

Homework 1

Encryption

Botond Lajos Perényi

Task 1: Affine cipher in \mathbb{Z}_{97} .

- (a) Encryption and Decryption functions with key $k = (a, b)$ (the message is m and the resulting ciphertext is c):

$$E(k, m) = a \cdot m + b \bmod 97$$

$$D(k, c) = a^{-1} \cdot (c - b) \bmod 97$$

- (b) The number of possible meaningful and different keys is

$$|a| \cdot |b|$$

Where $|a|$ is the possibilities for a and $|b|$ is the different possibilities for b . b can have 97 different values, and a can have as many as there are co-primes below 97 with 97. This is given by Euler's Totient function: $\phi(97) = 96$ (this is because 97 is prime). In total the number of different keys is:

$$96 \cdot 97 = 9312$$

- (c) We have an intercepted ciphertext-plaintext pair: (DOG)=(28 83 43), and a ciphertext with the same key: (78 23 33).

To figure out the key we can use two letters from the known ciphertext-plaintext pair with either the Encryption or the Decryption functions: (I choose the decryption with letters (DO) = (28 83))

$$D(k, 28) = a^{-1} \cdot (28 - b) \bmod 97 = (D)3$$

$$D(k, 83) = a^{-1} \cdot (83 - b) \bmod 97 = (O)14$$

Thus we get:

$$a^{-1} \cdot (28 - b) \bmod 97 = 3$$

$$a^{-1} \cdot (83 - b) \bmod 97 = 14$$

Rewriting the equations we get:

$$b = 28 - 3a \bmod 97$$

$$b = 83 - 14a \bmod 97$$

Making the two equal each other:

$$28 - 3a = 83 - 14a \bmod 97$$

With rearranging we get:

$$55 = 11a \bmod 97$$

We need the multiplicative inverse of 11 in mod 97, which is 53. (Using the Extended Euclidean Algorithm this is fairly straightforward.) With multiplication we get:

$$a = 55 \cdot 53 \bmod 97 = 2915 \bmod 97 = 5$$

Substituting back to one previous equation we get:

$$b = 28 - 3 \cdot 5 \bmod 97 = 28 - 15 \bmod 97 = 13$$

Meaning the key is: $k = (5, 13)$

For decrypting the second message we firstly need the multiplicative inverse of 5 (mod 97) which is 39. Writing this into the decryption function we get:

$$D(k, 78) = 39 \cdot (78 - 13) \bmod 97 = 13(N)$$

$$D(k, 23) = 39 \cdot (23 - 13) \bmod 97 = 2(C)$$

$$D(k, 33) = 39 \cdot (33 - 13) \bmod 97 = 4(E)$$

The encrypted message is (NCE).

Task 2

Task 3

Task 4

Task 5