

The Republic of Iraq

***Ministry of Higher Education and
Scientific Research***

University of Qadisiyah

***College of Computer Science and
Information Technology***

Department of Mathematics



Al Gebric Cryptography

***Research submitted to the Council of the Faculty of Computer Science and
Information Technology / Department of Mathematical Sciences / University
of Qadisiyah / as part of the requirements for obtaining a bachelor's degree***

Supervised by

Sahar Jafar

Done by

Naba'a Maitham Ni'ma

.Abstract

Cryptanalysis deals with the revers problem of devising ways to decipher an intercepted secret message without possessing the secret key used by the sender this is referred to as " breaking the code ". cryptography and cryptanalysis are the two main components of the science of cryptology

Introduction

Cryptography is the study of methods of transforming a secret message in such a way that it can be understood only by an authorized recipient who has been provided with secret key for deciphering it. If the message is intercepted by an unauthorized recipient (let us call him the Enemy); he should not be able to interpret it. Basically there are two ways in cryptography of transforming a message. One of them called transposition, is to rearrange the characters in the message according to some rule. The other method called substitution, is to replace each character by another according to some rule.

The general principle involved in the substitution method is to select a permutation f of the set of letters of the alphabet (in which the message is written) and replace each letter x in the message with $f(x)$, we refer to this permutation f as the key. Suppose we wish to send this message to friend:

ALGEBRA IS GREATFUN

Since we don't want the enemy to know this secret, we decide to send the message in a disguised form. Let us take f to be the permutation given by the table below for each letter x in the top row, $f(x)$ is the letter directly below x

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N F P R K S C E L A J Q G T B I M D H R X Z V Y U W

Replacing each letter x in the message with $f(x)$, and suppressing the blank spaces, we transform the original message to