MATH 235 01: Basic Algebra   Fall 2002

Assignment 3

I. Shift Cipher.

Given a bijection ϕ :

$A \to 0, B \to 1, C \to 2, D \to 3, E \to 4, F \to 5, G \to 6, H \to 7, I \to 8, J \to 9, K \to 10,$

$L \to 11, M \to 12N \to 13, O \to 14, P \to 15, Q \to 16, R \to 17, S \to 18, T \to 19,$

$U \to 20, V \to 21, W \to 22, X \to 23, Y \to 24, Z \to 25$

A plain text (a sequence of letters) $a_1a_2\dots a_m$ is mapped into a sequence of numbers $x_1x_2\dots x_m$, where $x_i = \phi(a_i) \in \mathbb{Z}_{26}$:

$$a_1a_2\dots a_m \to x_1x_2\dots x_m$$

Given a key $K \in \mathbb{Z}_{26}$.

Encryption function with the key K:

$$e_K(x) = (x + K)(mod\ 26).$$

Encryption of the sequence:

$$x_1x_2\dots x_m \to e_K(x_1)e_K(x_2)\dots e_K(x_m)$$

Message to send over an insecure channel:

$$b_1b_2\dots b_m, \quad where\ b_i = \phi^{-1}(e_K(x_i)).$$

Example 1.

Text: GO
Sequence of numbers: 6 14
Key $K = 12$
Encrypted sequence: 18 0
Message to send: SA

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.

II. Affine Cipher.

Given: the bijection ϕ as above.

As above each plain text $a_1a_2 \dots a_m$ is mapped to a sequence of numbers $x_1x_2 \dots x_m$, where $x_i = \phi(a_i) \in \mathbb{Z}_{26}$.

Given keys: $a, b \in \mathbb{Z}_{26}$ such that a is relatively prime to 26.

Encryption function with the keys a, b:

$$e(x) = (ax + b)(mod\ 26).$$

Encryption of the sequence:

$$x_1x_2 \dots x_m \to e(x_1)e(x_2) \dots e(x_m)$$

Message to send over an insecure channel:

$$b_1b_2 \dots b_m, \quad where\ b_i = \phi^{-1}(e(x_i)).$$

Example 2.

Text: HOT
Sequence of numbers: 7 14 19
Keys: $a = 7, b = 3$
Encrypted sequence: 0 23 6
Message to send: AXG

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.

III. RSA type.
Given: the bijection ϕ as above.

As above each plain text $a_1a_2 \dots a_m$ is mapped to a sequence of numbers $x_1x_2 \dots x_m$, where $x_i = \phi(a_i) \in \mathbb{Z}_{26}$.

Given keys: primes p, q, $n = pq$, a number d such that d is relatively prime to $k = (p-1)(q-1)$, a number e such that $ed \equiv 1(mod\ k)$.

Encryption function with the keys e, n:

$$e(x) = x^e(mod\ n).$$

Encryption of the sequence:

$$x_1x_2 \dots x_m \to e(x_1)e(x_2) \dots e(x_m)$$

Message to send over an insecure channel (the same as the encrypted message):

$$e(x_1)e(x_2) \dots e(x_m)$$

Public information: n, e

Example 3.

Text: GO
Sequence of numbers: 6 14
Keys: $p = 5, q = 11, n = 55, k = 40, d = 27, e = 3$
Encrypted sequence: 51 49 *(indeed,* $6^3 \equiv 51(mod\ 55)$*,* $14^3 = 49(mod\ 55)$*)*
Message to send: 51 49

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.