OLGA RADKO MATH CIRCLE, SPRING 2024: ADVANCED 3

FERNANDO FIGUEROA AND JOAQUÍN MORAGA

Worksheet 2: Introduction to Cryptography

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plaintext and the disguised message is called the ciphertext.

An enciphering transformation is a function that takes any plaintext message and gives a ciphertext message. In other words it is a function $f : \mathcal{P} \to \mathcal{C}$, where $\mathcal{P}$ and $\mathcal{C}$ are the sets of all possible plaintexts and ciphertexts, respectively. We will usually require that f is one-to-one and onto, i.e. for any ciphertext there is exactly one plaintext that gets encrypted into it. The deciphering transformation is f^{-1}, the inverse of the enciphering transformation.

Our first encryption method will be to turn phrases into numbers. Our plaintexts will be phrases containing only words and blank spaces, and our ciphertexts will be natural numbers.

First of all, we can assign numbers to letters, simply by giving numbers $\{0, 1, \ldots, 25\}$ to $\{A, B, \ldots, Z\}$ according to the alphabetical order. We will assign the value 26 to blank space, so we can write phrases as numbers.

In order to transform a phrase into a natural number we will use base 27. Thus a word like NO, would correspond to $27 * 13 + 14 = 365$, and the word YES would correspond to $27^2 * 24 + 27 * 14 + 18 = 17973$.

Problem 2.1:

Explain the deciphering transformation that turns numbers into phrases, given the previous encryption transformation.

Give the plaintext for the following ciphertexts (for this problem you may use a calculator):

(1) 1477
(2) 176430
(3) 197401661

Solution 2.1:

A different way to assign a numerical value to a phrase (made of letters and blank spaces), is to assign as ciphertext a tuple of numbers, where each individual symbol $\{A, \ldots, Z, \text{" "}\}$ corresponds to a number $0, 1, \ldots, 26$.

Problem 2.2:

Give the plaintext for the following ciphertexts:

(1) $\{19, 14, 12, 0, 19, 14\}$
(2) $\{2, 0, 19\}$
(3) $\{19, 7, 4, 26, 16, 20, 8, 2, 10, 26, 1, 17, 14, 22, 13, 26, 5, 14, 23, 26, 9, 20, 12, 15, 18, 26, 14, 21, 4, 17, 26, 19, 7, 4, 26, 11, 0, 25, 24, 26, 3, 14, 6\}$

Solution 2.2:

The advantage of using numbers is that it is easier to define functions in a succinct way, e.g. via addition, multiplication or other methods. If we want both plaintext and ciphertext to be composed of letters, we can create an enciphering transformation via the following functions:

$\mathcal{P} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{N} \xrightarrow{f^{-1}} \mathcal{C}$.

Where $\mathcal{P}, \mathcal{C}$ and $\mathcal{N}$ are phrases (plaintext),phrases (ciphertext) and tuples of numbers, respectively. f an enciphering map from phrases to tuples of numbers, as in Problem 2.2, and g a function such as adding a number.

Problem 2.3:

Give the plaintext for the following phrases, where the g in the previous paragraphs is given by adding 3 modulo 27. This is an example of a Caesar cipher, where the encryption is given by shifting the symbols by a fixed number.

(1) AHV
(2) ZDWHUPHORQ
(3) PDWKHPDWLFV

Solution 2.3:

Problem 2.4:

What would be some possible ways to decipher a message that is encrypted via Caesar cipher, as in the previous exercise, but we do not know the number by which it was shifted?

Can you decipher the plaintext for the following message encrypted by some Caesar cipher (our symbols are $\{A, \ldots, Z, \text{" "}\}$, where " " denotes a blank space between letters.)

"FURMCGVPXMODAI MSAJMWGZBEMAHRDMFURMYNLKMQAT"

Solution 2.4:

If we know the general method by which a message is encrypted, we can use information about the language to make an educated guess on the most likely encryption. For example, the most common letter in English is E, so one can expect the most common letter in plaintexts to be E

Problem 2.5:

The following ciphertext was obtained by shifting letters and keeping the blank spaces and blank spaces.

"PX PXKX ENVDR UXVTNLX HYMXG MAX YKXJNXGVR FXMAHW GXXWL EHGZXK VBIAXK-MXQM"

Can you determine what was the shift?

Solution 2.5:

By knowing that a message was encrypted through a Caesar cipher, one can find the encrypted message, by trying all possible shifts (via a computer, for example). So, this is not the safest way to encrypt a message. The general idea would be to find more general functions on $\mathbb{Z}/27\mathbb{Z}$ when we use the english alphabet and blank spaces or more generally $\mathbb{Z}/n\mathbb{Z}$ if we use an alphabet of n "letters".

Instead of adding i.e. $g(x) = x + b$, one can take affine transformations, i.e. $g(x) = ax + b$.

Problem 2.6:

What conditions do we have to ask to a and b for the encryption given by the function $g(x) = ax + b$ applied to each "letter", in order to guarantee that our message can be deciphered to obtain the original message? In other words, what conditions do we need to impose to guarantee that every ciphertext corresponds to a unique plaintext?

Solution 2.6:

Problem 2.7:

In the 27 letter alphabet (26 letters, with blank space=26), use the affine enciphering with $g(x) = 9x + 13$ to encode the following text:

CATCH THE CAT.

What other plaintexts can get encoded into the ciphertext that you got?

Solution 2.7:

Problem 2.8:

In a long ciphertext which you are trying to analyze, you know that the blank spaces are unchanged and the letters (26) are shifted by an affine transformation. If you know that Y, V in ciphertext correspond to E, T in plaintext respectively. Decipher the following ciphertext:

“”QAOOYQQ EV HEQV”

Solution 2.8:

Remember that for an encryption to be valid, we would like any ciphertext to correspond to a unique plaintext.

Problem 2.9:

How many valid affine transformations are there for an alphabet of 26 letters?

What about for a general N?

Solution 2.9:

Problem 2.10:

(1) Show that in $\mathbb{F}_5$, the function $g(x) = x^3$ can be used to permutate the letters in an alphabet of 5 letters to obtain a valid enciphering function.
(2) What values can α take, so the function $g(x) = x^\alpha$ in $\mathbb{F}_5$, can be used to permutate the letters in an alphabet of 5 letters to obtain a valid enciphering function?

Solution 2.10:

For the following problems you may use without proof the following fact: For any prime number p, there exists a number α, such that, any nonzero number in $\mathbb{F}_p$ can be written as α^n for some n.

Let p be a prime number, such that $p \equiv 2 \pmod 3$

Problem 2.11:

Show that the function $g(x) = x^3$ in $\mathbb{F}_p$ gives a valid encryption when change letter by letter in an alphabet containing p letters.

Solution 2.11:

Let p and q be a prime numbers, such that $p \not\equiv 1 \pmod{q}$

Problem 2.12:

Show that the function $g(x) = x^q$ in $\mathbb{F}_p$ gives a valid encryption when changing letter by letter in an alphabet containing p letters.

What other conditions do we need to impose when q is not a prime number?

Solution 2.12:

We define the product of two encryptions, to be the cryptosystem that results from first encrypting plaintext into ciphertext by an encryption f_1 and then encrypting a second time by an encryption f_2. Thus one gets an encryption $f = f_2 \circ f_1$. We will also sometimes refer to this as the composition of two encryptions.

Problem 2.13:

Show that the product of two affine encryptions is still an affine encryption.

Solution 2.13:

Instead of considering each letter as a number from 0 to 25 (or 26 if we allow blank spaces), we can pair the letters in digraphs (two letters) and consider each digraph as a number from 0 to 675 (or 728 if we allow blank spaces). In this numeric system, we can apply shifts or affine transformations, to change each digraph by the same rule

Problem 2.14:

Suppose our alphabet consists of only the letters and we apply an encryption that sends the plaintext NO to ciphertext QY. Encrypt the plaintext ON, by that encryption.

Solution 2.14:

We have mostly thought about encryptions where plaintext and ciphertext have a common alphabet, or at least the same number of letters

Now choose an alphabet with N letters for the plaintext, and an alphabet with M letters for the cyphertext, where $M > N$.

Split the plaintext into digraphs, so we will be working with N^2 digraphs in plaintext and M^2 digraphs in ciphertext.

Fix a number L, with $N^2 \leq L \leq M^2$, and choose integers a, b, with $\gcd(a, L) = 1$. Encipher the digraphs via the function

$$g(X) = aX + b.$$

Where the equations is inside $\mathbb{Z}/L\mathbb{Z}$.

We will call such a function to be an (N, M)-affine digraph encryption.

Problem 2.15:

Let f_1 and f_2 be two cryptosystems as in the explanation given in the previous paragraphs, more especifically f_1 is an (N, N_1)-affine digraph encryption and f_2 is an (N_1, N_2)-affine digraph encryption.

Is the composition of $f_1 \circ f_2$ always an (N, N_2)-affine digraph encryption?

Solution 2.15:

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: fzamora@math.princeton.edu

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: jmoraga@math.ucla.edu