Cryptography

Introduction

Number theory plays a key role in cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge.

Number theory is the basis of many classical ciphers, first used thousands of years ago, and used extensively until the 20th century.

These ciphers encrypt messages by changing each letter to a different letter, or each block of letters to a different block of letters

We will discuss some classical ciphers, including shift ciphers, which replace each letter by the letter a fixed number of positions later in the alphabet, wrapping around to the beginning of the alphabet when necessary

The classical ciphers we will discuss are examples of private key ciphers where knowing how to encrypt allows someone to also decrypt messages.

With a private key cipher, two parties who wish to communicate in secret must share a secret key.

The classical ciphers we will discuss are also vulnerable to cryptanalysis, which seeks to recover encrypted information without access to the secret information used to encrypt the message.

We will show how to cryptanalyze messages sent using shift ciphers

- The most widely used public key system, called the RSA cryptosystem, encrypts messages using modular exponentiation, where the modulus is the product of two large primes.
  The encrypt requires that someone know the modulus and an exponent. (It does not require that the two prime factors of the modulus be known.)
- As far as it is known, knowing how to decrypt requires someone to know how to invert the encryption function, which can only be done in a practical amount of time when someone knows these two large prime factors.
- In this chapter we will explain how the RSA cryptosystem works, including how to encrypt and
  decrypt messages.

The subject of cryptography also includes the subject of cryptographic protocols, which are exchanges of messages carried out by two or more parties to achieve a specific security goal.

Classical Cryptography

- One of the earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three).
- For instance, using this scheme the letter B is sent to E and the letter X is sent to A. This is an example of **encryption**, that is, the process of making a message secret.

Caesar's encryption

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

WE can assign numbers to the alphabets A to Z from 0 to 25 as

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

Caesar's encryption

For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer $p, p \leq 25$,

the integer $f(p)$ in the set {0, 1, 2, . . . , 25} with

$$f(p) = (p + 3) \bmod 26.$$

In the encrypted version of the message, the letter represented by *p* is replaced with the letter represented by $(p + 3) \bmod 26$.

Example to illustrate Caesar's encryption

EXAMPLE What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution: First replace the letters in the message with numbers. This produces 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$. This gives 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN."

Decryption to Caesar's Encrypted Message

To recover the original message from a secret message encrypted by the Caesar cipher, the function f^{-1}, the inverse of f, is used.

Note that the function f^{-1} sends an integer

p from $\boldsymbol{Z}_{26}$, to $f^{-1}(p) = (p - 3)$ **mod** 26.

In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet.

The process of determining the original message from the encrypted message is called **decryption**.

Generalization to Caesar's Encryption and Decryption

There are various ways to generalize the Caesar cipher.

For example, instead of shifting the numerical equivalent of each letter by 3, we can shift the numerical equivalent of each letter by k, so that

(Encryption)

$f(p) = (p + k) \bmod 26$. Such a cipher is called a shift cipher.

Note that decryption can be carried out using

$f^{-1}(p) = (p - k) \bmod 26$.

Note: The integer k is called a **key**.

Encryption Example by Shift Cipher

Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with shift $k = 11$.

Solution: To encrypt the message "STOP GLOBAL WARMING" we first translate each letter to the corresponding element of $\boldsymbol{Z}_{26}$.

This produces the string

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

We now apply the shift $f(p) = (p + 11) \bmod 26$ to each number in this string.

We obtain

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating this last string back to letters, we obtain the ciphertext "DEZA RWZMLW HLCXTYR."

Decryption Example by Shift Cipher

Example: Decrypt the ciphertext message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted with the shift $k = 7$.

Solution: To decrypt the ciphertext "LEWLYPLUJL PZ H NYLHA ALHJOLY" we first translate the letters back to elements of $\boldsymbol{Z}_{26}$.

We obtain

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Finally, we translate these numbers back to letters to obtain the plaintext.

We obtain

"EXPERIENCE IS A GREAT TEACHER."

Affine Cipher

We can generalize shift ciphers further to slightly enhance security by using a function of the form

$f(p) = (ap + b) \bmod 26$,

where a and b are integers, chosen so that f is a bijection.

Note: The function $f(p) = (ap + b) \bmod 26$ is a bijection if and only if $\gcd(a, 26) = 1$.

Such a mapping is called an affine transformation, and the resulting cipher is called an affine cipher.

One letter Example to Affine Cipher

What letter replaces the letter K when the function $f(p) = (7p + 3) \bmod 26$ is used for encryption?

Solution: First, note that 10 represents K.

Then, using the encryption function specified, it follows that

$f(10) = (7 * 10 + 3) \bmod 26 = 21$.

Because 21 represents V, K is replaced by V in the encrypted message