MATH 235 01: Basic Algebra Fall 2002

Solutions to Assignment 3

Problem 1. Suppose a plain text was encrypted using a Shift Cipher and the following message was sent:

$$HPHTWWXPPELEXTOYTRSE$$

Find the key K and decrypt the original text.

Solution. Try $K = 1, 2, 3, \dots$ until a reasonable text occurs. Easy to check that $K = 11$ and the text is **WEWILLMEETATMIDNIGHT**.

Problem 2. Suppose a plain text was encrypted using an Affine Cipher with keys $a = 7, b = 3$ and the following message was sent:

$$TXXYQHTAZ$$

Decrypt the original text.

Solution. The decryption function is

$$d(y) = a^{-1}(y - b)(mod\ 26) = 7^{-1}(y - 3)(mod\ 26)$$

Solve equation $7x = 1(mod\ 26)$ to find 7^{-1}. Easy to see that

$$7^{-1} = 15(mod\ 26)$$

Now

$$T \to 19,\ X \to 23,\ Y \to 24,\ Q \to 16,\ H \to 7,\ A \to 0,\ Z \to 25$$

Decrypting:

$$d(19) = 15(19 - 3)(mod\ 26) = 240(mod\ 26) = 6(mod\ 26)$$

Similarly,

$$d(23) = 14,\ d(24) = 3,\ d(16) = 13,\ d(7) = 8,\ d(0) = 7,\ d(25) = 18$$

Converting to letters: **GOODNIGHS**
Remark: was an error in encrypting the last letter.

Problem 3. Suppose a plain text was encrypted using the system described above with public information $n = 77, e = 43$ and the following message was sent:

$$11\ 0\ 61\ 53$$

Decrypt the original text.

Solution.

$$n = 7 \cdot 11,\ p = 7,\ q = 11,\ k = (7-1)(11-1) = 60$$

To find d solve the equation

$$43d = 1(mod\ 60)$$

Easy to check that $d = 7$.

Decryption function:

$$d(y) = y^d(mod\ 77) = y^7(mod\ 77)$$

Hence

$$d(11) = 11^7 = 11(mod\ 77)$$

Similarly,

$$d(0) = 0,\ d(61) = 19,\ d(53) = 4$$

Converting to letters: **LATE**

Remark: avoid heavy calculations using the following method. To compute, say $61^7(mod\ 77)$:

$61^2 = 25(mod\ 77)$

$61^4 = (61^2)^2 = 25^2(mod\ 77) = 9(mod\ 77)$

$61^7 = (61^4) \cdot (61^2) \cdot 61 = 25 \cdot 9 \cdot 61(mod\ 77) = 19(mod\ 77)$