Cryptosystem Using Greek Alphabets

M. Antony Arockiasamy, G. Charles Antony Raj

PG And Research Department of Mathematics, Sacred Heart College (Autonomous), Tirupattur, Vellore, India.
PG And Research Department of Mathematics,Sacred Heart College (Autonomous), Tirupattur, Vellore, India.
arockiaanto2008@gmail.com, charcar17@gmail.com

ABSTRACT: Cryptography is the study of encoding and decoding secret messages, videos, audio and images. In this paper a study on modified encryption and decryption technique is done to cryptanalyst by using Greek Alphabets. Addition, Subtraction and Multiplication tables of mod 24 for Greek Alphabets are created. Using Shift transformation, Julius Caesar method, Affine transformation, Digraph, Enciphering matrices, Knapsack problem, new ciphertext codes are generated.

Keywords: Greek Alphabets, Shift transformation, Julius Caesar method, Affine transformation, Digraph, Enciphering matrix

1. INTRODUCTION

Cryptology is defined as the science of making communication incomprehensible to all people except those who have a right to read and understand it. The study of cryptology consists of two parts; cryptography, which concerns itself with the secrecy system itself and its design, and cryptanalysis, which concerns itself with the breaking of the secrecy system above [3]. Cryptography is the process of writing using various methods (“ciphers”) to keep messages secret. Cryptanalysis is the science of attacking ciphers, finding weaknesses, or even proving that a cipher is secure. Cryptology covers both: it’s the complete science of secure communication [1]. Cryptography is the one of the Branch of Number Theory concerned with the theory and applications oriented topic. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that block adversaries, various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, there by precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power an example is the one-time pad but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms. The message to be encrypted is known as plain text. It is the original message before transformation. The result of the Encryption process is known as Cipher Text. Encryption and Decryption Algorithm are referred as Cipher. Key is a number or set of numbers operated by a Cipher. The Art of breaking cipher is known as cryptanalysis and the art of devising them is known as cryptology [4]. Sender sends a message using Plain text. After that, message is encrypted and a key is added, so it becomes Cipher text and goes to receiver side. At the Receiver side, Decryption algorithm converts Cipher text to plain text and thus provides original data. The readable message (original) is called plaintext.The secret message (not readable) is called cipher text.The process of converting plaintext to ciphertext is called Enciphering transformation.The process of converting ciphertext to plaintext is called Deciphering transformation.

Section 2: Main Results

In the second section the basic definitions are introduced and main results are derived and some properties of cryptosystem using Greek alphabets are obtained.

2.1 Greek Alphabet

The **Greek alphabet** is the script that has been used to write the **Greek language** since the 8th century BC. It was derived from the earlier **Phoenician alphabet**, and was the first alphabetic script to have distinct letters for vowels as well as consonants.

Table 1 Greek Alphabets

Name	Capital letters	Small letters	Equivalents
Alpha	Α	α	a
Beta	Β	β	b
gamma	Γ	γ	g
Delta	Δ	δ	d
epsilon	Ε	ε	e
Zeta	Ζ	Ζ	z
Eta	Η	Η	h
Theta	Θ	Θ	th
Iota	Ι	ı	i
kappa	Κ	κ	k
lambda	Λ	λ	l

Mu	Μ	μ	m
Nu	Ν	ν	n
Xi	Ξ	ξ	x
omicron	Ο	ο	o
Pi	Π	π	p
Rho	Ρ	ρ	r
sigma	Σ	σ(ς)	s
Tau	Τ	τ	t
upsilon	Υ	υ	u, y
Phi	Φ	φ	ph
Chi	Χ	χ	ch
Psi	Ψ	ψ	ps
omega	Ω	ω	ō

Here is an easy one. The 24 letters of the Greek alphabet are divided into two parts. The Vowels and the Consonants.

There are 7 Vowels and 17 Consonants. They are:

Vowels	α,ε,η,ι,υ,ο,ω
Consonants	β,γ,δ,ζ,θ,κ,λ,μ,ν,ξ,π,ρ,σ,τ,φ,χ,ψ

Vowels are either short or long. There are separate Greek characters (ε, η, ο, ω) for the e and o sounds, but not for a, i and u sounds. A straight line that appears above the vowel when it is long - , η, ī, ω, ū; the short vowels are α, ε, ι, ο υ.

Table 2 Greek Vowels

Greek Vowels	Roman alphabet equivalents	Name
α Α	a	alpha
ε Ε	e	epsilon
η Η	ē or ê	eta
ι Ι	i	iota
ο Ο	o	omicron
ω Ω	ō	omega
υ Υ	y, u	upsilon
ου ΟΥ	ou	omicron + upsilon

2.2 Coding Numbers

We define the codes for the Greek alphabets as in table below.

Table 3 Greek Alphabets Codes

Α	β	γ	δ	ε	Ζ	η	Θ	ι	κ	λ	μ	Ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

2.3 Shift Transformation

The shift transformation is defined as C ≡ P + b mod N. Where “P” refers to Plaintext, “C” denotes Ciphertext, “N” refers to Number of alphabets and “a” indicates Enciphering key [2].

2.4 Julius Caesar Method

Julius Caesar method is given by C ≡ P + 3 mod N, with regular symbols P, C and N carrying the meanings as defined in 2.6 [2]. The Shift (or Caesar) Cipher is another monoalphabetic substitution cipher. Although more secure than the Atbash Cipher, it is still an easy cipher to break, especially by today's standards. Originally, it was used by Julius Caesar for sending encrypted messages to his troops, as recorded by Suetonius. This describes what we would now call a shift of 3, and describes the cipher that Caesar used quite well. That is, "a" was encrypted as "D", "b" as "E", etc.

2.5 Example

Using the Julius Caesar method defined in 2.7, we find the cipher text to the plain text**“θε-ον**” (**the-on**) (which means “**god**”) when N = 24 as “**κθδσπ**”. We also prove the reverse process. We know that, C ≡ P + 3 mod 24. Each letter is encrypted by its corresponding coding number table 2.1

θ= 7, C = 7 + 3 mod 24
= 10 mod 24 = 10
= λ
ε = 4 , C = 4 + 3 mod 24
= 7 mod 24 = 7
= θ
- = 0, C = 0 + 3 mod 24
= 3 mod 24 = 3
= δ
ο = 15 , C =15 + 3 mod 24
= 18 mod 24 = 18
= σ
ν = 13 , C = 13 + 3 mod 24
= 16 mod 24 = 16
= π

Thereforethe plaintext “**θε-ον**” is enciphered as “**κθδσπ**” that is “**θε-ον**” → “**κθδσπ**”.

Reverse:
Find the plaintext to the ciphertext when N = 24, “**κθδσπ**”. We know that, P ≡ C - 3 mod 24. Each letter is encrypted by its corresponding coding number table 2.1
λ = 10, P = 10 - 3 mod 24
= 7 mod 24 = 7 = θ
θ = 7, P = 7 - 3 mod 24
= 4 mod 24 = 4
= ε
δ= 3, P = 3 - 3 mod 24
= 0 mod 24 = 0
= -
σ= 18, P = 18 - 3 mod 24
= 15 mod 24 = 15
= ο
π= 16, P = 16 - 3 mod 24
= 13 mod 24 = 13
= ν

Thereforethe ciphertext “**κθδσπ**” is deciphered as “**θε-ον**” that is“**κθδσπ**” → “**θε-ον**”.

2.6 Example

So suppose that we intercept the message “**φσξεγ**”, which we know was enciphered using a shift transformation on single letters of the 24-letter alphabet, as in the example above. It remains for us to find the b. One way to do this is by frequency analysis. This works as follows. Suppose that we have already intercepted a long string of ciphertext, say several hundred letters. We know that “α” is the most frequently occurring letter in the Greek language. So it is reasonable to assume that the most frequently occurring letter in the ciphertext is the encryption of α.Suppose that we find that “ξ” is the most frequently occurring character in the ciphertext.

We know that, P ≡ C – b mod N
Also, we know the frequent letters α, ξ.
The numerical values are α = 0, ξ = 13

P ≡ C – b mod N
0 ≡ 13 – b mod 24
b ≡ 13 mod 24

The required formula is,

P ≡ C – 13 mod 24

φ = 20, P = 20 -13 mod 24
= 7 mod 24 = 7
= θ

σ= 17, P = 17 -13 mod 24
= 4 mod 24 = 4
= ε

ξ = 13, P = 13 -13 mod 24
= 0 mod 24 = 0
= α

ε = 4, P = 4 -13 mod 24
= -9 mod 24 = 15
= ο

β = 1, P = 1 -13 mod 24
= -12 mod 24 = 12
= ν

Thereforethe ciphertext “**φσξεγ**” is deciphered as “**θε-ον**” that is “**φσξεγ**” → “**θε-ον**”.

2.7 Greek Alphabets Tables

In this section, we present Addition, Subtraction & Multiplication tables of Greek alphabets for mod 24 this will generate a lot of interest in the study of Cryptosystem using Greek alphabets. At the end of this section we present interesting properties of this table.

Table 4 Greek Alphabets- Addition Table For Mod 24

+	α	β	γ	δ	Ε	ζ	η	θ	ι	κ	λ	μ	ν	Ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
α	α	β	γ	δ	Ε	ζ	η	θ	ι	κ	λ	μ	ν	Ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
β	β	γ	δ	ε	Ζ	η	θ	ι	κ	λ	μ	ν	ξ	Ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	α
γ	γ	δ	ε	ζ	Η	θ	ι	κ	λ	μ	ν	ξ	ο	Π	ρ	σ	τ	υ	φ	χ	ψ	ω	α	β
δ	δ	ε	ζ	η	Θ	ι	κ	λ	μ	ν	ξ	ο	π	Ρ	σ	τ	υ	φ	χ	ψ	ω	α	β	γ
ε	ε	ζ	η	θ	Ι	κ	λ	μ	ν	ξ	ο	π	ρ	Σ	τ	υ	φ	χ	ψ	ω	α	β	γ	δ
ζ	ζ	η	θ	ι	Κ	λ	μ	ν	ξ	ο	π	ρ	σ	Τ	υ	φ	χ	ψ	ω	α	β	γ	δ	ε
η	η	θ	ι	κ	Λ	μ	ν	ξ	ο	π	ρ	σ	τ	Υ	φ	χ	ψ	ω	α	β	γ	δ	ε	ζ
θ	θ	ι	κ	λ	Μ	ν	ξ	ο	π	ρ	σ	τ	υ	Φ	χ	ψ	ω	α	β	γ	δ	ε	ζ	η
ι	ι	κ	λ	μ	Ν	ξ	ο	π	ρ	σ	τ	υ	φ	Χ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ
κ	κ	λ	μ	ν	Ξ	ο	π	ρ	σ	τ	υ	φ	χ	Ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι
λ	λ	μ	ν	ξ	Ο	π	ρ	σ	τ	υ	φ	χ	ψ	Ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ
μ	μ	ν	ξ	ο	Π	ρ	σ	τ	υ	φ	χ	ψ	ω	Α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ
ν	ν	ξ	ο	π	Ρ	σ	τ	υ	φ	χ	ψ	ω	α	Β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ
ξ	ξ	ο	π	ρ	Σ	τ	υ	φ	χ	ψ	ω	α	β	Γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν
ο	ο	π	ρ	σ	Τ	υ	φ	χ	ψ	ω	α	β	γ	Δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ

π	π	ρ	σ	τ	Υ	φ	χ	ψ	ω	α	β	γ	δ	Ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο
ρ	ρ	σ	τ	υ	Φ	χ	ψ	ω	α	β	γ	δ	ε	Ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π
σ	σ	τ	υ	φ	Χ	ψ	ω	α	β	γ	δ	ε	ζ	Η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ
τ	τ	υ	φ	χ	Ψ	ω	α	β	γ	δ	ε	ζ	η	Θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ
υ	υ	φ	χ	ψ	Ω	α	β	γ	δ	ε	ζ	η	θ	Ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ
φ	φ	χ	ψ	ω	Α	β	γ	δ	ε	ζ	η	θ	ι	Κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ
χ	χ	ψ	ω	α	Β	γ	δ	ε	ζ	η	θ	ι	κ	Λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ
ψ	ψ	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	Μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ
ω	ω	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	Ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ

Table 5 Greek Alphabets -Subtraction Table For Mod 24

–	**α**	**β**	**γ**	**δ**	**ε**	**ζ**	**η**	**θ**	**ι**	**κ**	**λ**	**μ**	**ν**	**Ξ**	**ο**	**π**	**ρ**	**σ**	**τ**	**υ**	**φ**	**χ**	**ψ**	**ω**
α	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	Μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β
β	β	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	Ν	μ	λ	κ	ι	θ	η	ζ	ε	δ	γ
γ	γ	β	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	Ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε	δ
δ	δ	γ	β	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	Ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε
ε	ε	δ	γ	β	α	ω	ψ	χ	φ	υ	τ	σ	ρ	Π	ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ
ζ	ζ	ε	δ	γ	β	α	ω	ψ	χ	φ	υ	τ	σ	Ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ	η
η	η	ζ	ε	δ	γ	β	α	ω	ψ	χ	φ	υ	τ	Σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ
θ	θ	η	ζ	ε	δ	γ	β	α	ω	ψ	χ	φ	υ	Τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι
ι	ι	θ	η	ζ	ε	δ	γ	β	α	ω	ψ	χ	φ	Υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ
κ	κ	ι	θ	η	ζ	ε	δ	γ	β	α	ω	ψ	χ	Φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ
λ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β	α	ω	ψ	Χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ
μ	μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β	α	ω	Ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν
ν	ν	μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β	α	Ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ
ξ	ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β	Α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο
ο	ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	Β	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π
π	π	ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε	δ	Γ	β	α	ω	ψ	χ	φ	υ	τ	σ	ρ

ρ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ	ε	Δ	γ	β	α	ω	ψ	χ	φ	υ	τ	σ
σ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ	η	ζ	Ε	δ	γ	β	α	ω	ψ	χ	φ	υ	τ
τ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ	η	Ζ	ε	δ	γ	β	α	ω	ψ	χ	φ	υ
υ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	θ	Η	ζ	ε	δ	γ	β	α	ω	ψ	χ	φ
φ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	ι	Θ	η	ζ	ε	δ	γ	β	α	ω	ψ	χ
χ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	κ	Ι	θ	η	ζ	ε	δ	γ	β	α	ω	ψ
ψ	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	λ	Κ	ι	θ	η	ζ	ε	δ	γ	β	α	ω
ω	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	μ	Λ	κ	ι	θ	η	ζ	ε	δ	γ	β	α

Table 6 Greek Alphabets-Multiplication Table For Mod 24

×	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	Ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
α	α	α	α	α	α	α	α	α	α	α	α	α	α	Α	α	α	α	α	α	α	α	α	α	α
β	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	Ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
γ	α	γ	ε	η	ι	λ	ν	ο	ρ	τ	φ	ψ	α	Γ	ε	η	ι	λ	ν	ο	ρ	τ	φ	ψ
δ	α	δ	η	κ	ν	π	τ	χ	α	δ	η	κ	ν	Π	τ	χ	α	δ	η	κ	ν	π	τ	χ
ε	α	ε	ι	ν	ρ	φ	α	ε	ι	ν	ρ	φ	α	Ε	ι	ν	ρ	φ	α	ε	ι	ν	ρ	φ
ζ	α	ζ	λ	π	φ	β	η	μ	ρ	χ	γ	θ	ν	Σ	ψ	δ	ι	ξ	τ	ω	ε	κ	ο	υ
η	α	η	ν	τ	α	η	ν	τ	α	η	ν	τ	α	Η	ν	τ	α	η	ν	τ	α	η	ν	τ
θ	α	θ	ο	χ	ε	μ	τ	β	ι	π	ψ	ζ	ν	Υ	γ	κ	ρ	ω	η	ξ	φ	δ	λ	σ
ι	α	ι	ρ	α	ι	ρ	α	ι	ρ	α	ι	ρ	α	Ι	ρ	α	ι	ρ	α	ι	ρ	α	ι	ρ
κ	α	κ	τ	δ	ν	χ	η	π	α	κ	τ	δ	ν	Χ	η	π	α	κ	τ	δ	ν	χ	η	π
λ	α	λ	φ	η	ρ	γ	ν	ψ	ι	τ	ε	ο	α	Λ	φ	η	ρ	γ	ν	ψ	ι	τ	ε	ο
μ	α	μ	ψ	κ	φ	θ	τ	ζ	ρ	δ	ο	β	ν	Ω	λ	χ	ι	υ	η	σ	ε	π	γ	ξ
ν	α	ν	α	ν	α	ν	α	ν	α	ν	α	ν	α	Ν	α	ν	α	ν	α	ν	α	ν	α	ν
ξ	α	ξ	γ	π	ε	σ	η	υ	ι	χ	λ	ω	ν	Β	ο	δ	ρ	ζ	τ	θ	φ	κ	ψ	μ
ο	α	ο	ε	τ	ι	ψ	ν	γ	ρ	η	φ	λ	α	Ο	ε	τ	ι	ψ	ν	γ	ρ	η	φ	λ
π	α	π	η	χ	ν	δ	τ	κ	α	π	η	χ	ν	Δ	τ	κ	α	π	η	χ	ν	δ	τ	κ
ρ	α	ρ	ι	α	ρ	ι	α	ρ	ι	α	ρ	ι	α	Ρ	ι	α	ρ	ι	α	ρ	ι	α	ρ	ι

σ	α	σ	λ	δ	φ	ξ	η	ω	ρ	κ	γ	υ	ν	Ζ	ψ	π	ι	β	τ	μ	ε	χ	ο	θ
τ	α	τ	ν	η	α	τ	ν	η	α	τ	ν	η	α	Τ	ν	η	α	τ	ν	η	α	τ	ν	η
υ	α	υ	ο	κ	ε	ω	τ	ξ	ι	δ	ψ	σ	ν	Θ	γ	χ	ρ	μ	η	β	φ	π	λ	ζ
φ	α	φ	ρ	ν	ι	ε	α	φ	ρ	ν	ι	ε	α	Φ	ρ	ν	ι	ε	α	φ	ρ	ν	ι	ε
χ	α	χ	τ	π	ν	κ	η	δ	α	χ	τ	π	ν	Κ	η	δ	α	χ	τ	π	ν	κ	η	δ
ψ	α	ψ	φ	τ	ρ	ο	ν	λ	ι	η	ε	γ	α	Ψ	φ	τ	ρ	ο	ν	λ	ι	η	ε	γ
ω	α	ω	ψ	χ	φ	υ	τ	σ	ρ	π	ο	ξ	ν	Μ	λ	κ	ι	θ	η	ζ	ε	δ	γ	β

2.8 Properties OfAddition Table

- In Greek alphabetic system, if we add number say (x) with "α" we get the same number.
- In each row of the addition table, the alphabets appear in correct cyclic order from first column to last column.
- In each column of the addition table, the alphabets appear in correct cyclic order from first row to last row.

2.9 Properties Of Subtraction table

- In Greek alphabetic system, if we subtract number say (x) with "α" we get the same number.
- In each row of the subtraction table, the alphabets appear in correct cyclic order from last column to first column.
- In each column of the subtraction table, the appearing alphabets are in correct cyclic order from last row to first row.

2.10 Properties OfMultiplication Table

- We create a multiplication table using Greek alphabets. In this table, only few alphabets, have the inverses. They are α, ζ, θ, μ, ξ, σ, υ, ω .
- The product of anyalphabet with these alphabets result in distinct alphabets. That is, In the multiplication table, 1st,5th,7th,11th,13th,17th,19th,23rd rows have all 24 alphabets and they are distinct.
- In the table, 8th row and column, there is a special property that "α, ι, ρ" arerepeated cyclically. There is an order "α, ι, ρ" only exist respectively in the row and column.
- In the 16th row and column, "α, ρ, ι" repeated again and again.
- Similarly the following repetitions are found.
    - 12th row & column - α, ν
    - 6th row & column - α, η, ν, τ
    - 18th row & column - α, τ, ν, η
    - 4th - α, ε, ι, ν, ρ, φ
    - 20th- α, δ, η, κ, ν, π, τ, χ
    - 3rd - α, δ, η, κ, ν, π, τ, χ
    - 9th - α, κ, τ, δ, ν, χ, η, π
    - 15th - α, π, η, χ, ν, δ, τ, κ
    - 21st- α, χ, τ, π, ν, κ, η, δ
    - 2nd - α, γ, ε, η, ι, λ, ν, ο, ρ, τ, φ, ψ
    - 10th - α, λ, φ, η, ρ, γ, ν, ψ, ι, τ, ε, ο
    - 14th - α, ο, ε, τ, ι, ψ, ν, γ, ρ, η, φ, λ
    - 22nd - α, ψ, φ, τ, ρ, ο, ν, λ, ι, η, ε, γ
- Finally there is an interesting property common to all the three tables ν + ν = α , ν – ν = α and also ν × ν = α. It is highlighted in yellow in the tables.

2.11Addition Examples

1) Using the table 4, we find the plaintext to the ciphertext.Addition of "**κοινωνια**" (**koinonia**-which means "**society**") and "**γπηρεσια**" (**hypiresia** -which means "**service**") gives the code word"**μζοεδζρα**".
2) Similarly using the table 3, we find the plaintext to the ciphertext.Addition of "**φυση**" (**physis**-which means "**nature**") and "**κοσμος**" (**kosmos**-which means "**world**") leads to the code **"κοξηθω".**

2.12Subtraction Examples

1) Using the table-5 "**εκκλησια**" (**ecclesia**-which means "**church**") minus"**ευτυχια**" (**ephtychia**-which means "**happiness**")= **"εζορμφαα".**
2) "**ιστορια**" (**historia**-which means "**history**") minus "**σχολειο**" (**ereuna**-which means "**school**") = **"πφεεναλ".**

2.13 Multiplication Examples

1) Using the table-6 the product of"**φιλος**" (**philos**-which means "**friend**") and "**αγαπη**" (**aghape**-which means "**love**") leads to the new code **"αρριερηδη".**
2) The multiplication of "**ποιηση**" (**poise**-which means "**poetry**") and "**γραφη**" (**ghraphe**-which means "**writing**") gives the new code **"ηεαιφααοην".**

Section 3: Additional Results

In this section we will continue to use the Greek alphabets cipher codes with additional support from affine transformation, matrix transformation, digraph properties and knapsack problems to find new ciphertexts.

3.1 Affine Transformation

A transformation defined by C ≡ aP + b mod N and $P \equiv a'C + b' mod\, N$, where a & b are enciphering keys, "N" is number of Greek alphabets, “P” is plaintext and $a^{'} = a^{-1}\, mod\, N$ and $b^{'} = -\,a^{-1}b\, mod\, N$ [2].

3.2 Digraph

Considering two letters at a time is digraph. The corresponding numerical value is P = xN + y. Where, x -1st letter, y - 2nd letter, N – Number of alphabets, $C \equiv aP + b\, modN^2$. Here, as before “a” must have no common factor with N (which means it has no common factor with N^2)$P \equiv a^{'}C + b^{'}mod\, N^2$ and C = $x^{'}N + y^{'}$ then looking up the letters with numerical equivalents $x^{'}$ and $y^{'}$, Where$a^{'} = a^{-1}$ mod N^2 and $b^{'} = -\,a^{-1}b$ mod N^2 [2].

3.3 Enciphering Matrices

$$\text{Let } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$A^{-1} = \frac{1}{|A|}\, Adj\, A$$

$$= \frac{1}{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= D^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$$

C = AP is the enciphering formula,
P = $A^{-1}C$

Where, A is enciphering matrix
C is ciphertext
P is plaintext
$A^{-1}$is deciphering matrix

3.4 Knapsack Problem

For a given set of k integers $\{v_0, v_1, v_2, \dots, v_{k-1}\}$ and an integer v if there exist a k-bit integer n =$(\varepsilon_{k-1}\varepsilon_{k-2} \dots \varepsilon_2\varepsilon_1)$. Such that $\sum_{i=0}^{k-1} v_i\varepsilon_i = v$, then the problem is said to be Knapsack problem [2].

3.5 Example

We know that the word “**mathematics**” spelt as “**μαθηματικα**” (**mathimatika**) in Greek. Taking a = 7, b = 12, this word is enciphered as “**σνξησντφδν**” with N = 24 using affine transformation defined 3.1. We also prove the reverse process.

We know that, C = aP + b mod N

μ = 11, C = 7(11) + 12 mod 24
= 77 + 12 mod 24
= 89 mod 24 = 17
= σ

α = 0, C = 7(0) + 12 mod 24
= 12 mod 24 = 12
= ν

θ = 7, C = 7(17) + 12 mod 24
= 49 + 12 mod 24
= 61 mod 24 = 13
= ξ

η = 6, C = 7(6) + 12 mod 24
= 42 + 12 mod 24
= 54 mod 24 = 6
= η

μ = 11, C = 7(11) + 12 mod 24
= 77 + 12 mod 24
= 89 mod 24 = 17
= σ

α = 0, C = 7(0) + 12 mod 24
= 12 mod 24 = 12
= ν

τ = 18, C = 7(18) + 12 mod 24
= 126 + 12 mod 24
= 138 mod 24 = 18
= τ

ι = 8, C = 7(8) + 12 mod 24
= 56 + 12 mod 24
= 68 mod 24 = 20
= φ

κ = 9, C = 7(9) + 12 mod 24
= 63 + 12 mod 24
= 75 mod 24 = 3
= δ

α = 0, C = 7(0) + 12 mod 24
= 12 mod 24 = 12
= ν

Thereforethe plaintext “**μαθηματικα**” is enciphered as “**σνξησντφδν**” that is “**μαθηματικα**” → “**σνξησντφδν**”.

Reverse:
Find the plaintext to the ciphertext when N = 24, “**σνξησντφδν**”.

We know that, $P \equiv a^{'}C + b^{'}mod\, N$.Where $a^{'} = 7$ and $b^{'} = 12$

σ = 17, C = 7(17) + 12 mod 24
= 119 + 12 mod 24
= 131 mod 24 = 11
= μ

ν = 12, C = 7(12) + 12 mod 24
= 84 + 12 mod 24
= 96 mod 24 = 0
= α

ξ = 13, C = 7(13) + 12 mod 24
= 91 + 12 mod 24
= 103 mod 24 = 7
= θ

η = 6, C = 7(7) + 12 mod 24
= 49 + 12 mod 24
= 54 mod 24 = 6
= η

σ = 17, C = 7(17) + 12 mod 24
= 119 + 12 mod 24
= 131 mod 24 = 11
= μ

ν = 12, C = 7(12) + 12 mod 24
= 84 + 12 mod 24
= 96 mod 24 = 0
= α

τ = 18, C = 7(18) + 12 mod 24
= 126 + 12 mod 24
= 138 mod 24 = 18
= τ

φ = 20, C = 7(20) + 12 mod 24
= 140 + 12 mod 24
= 152 mod 24 = 8
= ι

δ = 3, C = 7(3) + 12 mod 24
= 21 + 12 mod 24

= 33 mod 24 = 9
= κ
v = 12, C = 7(12) + 12 mod 24
= 84 + 12 mod 24
= 96 mod 24 = 0
= α

Thereforethe ciphertext “**σνξησντφδν**” is deciphered as “**μαθηματικα**” that is “**σνξησντφδν**”→ “**μαθηματικα**”.

3.6 Example

We know that the word “**idea**” spelt as “**ιδεα**” (**idea**) in Greek. Taking Enciphering formula C = 7 P + 11 mod 576, this word is enciphered as “**κιεμ**”with N = 24 using digraph defined 3.2. We also prove the reverse process.
We know that P = xN + y and C ≡ aP + b mod N^2

“ιδ” = (8)(24) + 3
= 195
C = 7 (195) + 11 mod 576
= 1365 + 11 mod 576
= 1376 mod 576
C = 224
224 = 9 (24) + 8
C = (9) (8)
= “κι”
“εα” = (4) (24) + 0
= 96
C = 7 (96) + 11 mod 576
= 672 + 11 mod 576
= 683 mod 576
C = 107
107 = 4 (24) + 11
C = (4) (11)
= “εμ”

Thereforethe plaintext “**ιδεα**” is enciphered as “**κιεμ**” that is “**ιδεα**” → “**κιεμ**”.

Reverse:

We know that, C = $x^{'}N + y^{'}$ and $P \equiv a^{'}C + b^{'} mod\ N^2$

$a^{'}$ = 576 = 82 (7) + 2
7 = 3 (2) + 1
1 = 7 (1) – 3 (2)
= 7 (1) – 3 [1 (576) – 82 (7)]
= 247 (7)
$a^{'}$ = 247
$b^{'}$ = - 247 (11) mod 576
= - 413 mod 576
$b^{'}$ = 163
“κι” = (9)(24) + 8
= 224
P = 247 (224) + 163 mod 576
= 55328 + 163 mod 576
= 55491 mod 576
P = 195
195 = 8 (24) + 3
P = (8) (3)
= “ιδ”
“εμ” = (4) (24) + (11)
= 107
P = 247 (107) + 163 mod 576
= 26429 + 163 mod 576
= 26592 mod 576
P = 96
96 = 4 (24) + 0
C = (4) (0)
= “εα”

Thereforethe ciphertext“**κιεμ**” is enciphered as “**ιδεα**” that is “**κιεμ**”→ “**ιδεα**”.

3.7 Example

Using the enciphering matrices defined in 3.3, we find the plaintext to the ciphertext taking alphabets in columns. “**καρδια**” (**kardia**) (which means “**heart**”). We use the enciphering matrix A = $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ and N = 24 as “**τπσρρι**”.
We also prove the reverse process.
We know that, C = AP

$$C = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} \kappa & \rho & \iota \\ \alpha & \delta & \alpha \end{pmatrix}$$
$$= \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 9 & 16 & 8 \\ 0 & 3 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 18+0 & 32+9 & 16+0 \\ 63+0 & 112+24 & 56+0 \end{pmatrix}$$
$$= \begin{pmatrix} 18 & 41 & 16 \\ 63 & 136 & 56 \end{pmatrix}$$
$$= \begin{pmatrix} 18 & 17 & 16 \\ 15 & 16 & 8 \end{pmatrix}$$
$$C = \begin{pmatrix} \tau & \sigma & \rho \\ \pi & \rho & \iota \end{pmatrix}$$

Thereforethe plaintext “**καρδια**” is enciphered as “**τπσρρι**” that is “**καρδια**” → “**τπσρρι**” .

Reverse:

Use N = 24 and A = $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ to decipher “**τπσρρι**”.
We know that, C = AP
P = A^{-1}C
A^{-1} = $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$
D = 16 – 21 = -5 = 19
D^{-1} = -5 mod 24
= 19

$$A^{-1} = 19\begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$$
$$= \begin{pmatrix} 152 & -57 \\ -133 & 38 \end{pmatrix}$$
$$= \begin{pmatrix} 8 & -9 \\ -13 & 14 \end{pmatrix}$$
$$A^{-1} = \begin{pmatrix} 8 & 15 \\ 11 & 14 \end{pmatrix}$$

P = A^{-1}C

$$= \begin{pmatrix} 8 & 15 \\ 11 & 14 \end{pmatrix}\begin{pmatrix} 18 & 17 & 16 \\ 15 & 16 & 8 \end{pmatrix}$$
$$= \begin{pmatrix} 144+225 & 136+240 & 128+120 \\ 198+210 & 187+224 & 176+112 \end{pmatrix}$$
$$= \begin{pmatrix} 369 & 376 & 248 \\ 408 & 411 & 228 \end{pmatrix}$$
$$= \begin{pmatrix} 9 & 16 & 8 \\ 0 & 3 & 0 \end{pmatrix}$$
$$P = \begin{pmatrix} \kappa & \rho & \iota \\ \alpha & \delta & \alpha \end{pmatrix}$$

Thereforethe ciphertext “**τπσρρι**” is deciphered as “**καρδια**” that is “**τπσρρι**” → “**καρδια**”.

3.8 Example

Using the enciphering matrices defined in 3.3, we find the plaintext to the ciphertext taking alphabets in rows.

“**καρδια**” (**kardia**) (which means “**heart**”). We use the enciphering matrix A = $\begin{pmatrix}2 & 3\\7 & 8\end{pmatrix}$ and N = 24 as “**δαιπρρ**”. We also prove the reverse process.

We know that, C = AP

$$C = \begin{pmatrix}2 & 3\\7 & 8\end{pmatrix}\begin{pmatrix}\kappa & \alpha & \rho\\\delta & \iota & \alpha\end{pmatrix}$$

$$= \begin{pmatrix}2 & 3\\7 & 8\end{pmatrix}\begin{pmatrix}9 & 0 & 16\\3 & 8 & 0\end{pmatrix}$$

$$= \begin{pmatrix}18+9 & 0+24 & 32+0\\63+24 & 0+64 & 112+0\end{pmatrix}$$

$$= \begin{pmatrix}27 & 24 & 32\\87 & 64 & 112\end{pmatrix}$$

$$= \begin{pmatrix}3 & 0 & 8\\15 & 16 & 16\end{pmatrix}$$

$$C = \begin{pmatrix}\delta & \alpha & \iota\\\pi & \rho & \rho\end{pmatrix}$$

Thereforethe plaintext “**καρδια**” is enciphered as “**δαιπρρ**” that is “**καρδια**” → “**δαιπρρ**” .

Reverse:

Use N = 24 and A = $\begin{pmatrix}2 & 3\\7 & 8\end{pmatrix}$ to decipher “**δαιπρρ**”.

We know that, C = AP

P = A^{-1}C

A^{-1} = $\begin{pmatrix}2 & 3\\7 & 8\end{pmatrix}$

D = 16 – 21 = -5 = 19

D^{-1} = -5 mod 24

= 19

$$\mathrm{A}^{-1} = 19\begin{pmatrix}8 & -3\\-7 & 2\end{pmatrix}$$

$$= \begin{pmatrix}152 & -57\\-133 & 38\end{pmatrix}$$

$$= \begin{pmatrix}8 & -9\\-13 & 14\end{pmatrix}$$

$$\mathrm{A}^{-1} = \begin{pmatrix}8 & 15\\11 & 14\end{pmatrix}$$

P = A^{-1}C

$$= \begin{pmatrix}8 & 15\\11 & 14\end{pmatrix}\begin{pmatrix}3 & 0 & 8\\15 & 16 & 16\end{pmatrix}$$

$$= \begin{pmatrix}24+225 & 0+240 & 64+240\\33+210 & 0+224 & 88+224\end{pmatrix}$$

$$= \begin{pmatrix}249 & 240 & 304\\243 & 224 & 312\end{pmatrix}$$

$$= \begin{pmatrix}9 & 0 & 16\\3 & 8 & 0\end{pmatrix}$$

$$P = \begin{pmatrix}\kappa & \alpha & \rho\\\delta & \iota & \alpha\end{pmatrix}$$

Thereforethe ciphertext “**δαιπρρ**” is deciphered as “**καρδια**” that is “**δαιπρρ**” → “**καρδια**”.

3.9 Example

Using the knapsack defined in 3.4, we find the plaintext to the ciphertext “**ζωη**” (**zoe**) - “**life**” taking a = 17, b =18, m =61 and enciphering key {34, 51, 58, 11, 39}. We also prove the reverse process.

“ζ “= 5 = $(00101)_2$

= 0(34) + 0(51) + 1(58) + 0(11) + 1(39)

= 97

“ω” = 27 = $(11111)_2$

= 1(34) + 1(51) + 1(58) + 1(11) + 1(39)

= 193

“η” = 6 = $(00111)_2$

= 0(34) + 0(51) + 1(58) + 1(11) + 1(39)

= 108

Therefore the cipher is {97,193,108}.

Reverse:

We know that,

v = bc mod m

v = 18(97) mod 61

= 1746 mod 61= 38

v = 18(193) mod 61

= 3474 mod 61 = 58

v = 18(108) mod 61

= 1944 mod 61 = 53

To find the super increasing $\mathrm{bw_i} = \mathrm{v}$ and $\mathrm{av} = \mathrm{w_i}$

Therefore {34, 51, 58, 11, 39} mod 61 = {2, 3, 7, 15, 31} is a super increasing sequence.

v = 38, 31 ≤ 38 $\varepsilon_{4=1}$

15 > 7 $\varepsilon_{3=0}$

7 ≤ 7 $\varepsilon_{2=1}$

3 > 0 $\varepsilon_{1=0}$

2 > 0 $\varepsilon_{0=0}$

$(00101)_2 = \zeta$

v = 58, 31 ≤ 58 $\varepsilon_{4=1}$

15 ≤ 27 $\varepsilon_{3=1}$

7 ≤ 12 $\varepsilon_{2=1}$

3 ≤ 5 $\varepsilon_{1=1}$

2 ≤ 2 $\varepsilon_{0=1}$

$(11111)_2 = \omega$

v = 53, 31 ≤ 53 $\varepsilon_{4=1}$

15 ≤ 22 $\varepsilon_{3=1}$

7 ≤ 7 $\varepsilon_{2=1}$

3 > 0 $\varepsilon_{1=0}$

2 > 0 $\varepsilon_{0=0}$

$(00111)_2 = \eta$

Therefore the plaintext is “**ζωη**”.

References:

[1] Paul E. Gunnells, The mathematics of cryptology, Department of Mathematics and Statistics University of Massachusetts, Amherst, MA 01003.April 27, 2004.

[2] Koblitz, N., A course in number theory and cryptography. New York: Springer Verlag, 1987.

[3] Stu Schwartz, Cryptology for Beginners, Wissahickon HighAmbler, Pa 19002.

[4] Edward Schaefer, An introduction to cryptography and cryptanalysis, Santa Clara University.