CIS 3362 Homework #2: Classical Ciphers - Written Problems Solutions

1) Prove that encrypting a plaintext with two successive affine cipher keys is no more secure than encrypting a plaintext with a single set of affine cipher keys.

Solution

Let any two valid affine ciphers be $f(x) = (ax+b) \bmod 26$ and $g(x) = (cx+d) \bmod 26$. If we compose the two, we get:

$$g(f(x)) = (c(ax+b) + d) \bmod 26$$
$$= (acx + (bc+d)) \bmod 26$$

Since $\gcd(a, 26) = 1$ and $\gcd(c, 26) = 1$, it follows that $\gcd(ac, 26) = 1$. Thus, the coefficient in front of x is a valid value for the original key a in the cipher. Similarly, bc+d is a valid value mod 26. Thus, given a, b, c and d from any two affine functions, we can compose the two functions and come up with an equivalent pair $a' = ac \bmod 26$ and $b' = (bc+d) \bmod 26$ that form a single affine key that is equivalent to the given function composition.

2) Find $148^{-1} \bmod 327$.

Solution

Run the Extended Euclidean algorithm with 327 and 148:

$327 = 2 \times 148 + 31$
$148 = 4 \times 31 + 24$
$31 = 1 \times 24 + 7$
$24 = 3 \times 7 + 3$
$7 = 2 \times 3 + 1$

$7 - 2 \times 3 = 1$
$7 - 2(24 - 3 \times 7) = 1$
$7 - 2 \times 24 + 6 \times 7 = 1$
$7 \times 7 - 2 \times 24 = 1$
$7(31 - 24) - 2 \times 24 = 1$
$7 \times 31 - 7 \times 24 - 2 \times 24 = 1$
$7 \times 31 - 9 \times 24 = 1$
$7 \times 31 - 9(148 - 4 \times 31) = 1$
$7 \times 31 - 9 \times 148 + 36 \times 31 = 1$
$43 \times 31 - 9 \times 148 = 1$
$43(327 - 2 \times 148) - 9 \times 148 = 1$
$43 \times 327 - 86 \times 148 - 9 \times 148 = 1$
$43 \times 327 - 95 \times 148 = 1$

Considering the last equation mod 327 we get

43 x 327 - 95 x 148 ≡ 1 mod 327
43 x 0 - 95 x 148 ≡ 1 mod 327
- 95 x 148 ≡ 1 mod 327

It follows that $148^{-1} \equiv -95 \equiv 232 \pmod{327}$.

3) For an alphabet of size 79, a set of affine encryption keys is a = 46, b = 22. (Thus the encryption function is f(x) = (46x + 22) % 79.) Determine the corresponding set of decryption keys.

Solution
Take the equation and solve for x (we substitute y for f(x) for convenience):

y ≡ (46x + 22) mod 79
y - 22 ≡ 46x mod 79

At this point we must find 46^{-1} mod 79. Run the Extended Euclidean Algorithm:

79 = 1 x 46 + 33
46 = 1 x 33 + 13
33 = 2 x 13 + 7
13 = 1 x 7 + 6
7 = 1 x 6 + 1

7 - 1 x 6 = 1
7 - (13 - 7) = 1
2 x 7 - 1 x 13 = 1
2(33 - 2 x 13) - 1 x 13 = 1
2 x 33 - 5 x 13 = 1
2 x 33 - 5(46 - 33) = 1
2 x 33 - 5 x 46 + 5 x 33 = 1
7 x 33 - 5 x 46 = 1
7(79 - 46) - 5 x 46 = 1
7 x 79 - 12 x 46 = 1

Taking this equation mod 79, we find that $46^{-1} \equiv -12 \equiv 67 \pmod{79}$.

Thus, we multiply our equation (the one we had before starting the Extended Euclidean Algorithm) through by 67:

y - 22 ≡ 46x (mod 79)
67(y - 22) ≡ 67(46x) (mod 79)
x ≡ 67y - 1474 (mod 79)
x ≡ 67y + 27 mod 79

It follows that our decryption keys are a = 67, b = 27.

4) A set of letters consists of 20 As, 35 Bs, 40 Cs, 5 Ds, 10 Es, and 50 Fs. What is the index of coincidence of the set?

Solution

$$IC = \frac{20 \times 19 + 35 \times 34 + 40 \times 39 + 5 \times 4 + 10 \times 9 + 50 \times 49}{160 \times 159} = \frac{5690}{160 \times 159} = \frac{569}{2544} \sim .224$$

5) The set of letters S consists of 15 As, 25 Bs, 35 Cs, 15 Ds, and 10 Es. The set of letters T consists of 60 As, 25 Bs, 15 Cs, 20 Ds and 40 Es. What is the mutual index of coincidence between sets S and T? **Leave your answer as a fraction in lowest terms.**

Solution

$$MIC = \frac{15 \times 60 + 25 \times 25 + 35 \times 15 + 15 \times 20 + 10 \times 40}{100 \times 160} = \frac{2750}{16000} = \frac{11}{48} \sim .229$$

6) Encrypt the plaintext "FOOTBALLGAMEONTHURSDAY" using the Vigenere cipher and the keyword "KNIGHTS". (For practice for the first exam, do this by hand with a chart with the values of the letters.)

Solution

```
P =  5 14 14 19  1  0 11 11  6  0 12  4 14 13 19  7 20 17 18  3  0 24
K = 10 13  8  6  7 19 18 10 13  8  6  7 19 18 10 13  8  6  7 19 18 10
C = 15 27 22 25  8 19 29 21 19  8 18 11 33 31 29 20 28 23 25 22 18 34
       1              3                 7  5  3     2              8
```

Ciphertext letters = **PBWYITDVTISLHFDUCXZWRI**

The first line written above is the plaintext converted to numbers. The second line is the key converted to numbers and the third line is the added cipher text. The fourth line contains only values greater than 26 modded by 26 and then those numbers are all converted back to letters to get the actual cipher text (which is bolded).

7) Encrypt the message, "WHENWALLSCOMEDOWNEVERYONEWINS" using the Playfair cipher with the key "BRICKS" and the padding character "X". (Please do NOT use a program to do this.)

Solution
Here is the corresponding Playfair square:

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

Here is the message split into pairs (with padding characters added, as needed):

```
WH EN WA LX LS CO ME DO WN EV ER YO NE WI NS
```

Converting the pairs we get:

RP FM RH QI GD BT TM SQ ZH SY AC VT MF XR GF

8) Decrypt the message, "ABEPCLCFWNAMNX", which was enciphered using the Playfair cipher with the key "TURTLES". Note: The padding character used was "Q". (Please do NOT use a program to do this.)

Solution
Here is the corresponding Playfair square:

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

Here is the ciphertext broken into pairs:

```
AB EP CL CF WN AM NX
```

Here is the corresponding plaintext:

```
SA LQ LY SI NG SN OW
```

Getting rid of the padding character we obtain the plaintext: **SALLY SINGS NOW.**