF DECODED WILL LEAD YOU TO A PRIZE BUT ONLY THE FIRST PERSON WHO DOES IT WILL GET THE PRIZE BECAUSE AS YOU KNOW AS A TEACHER I AM NOT SO RICH IF YOU SOLVE QUESTION TWO FIRST YOU WILL GET A FREE COPY OF THE CODE BOOK IF YOU SOLVE QUESTION TRHEE FIRST YOU WILL GET TEN DOLLARS GOOD LUCK**

2) Decode the following message, which was encrypted using the Vigenere cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

Here is the ciphertext:

```
vvgvexzqjzzsiogqhrlawvmldznhipghnuqeuqbsplqoevoeecslmbpyqpega
kexciwebzepglrhalfzosozzdavhryhyryhqachttnsrgawfrvskntwmeaoku
ekdsmfqyepghnnswrwoghmcewvhbulfzwiumjtymvsnpkfrniltmxwwqknvah
vzrwavesmnesvhnuztwzbspagcbpkcrmmfqbqcwotugaogtrltmcpgqufjvuc
ojazlesmeoqgiofvazukstaaohtwrzkixazopkqdvpntytweqadlogfvtztyz
twrcwwgvhrebskzhamtdeihfqkknkeecqqe
```

Using the Cryptool.html, a key length of 15 gave the highest index of coincidence of 6.48% which is ideal. The next step is to find the actual key. This is done by creating 15 bins and cycling through the ciphertext, placing characters in each bin. Assume the first bin is unchanged and test a shift on the second bin for 0, 1, 2, … , 25 times. For each shift, determine the MIC between the first bin and the shifted second bin. The shift with the highest MIC is the relative shift between the first bin and the second bin. Repeat this by comparing the first and third bin and then the first and fourth bin, etc. Then, shift this shifted key until it sorta looks like English. For the execution of this, I used 3.c to produce the 26 shifted keys and I found that

```
Shifted key: abylecqkgjjgaml.
All shifts of the key:
Shift   Key
0       abylecqkgjjgaml
1       bczmfdrlhkkhbnm
2       cdangesmillicon
3       debohftnjmmjdpo
4       efcpiguoknnkeqp
5       fgdqjhvploolfrq
6       gherkiwqmppmgsr
7       hifsljxrnqqnhts
8       ijgtmkysorroiut
9       jkhunlztpsspjvu
10      klivomauqttqkwv
11      lmjwpnbvruurlxw
12      mnkxqocwsvvsmyx
13      nolyrpdxtwwtnzy
14      opmzsqeyuxxuoaz
15      pqnatrfzvyyvpba
16      qrobusgawzzwqcb
17      rspcvthbxaaxrdc
18      stqdwuicybbysed
19      turexvjdzccztfe
20      uvsfywkeaddaugf
21      vwtgzxlfbeebvhg
22      wxuhaymgcffcwih
23      xyvibznhdggdxji
24      yzwjcaoiehheykj
25      zaxkdbpjfiifzlk
```

"cdangesmillicon" was closest to English. The plaintext using this key produced

```
cdangesmilliconcdangesmilliconc
tsgiythebookgatoeryusdadsoffuce
```

Some of this is English, but the others we have to make out to what it should be. At the end offuce is probably office so if o is changed in the key to a, (o - 14 = a to make u+14 = i). Now the plaintext reads

```
tsgiythebookgotoeryusdadsoffice
togetthebookgoto
```

We see “the book go to”, so the preceding text is probably “to get”. Making the adjustments changes the key to (s – 4 = o so d + 4 = **h**, i – 4 = e, so n + 4 = **r**, and y – 5 = t, so g + 5 = **L**. The new key is c**h**a**rl**esmillican which is an English key and produces the plaintext of

```
To get the book go to arups dads office and face the door then
rotate ninety degrees to the left look across the way and you
will see two gray file cabinets out in the hall walk over to
those file cabinets and face them look at the one on the left
and open the second cabinet from the top in there you should
find the code book which is your prize for decoding this message
first hopefully the custodial staff didn’t take it.
```

Note from Arup: Also, you might have noticed when the initial key guess was “cdangesmillicon”, that this looks an awful lot like UCF’s first president, Charles Millican, and this is what the key was. (So you might just go straight to trying that out before anything else!)

3) Decode the following message, which was encrypted using the Vigenere cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

```
dvapngkzabsybpgpekgpsjzcvyghecirtxvlvffxwsykuumdqirwbgicahzyu
hstlhofnduckdnabsjkhtycyzjauszvnjzbqcjpkglfrnvskwwdnoxvtwldki
qimchieprrjzqbxgyrgtzmvyghecirtxvlkjojbhktldzcvfknhtlzctpkcxg
cxhnrtnvscicpmaeffupagrlsttoieqymmvmjmknrtlvsnuwdnruwigzrifrd
mvkeepycuknatqkkhpauqljszwbvydbqqdciawtxtwhryfsawvkcpnvshzewm
hnvfahkgcmddqgieubjnpycwmullamgpurlhtomesvjnrpqbzrj
```

Using cryptool.html, a key length of 12 gave the highest index of coincidence of 6.02%. Using 3.c gave these possible keys.

```
Shifted key: apwnrmepjzfi
All shifts of the key:
Shift   Key
0       apwnrmepjzfi
1       bqxosnfqkagj
2       cryptogrlbhk
3       dszquphsmcil
4       etarvqitndjm
5       fubswrjuoekn
6       gvctxskvpflo
7       hwduytlwqgmp
8       ixevzumxrhnq
9       jyfwavnysior
10      kzgxbwoztjps
11      lahycxpaukqt
12      mbizdyqbvlru
13      ncjaezrcwmsv
14      odkbfasdxntw
15      pelcgbteyoux
16      qfmdhcufzpvy
17      rgneidvgaqwz
18      shofjewhbrxa
19      tipgkfxicsyb
20      ujqhlgyjdtzc
21      vkrimhzkeuad
22      wlsjnialfvbe
23      xmtkojbmgwcf
24      ynulpkcnhxdg
25      zovmqldoiyeh
```

The 3rd key is “cryptogrlbhk” which can be eyeballed to be cryptography. Using cryptography as the key produces the plaintext of

```
Because I am lazy I always use this location to hide stuff for
this class as question one implied there will be ten us dollars
for you if you are the first to break this message so this
location is quite close to my office imagine that you are at my
office and a fire broke out what would you do first go to the
nearest place that would give you something that would help you
fight the flame look carefully and youll find two five dollar
bills
```

Part B: Written Questions Similar to Quiz/Exam Questions

4) Find 83^{-1} mod 188

Solution

For this, we'll use EEA

```
188 = 2 * 83 + 22    => 22 = 188 – (2 * 83)
83 = 3 * 22 + 17     => 17 = 83 – (3 * 22)
22 = 1 * 17 + 5      => 5 = 22 – (1 * 17)
17 = 5 * 3 + 2       => 2 = 17 – (5 * 3)
5 = 2 * 2 + 1        => 1 = 5 – (2 * 2)

1 = 5 – (2 * 2)
1 = 5 – (2 * (17 – (5 * 6)))
1 = 5 – ((2 * 17) – (5 * 6))
1 = (7 * 5) – (2 * 17)
1 = 7 * (22 – 1 * 17) – (2 * 17)
1 = (7 * 22) – (9 * 17)
1 = (7 * 22) – (9 * (83 – (3 * 22)))
1 = (34 * 22) – (9 * 83)
1 = 34 * (188 – (2 * 83)) – (9 * 83)
1 = 34 * 188 – (77 * 83)
-77 * 83 = 1 mod 188
-77 + 188 = 111
```

83^{-1} mod 188 is 111.

5) For an affine cipher, we know that the ciphertext 'N' maps to the plaintext 'E' and the ciphertext 'W' maps to the plaintext 'T'. Determine both the decryption AND encryption functions. Both answers must be in the form f(x) = (ax + b) mod 26, where a and b are in between 0 and 25, inclusive.

Solution

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

Using the table from the reference sheet to get the values of the letters,
The encryption functions can be constructed as:

a) $13 \equiv 4a + b \bmod 26$
b) $22 \equiv 19a + b \bmod 26$

Subtracting equation a from equation b yields:

$9 \equiv 15a \bmod 26$

Value	1	3	5	7	11	17	25
Inverse Mod 26	1	9	21	15	19	23	25

Using this table, its clear we need to multiply both sides of the equation by 7 to yield:
$63 \equiv a \bmod 26$
$a \equiv 63 \bmod 26$
$a \equiv \mathbf{11} \bmod 26$

Substituting back into equation a yields:
$13 \equiv 4(11) + b \bmod 26$
$13 \equiv 44 + b \bmod 26$
$-31 \equiv b \bmod 26$
$b \equiv -31 \bmod 26$
$0b \equiv \mathbf{21} \bmod 26$

Therefore, the encryption function is **f(x) = (11x + 21) mod 26**

The decryption functions can be constructed as

a) $4 \equiv 13a + b \bmod 26$
b) $19 \equiv 22a + b \bmod 26$

Subtracting equation a from b yields:
$15 \equiv 9a \bmod 26$

Value	1	3	5	7	11	17	25
Inverse Mod 26	1	9	21	15	19	23	25

Using this table, its clear we need to multiply both sides of the equation by 3 to yield:
$45 \equiv a \bmod 26$
$a \equiv 45 \bmod 26$
$a \equiv \mathbf{19} \bmod 26$
Substituing back into equation a yields:
$4 \equiv 13(19) + b \bmod 26$
$4 \equiv 247 + b \bmod 26$
$-243 \equiv b \bmod 26$
$b \equiv -243 \bmod 26$
$b \equiv \mathbf{17} \bmod 26$

Therefore, the decryption function is **f(x) = (19x + 17) mod 26**

6) For an alphabet of size 100, how many possible keys would there be to the affine cipher? (Hint: Use logic and the inclusion-exclusion principle to more quickly determine the possible values of a, instead of listing them out one by one!)

Solution

There are **100** possible values for b.
Now, we must find how many values of a are possible. These are all integers from 1 to 100 that do not share any common factors with 100. 100 can be factorized into $2^2 * 5^2$. Let f(x) be the number of values that are in between 1 and 100 that x can divide into evenly. This leaves $100 – f(2) – f(5) + f(2*5) = 100 – 50 – 20 + 10 =$ **40** possible values of a.

So, our possible keys for the affine cipher f an alphabet of size 100 is 40*100 = **4000**

7) Let x be a positive integer. A set of letters consists of 20 As, 25 Bs, 35 Cs, 70 Ds, and 50 Es. What is the index of coincidence of the set? **Leave your answer as a fraction in lowest terms.**

Solution

The size of the set is 20 + 25 + 35 + 70 + 50 = 200 letters.

IOC formula is $\sum \frac{x(x-1)}{n(n-1)}$

$$\frac{20(19) + 25(24) + 35(34) + 70(69) + 50(49)}{200(199)}$$

$$\frac{20(19) + 600 + 1190 + 70(69) + 50(49)}{10(3980)}$$

$$\frac{10(38 + 60 + 119 + 483 + 245)}{10(3980)}$$

$$\frac{945}{3980}$$

$$\frac{189}{796}$$

The index of coincidence is $\mathbf{\frac{189}{796}}$.

8) The set of letters S consists of 30 As, 6 Bs, 24 Cs, 15 Ds, and 15 Es. The set of letters T consists of 25 As, 20 Bs, 15 Cs, 5 Ds and 35 Es. What is the mutual index of coincidence between sets S and T? **Leave your answer as a fraction in lowest terms.**

Solution

Set S is 30+6+24+15+15 = 90 letters and Set T is 25+20+15+5+35 = 100 letters. Using the formula for mutual index of coincidence, we get:

Mutual index of coincidence forumla: $\sum \frac{x * y}{n * m}$

$$\frac{30 * 25 + 6 * 20 + 24 * 15 + 15 * 5 + 15 * 35}{90 * 100}$$

$$\frac{15(50 + 8 + 24 + 5 + 35)}{15(600)}$$

$$\frac{122}{600}$$

$$\frac{61}{300}$$

The mutual index of coincidence is $\mathbf{\frac{61}{300}}$.