Jeremy Barthélemy  
ECE 646  
Hw. 3

Problem 1 (3 points)

Solve the following three (separate) equations:

1. 45 *x* 35 (mod 385)  
  
gcd(45, 385) = 5 = d  
d | b = 5 | 35, which is true, and so there are d solutions.   
The solutions will be x0, x0 + n/d = x1, x0 + 2n/d = x2, x0 + 3n/d = x3, x0 + 4n/d = x­4x0 = (a/d)-1 ⋅ (b/d) (mod n/d)  
Need to solve 9-1 \* mod 77

|  |  |  |  |
| --- | --- | --- | --- |
| I | qi | ri | xi |
| -2 | - | 77 | 0 |
| -1 | 8 | 9 | 1 |
| 0 | 1 | 5 | -8 |
| 1 | 1 | 4 | 9 |
| 2 | 4 | 1 | -17 |
| 3 | - | 0 |  |

So with -17, we add back 77 to get 60.  
x0 = 60\*7\*mod(77) = 35  
  
Solutions:  
x­0: 35  
x1: 35 + n/d = 35 + 385/5 = 112  
x2: 35 + 2n/d = 35 + 385\*2/5 = 189  
x3: 35 + 3n/d = 35 + 385\*3/5 = 266  
x4: 35 + 4n/d = 35 + 385\*4/5 = 343  
We can verify our results by simply:   
(45 \* x – 35) % 385 = 0

2. 24 *x*  36 (mod 385)  
  
gcd(24, 385) = 1 = d  
There is only one solution to this equation.  
  
We must solve for 24-1 mod 385:

|  |  |  |  |
| --- | --- | --- | --- |
| i | qi | ri | xi |
| -2 | - | 385 | 0 |
| -1 | 16 | 24 | 1 |
| 0 | 24 | 1 | -16 |
| 1 | - | 0 |  |

-16 + 385 = 369  
369 \* 36 mod 385 = 194  
  
x = 194

3. 21 *x*  49 (mod 385)

gcd(21, 385) = 7 = d  
d | b? 7 | 49 -> Yes, so there must be 7 solutions to this equation  
3 \* x = 7 \* (mod 55)   
Solve 3-1 \* mod(55)

|  |  |  |  |
| --- | --- | --- | --- |
| i | qi | ri | xi |
| -2 | - | 55 | 0 |
| -1 | 18 | 3 | 1 |
| 0 | 3 | 1 | -18 |
| 1 | - | 0 |  |

-18 + 55 = 37  
37\*7 (mod 55) = 39  
x0 = 39  
(21 \* 39 – 49) % 385 = 0  
  
x0: 39  
x1: = x0 + 1n/d = 39 + 385/7 = 94  
x2: = x0 + 2n/d = 39 + 385\*2 / 7 = 149  
x3: = x0 + 3n/d = 39 + 385\*3 / 7 = 204  
x4: = x0 + 4n/d = 39 + 385\*4 / 7 = 259  
x5: = x0 + 5n/d = 39 + 385\*5 / 7 = 314  
x6: = x0 + 6n/d = 39 + 385\*6 / 7 = 369

Problem 2 (3 points)

Break the affine cipher (i.e., find the key K=(k1, k2)) based on the knowledge of the following ciphertext obtained using this cipher:

HJWWLCGOURCFMCJFDDEBORSOHOFLCWURCFORAVQLWFDWHJWWLC GFCGEKWGOUFEKWU. GS.  
  
We know that there are 12 possible values for k1 and 26 possible values for k2 (0-25). The possible key values for k1 take any integer that is coprime with 26, and less than 26. So we have: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 (In other words, gcd(k1, 26) = 1).  
We know that C = k1\*Mi + k2 mod 26. We must calculate M = k1-1 \*(Ci – k2) mod 26. The most common letters in this ciphertext are W (with 9 appearances), and C and F (each with 7 appearances).  
We can map the most commonly used English letters to two of these as a test.  
I will assume that  
E -> W and T -> F, since F is used as many times as C, and hope to get the correct result.

F(4) -> 22  
f(19) -> 5  
  
4k1 + k2 = 22 mod(26)  
19k1 + k2 = 5 mod(26)  
->  
15k1 = -17 mod(26) = 9 mod(26)  
Solve  
15-1 mod (26)

|  |  |  |  |
| --- | --- | --- | --- |
| i | qi | ri | xi |
| -2 | - | 26 | 0 |
| -1 | 1 | 15 | 1 |
| 0 | 1 | 11 | -1 |
| 1 | 2 | 4 | 2 |
| 2 | 1 | 3 | -5 |
| 3 | 3 | 1 | 7 |
| 4 | - | 0 |  |

For the equation, 7 \* 9 mod(26) = 11  
We find 15 \* 11 – 9 % 26 = 0,   
so we test that k1 = 11, and shift k2 accordingly.

4\*11 + k2 = 22 mod(26)  
(44 + k2 – 22) mod(26) = 0  
For this to be true, k2 = 4  
k1 = 11, k2 = 4  
19\*11 + k2 = 5 mod(26)  
  
For the decryption, k1-1\*(ci –k2) mod(26),  
we find that k1-1 is 19, so for example, with ci = 7 (H), we map 19\*(7-4) mod 26 to find the solution. With this equation, we simply place ci for all values to obtain the plaintext in a spreadsheet:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | H | J | W | W | L | C | G | O | U | R |
| Map | 7 | 9 | 22 | 22 | 11 | 2 | 6 | 14 | 20 | 17 |
| M | 5 | 17 | 4 | 4 | 3 | 14 | 12 | 8 | 18 | 13 |
| M Map | F | R | E | E | D | O | M | I | S | N |
|  |  |  |  |  |  |  |  |  |  |  |
| C | C | F | M | C | J | F | D | D | E | B |
| Map | 2 | 5 | 12 | 2 | 9 | 5 | 3 | 3 | 4 | 1 |
| M | 14 | 19 | 22 | 14 | 17 | 19 | 7 | 7 | 0 | 21 |
| M Map | O | T | W | O | R | T | H | H | A | V |
|  |  |  |  |  |  |  |  |  |  |  |
| C | O | R | S | O | H | O | F | L | C | W |
| Map | 14 | 17 | 18 | 14 | 7 | 14 | 5 | 11 | 2 | 22 |
| M | 8 | 13 | 6 | 8 | 5 | 8 | 19 | 3 | 14 | 4 |
| M Map | I | N | G | I | F | I | T | D | O | E |
|  |  |  |  |  |  |  |  |  |  |  |
| C | U | R | C | F | O | R | A | V | Q | L |
| Map | 20 | 17 | 2 | 5 | 14 | 17 | 0 | 21 | 16 | 11 |
| M | 18 | 13 | 14 | 19 | 8 | 13 | 2 | 11 | 20 | 3 |
| M Map | S | N | O | T | I | N | C | L | U | D |
|  |  |  |  |  |  |  |  |  |  |  |
| C | W | F | D | W | H | J | W | W | L | C |
| Map | 22 | 5 | 3 | 22 | 7 | 9 | 22 | 22 | 11 | 2 |
| M | 4 | 19 | 7 | 4 | 5 | 17 | 4 | 4 | 3 | 14 |
| M Map | E | T | H | E | F | R | E | E | D | O |
|  |  |  |  |  |  |  |  |  |  |  |
| C | G | F | C | G | E | K | W | G | O | U |
| Map | 6 | 5 | 2 | 6 | 4 | 10 | 22 | 6 | 14 | 20 |
| M | 12 | 19 | 14 | 12 | 0 | 10 | 4 | 12 | 8 | 18 |
| M Map | M | T | O | M | A | K | E | M | I | S |
|  |  |  |  |  |  |  |  |  |  |  |
| C | F | E | K | W | U | G | S |  |  |  |
| Map | 5 | 4 | 10 | 22 | 20 | 6 | 18 |  |  |  |
| M | 19 | 0 | 10 | 4 | 18 | 12 | 6 |  |  |  |
| M Map | T | A | K | E | S | M | G |  |  |  |

So:   
HJWWL CGOUR CFMCJ FDDEB ORSOH OFLCW URCFO RAVQL WFDWH JWWLC GFCGE KWGOU FEKWU. GS.   
Maps to:  
FREEDOM IS NOT WORTH HAVING IF IT DOES NOT INCLUDE THE FREEDOM TO MAKE MISTAKES. MG.

Problem 3 (3 points)

Break the affine cipher (i.e., find the key K=(k1, k2)) based on the knowledge that

* the least frequent letter of the ciphertext is 'C'
* the second least frequent letter of the ciphertext is 'I'
* the most frequent trigram is 'WYF'.

WYF could very well be THE. So we can choose W = T, Y = H, and F = E and test.  
We can assume C = Z and I = J, being very infrequent letters in English.  
So I will test Z -> C, J -> I, vs. T -> W and E -> F and compare the calculations to see if my assumptions are correct.  
Plaintext -> Ciphertext  
f(25) -> 2  
f(9) -> 8   
25k1 + k2 = 2 mod(26)  
9k1 + k2 = 8 mod(26)  
to create  
16k1 = -6\*mod(26) = 20 mod(26)  
and  
  
f(19) -> 22  
f(4) -> 5  
19k1 + k2 = 22 mod(26)  
4k1 + k2 = 5\*mod(26)  
to create  
Solving these two equations separately:  
16k1 = 20 mod(26)  
15k1 = 17 mod(26)  
  
Solve 15-1 mod(26):

|  |  |  |  |
| --- | --- | --- | --- |
| i | qi | ri | xi |
| -2 | - | 26 | 0 |
| -1 | 1 | 15 | 1 |
| 0 | 1 | 11 | -1 |
| 1 | 2 | 4 | 2 |
| 2 | 1 | 3 | -5 |
| 3 | 3 | 1 | 7 |
| 4 | - | 0 |  |

Test with (7\*17) mod(26) = 15  
(15\*15 -17) % 26 = 0  
  
Using the original formulas for this case,  
(19\*15 + k2 -22) mod(26) = 0  
(4\*15 + k2 - 5) mod(26) = 0  
-> k1 = 15, k2 = 23  
  
Testing these keys to see if the popular trigram, WYF, = THE, as well as C = Z, I = J:  
  
Use equation Mi = k1-1(Ci – k2) mod (26), where k1-1 = 7,  
W = 22 -> 7\*(22-23) mod(26) = 19 = T  
Y = 24 -> 7\*(24-23) mod(26) = H  
F = 5 -> 7\*(5 – 23) mod (26) = 4 = E  
WYF is indeed THE, as I assumed.  
Now let’s test C and I:  
C = 2 -> 7\*(2-23) mod(26) = 9 = J  
I = 8 -> 7\*(8-23) mod(26) = 25 = Z  
So it appears as though my predictions were in reverse. Instead of Z mapping to C and J mapping to I, it is the contrary!  
The encrypted values of Z and J map to I and C, respectively.

Problem 4 (2 points)  
Decrypt    the    ciphertext   "UWMPO WAGGX FASVZ DDBEV WVG" using the Vigenère cipher with the key "WISDOM".  
First map the key letters to integers:  
W : 22  
I : 8  
S : 18  
D : 3  
O : 14  
M : 12  
We can then simply subtract the keys from these ciphertext values (and perform modulo 26) to find the plaintext, with the key WISDOM repeating across the ciphertext.:  
U– W = 20 – 22 = -2 -> mod 26 = 24 =Y  
W – I = 22 – 8 = 14 = O  
M – S = 12 – 18 = -6 -> mod 26 = 20 = U  
P – D = 15 – 3 = 12 = M  
O – O = 14 – 14 = 0 =A  
W – M = 22 – 12 = 10 = K  
  
A – W = 0 – 22 = -22 -> mod 26 = 4 = E  
G – I = 6 – 8 = -2 -> mod 26 = 24 = Y  
G – S = 6 – 18 = -12 -> mod 26 = 14 = O  
X – D = 23 – 3 = 20 = U  
F – O = 5 – 14 = -9 -> mod 26 = 17 = R  
A – M = 0 – 12 = -12 -> mod 26 = 14 = O  
  
S – W = 18 – 22 = -4 -> mod 26 = 22 = W  
V – I = 21 – 8 = 13 = N  
Z – S = 25 – 18 = 7 = H  
D – D = 0 = A  
D – O = 3 – 14 = -11 -> mod 26 = 15 = P  
B – M = 1 – 12 = -11 -> mod 26 = 15 = P  
  
E – W = 4 – 22 = -18 -> mod 26 = 8 = I  
V – I = 21 – 8 = 13 = N  
W – S = 22 – 18 = 4 = E  
V – D = 21 – 3 = 18 = S  
G – O = 6 – 14 = -8 -> mod 26 = 18 = S  
  
Plaintext: “YOU MAKE YOUR OWN HAPPINESS”

Problem 5 (2 points)

In the ciphertext obtained using Vigenère cipher, a four-character sequence FRHT appears at positions 21, 219, and 453. Additionally, the measure of roughness for this ciphertext is equal to 0.0058. Based on this information, determine the most likely period of the Vigenère cipher.  
The differences between these three positions are:  
198, 234  
We can calculate the gcd of these two values to give a better idea of the possible period of the key.  
gcd(198, 234)  
234-198 = 36  
36 \* 5 = 180, 198 – 180 = 18  
18 \* 2 = 36, so gcd(198, 234) = 18  
According to the period of roughness (0.0058), it is closest to the measure of rougness of 0.006, which is of a period of 5.  
Since 6 is close to 5, and is a factor of 18, it seems safe to assume that the period of the key is 6 characters.   
  
Problem 6 (3 points)

Determine the measure of roughness of the following ciphertext using the index of coincidence method (i.e., calculate the measure of rougness using the maximum possible precision). What is the most likely period of the general polyalphabetic cipher used to obtain this ciphertext?

ravzh jzfwp qdvzh qndia brkuz kudqn vzhfp vmdjz fdepr czqmr kkdqa zqpib pvnku dqdbr iimdx qdpkd qpcgi dnndq wdqnz cnkup cvzhq ndiad cozvv zhqpj urded fdckn pnbdi ipnvz hqwip cnldd wrckd qdnkd grcvz hqzbc jpqdd quzbd edquh fmidr krnpq dpiwz nndnn rzcrc kudju pcxrc xazqk hcdnz akrfd  
  
There are a total of N = 235 characters.

|  |  |  |
| --- | --- | --- |
| Letter | # of Letter | Index of Coincidence |
| A | 6 | 0.000545554 |
| B | 6 | 0.000545554 |
| C | 15 | 0.003818876 |
| D | 35 | 0.021640298 |
| E | 3 | 0.000109111 |
| F | 6 | 0.000545554 |
| G | 2 | 3.63702E-05 |
| H | 9 | 0.001309329 |
| I | 11 | 0.002000364 |
| J | 5 | 0.000363702 |
| K | 14 | 0.003309693 |
| L | 1 | 0 |
| M | 4 | 0.000218221 |
| N | 19 | 0.006219313 |
| O | 1 | 0 |
| P | 16 | 0.00436443 |
| Q | 21 | 0.007637752 |
| R | 14 | 0.003309693 |
| S | 0 | 0 |
| T | 0 | 0 |
| U | 9 | 0.001309329 |
| V | 10 | 0.001636661 |
| W | 5 | 0.000363702 |
| X | 3 | 0.000109111 |
| Y | 0 | 0 |
| Z | 20 | 0.006910347 |
|  |  |  |
|  | Total IC = | 0.066302964 |
|  | MR= | 0.027841426 |

Where the Measurement of Roughness is Total IC – 1/26  
From this, the period should be 1, as the value calculated is very close to 0.028.