T-79.503 Foundations of Cryptology
Homework 1
September 17, 2003

1. (Stinson 1.8) List all invertible elements in $\mathbb{Z}_m$, for $m = 28$, 33 and 35.

2. (Stinson 1.6 and 1.11 a)) If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an *involutory key*.

   a) Find all the involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

   b) Suppose that $K = (a, b)$ is a key in an affine cipher over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a+1) \equiv 0(\mathrm{mod} n)$.

3. (Stinson 1.15) Determine the inverses of the following matrices over $\mathbb{Z}_{26}$:

$$\text{a)} \quad \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \quad \text{b)} \quad \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

4. (see Stinson 1.24) An *Affine Hill Cipher* is the following modification of a *Hill Cipher*. The encryption operator is of the form

$$(y_1, \ldots, y_m) = (x_1, \ldots, x_m)L + b$$

   where L is an invertible $m \times m$-matrix and b is a $1 \times m$-vector over the ring $\mathbb{Z}_{26}$.

   Suppose Oscar has learned that the plaintext

   `adisplayedequation`

   is encrypted to the ciphertext

   `DSRMSIOPLXLJBZULLM`

   and Oscar also knows that $m = 3$. Compute L and b.

5. Who is the inventor, who borrowed the name of his new invention from the famous survivor

   `RLD ABLAIORXBLJ` ?

   At least you should be able to derive the inventor's initials, which were used as the key when the survivor's name was encrypted using the **affine cipher** on an alphabet of 27 letters. The first two letters of the survivor's name are `RO`. The plaintext and ciphertext alphabet consists of the 26 letters `A-Z` and the space between words. These 27 symbols are converted to integers modulo 27 as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	
0	1	2	3	4	5	6	7	8	9	10	11	12	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	"space"
13	14	15	16	17	18	19	20	21	22	23	24	25	26

6. The plaintext and the ciphertext alphabet is as above in the previous problem.

   Each plaintext character x is encrypted separately using a randomized substitution method. The key $K = (k_0, k_1, \ldots, k_9)$ is a permutation of the ten digits $\{0, 1, \ldots, 9\}$. The encryption process has the following steps.

   (a) Pick a character y from the plaintext alphabet at random. Interpret the pair (y, x) as the representation of an integer I to the base 27, that is, $I = 27 \cdot y + x$. Let a_2, a_1, a_0 be the digits of I in the decimal system, where a_2 is the most significant digit.

   (b) Use the key K to substitute a_i by k_{a_i}, $i = 0$, 1, 2.

   (c) The ciphertext $(c_2$, c_1, $c_0)$ is obtained as the 27-base representation of the integer $100 \cdot k_{a_2} + 10 \cdot k_{a_1} + k_{a_0}$.

   An attacker is observing plaintext-ciphertext pairs produced by this encryption method with the same fixed key. An encryption of the character 'space' is 'ABX' and an encryption for character 'B' is 'ACB'. Based on this information, derive a and b such that $k_a = 0$ and $k_b = 5$.