MINI PROJECT

TITLE : IMPLEMENTATION OF PLAY-FAIR CIPHER ENCRYPTION AND DECRYPTION

Candidate ID: 104917

Table of Contents

List of Figures

List of Tables

CHAPTER 1

Play-Fair Cipher Encryption and Decryption in C Programming

1.1 Introduction

In many applications in the life, there is a need to transfer information from the sender to the receiver. When information is transmitted, care should be taken so that the information is not accessible to a third party. Also along with the explosive growth in computer systems and their interconnection via network has increased the dependence of both organizations and individuals on the information stored and communicated using these systems which intern has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Also the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security. Cryptography is the design of certain techniques for ensuring the secrecy and/or authenticity of information. Earlier the requirement of information security within an organization was primarily provided by physical and administrative means. But the concept of network security became quite evident with the introduction of computers and later with introduction of distributed systems. The need of cryptographic algorithm is to avoid threat to integrity confidentiality and availability.
There are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system: Symmetric Key Encryption and Asymmetric Key Encryption, the main difference between them is the relationship between the encryption and the decryption key. Symmetric Cipher Technique is also known as Conventional, Single key, Secret Key, One – key and classical encryption techniques. Practically it is impossible to decrypt the cipher text with the key that is unrelated to the encryption key.

1.2 Aim of the project

To provide a safe and secure communication channel for both the communicating parties, and keeping sensitive information away from any unauthorized third parties with malicious intent to read/ modify or destroy sensitive information.

1.3 Problem statement

In today’s electronic world, cryptology as a form of computer security and universal electronic connectivity, of viruses and hackers, of electronic fraud, there is indeed no time at which security does not matter.

Hence, it is becoming more and more important to computer users to keep their data safe at all times. As sometimes very crucial and sensitive information, information such as bank account passwords, secret conversations in the army during a war and many such scenarios, and this information can get to the wrong hands, like an unauthorized third person who is not a part of the communication.

1.4 Solution

Hence to tackle with such security attacks we can make use of cryptographic algorithms, which are used to encrypt messages and data to keep them safe and then made use to decrypt the message once it is received by the authorized receiver in the communicating channel.

One of the best-known early ciphers is the Play-fair system. Compared to more sophisticated data encryption techniques such as RSA or DES which involve complex computational steps, Play-fair ciphers are relatively less complex. From the computational and hardware point of view, more complex algorithms require more power consumption, which make them less attractive for use in wireless devices such as mobile phones, wireless sensor, etc. In contrast, Play-fair cipher, being comparatively simpler than their more complex counterparts, are low power consumption algorithms and therefore are suitable for data security in wireless applications.

1.5 Project Description

The Play-fair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

1.5.1 ENCRYPTION

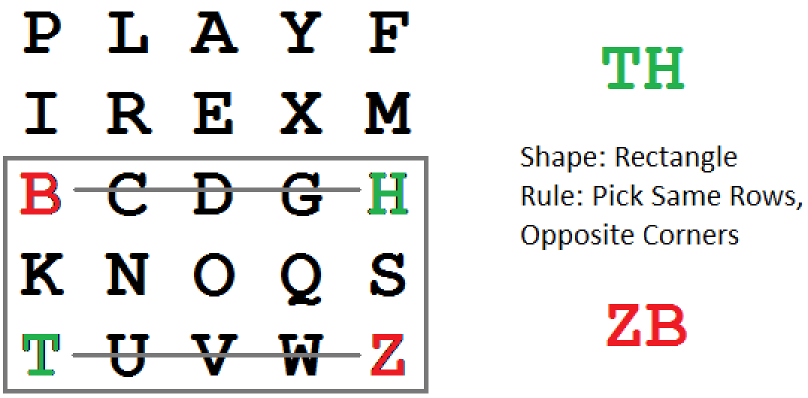
Plaintext is encrypted **two letters** at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as X, so that balloon would be treated as BA LX LO ON.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, AR is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, HS becomes BP and EA becomes IM (or JM, as the encipherer wishes).

1.5.2 DECRYPTION

Decryption procedure is same as the encryption algorithm, the keyword remains the same for encryption and decryption since this is a symmetric cipher. So the keyword is filled in the 5x5 matrix and the rest of the alphabets are filled in the matrix.

This time in decryption the cipher text is and used two letters at a time, and all the same rules followed to get the plaintext.



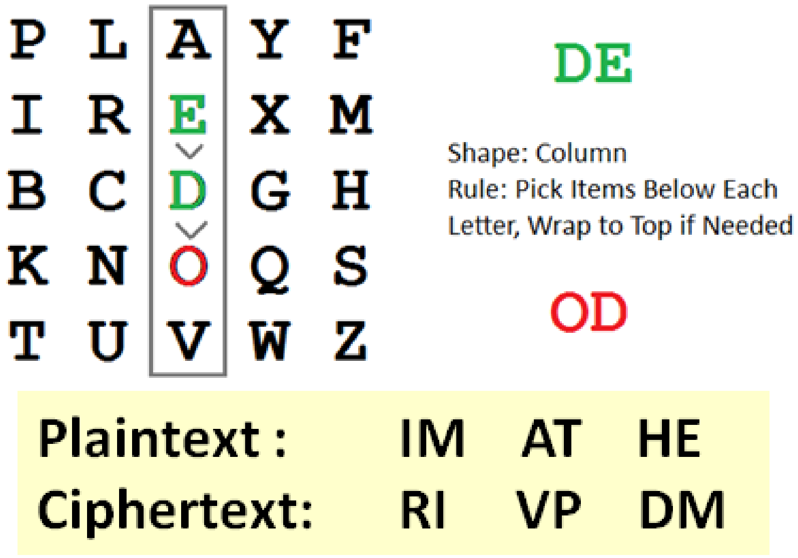
P	L	A	Y	F
I	R	E	X	M
B	~~C~~	~~D~~	~~G~~	H
K	N	O	Q	S
T	~~U~~	~~V~~	~~W~~	Z

TH

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

ZB

Fig 1.1: Example with letters in different row different column.



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

DE

Shape: Column
Rule: Pick Items Below Each
Letter, Wrap to Top if Needed

OD

Plaintext :	IM	AT	HE
Ciphertext:	RI	VP	DM

Fig 1.2: Example of Play-Fair Cipher with key word: PLAYFIREXM.

Examples:

1) Keyword: “KEYWORD”
Plaintext : “Why don’t you?”
WH YD ON TY OU
Ciphertext: “yieaesvkez”
YI EA ES VK EZ
2) Keyword: “KEYWORD”
Plaintext : “Come to the window ”
CO ME TO TH EW IN DO WX
Ciphertext: “lcnkzkvfyogqcebx”
LC NK ZK VF YO GQ CE BX

CHAPTER 2

Requirements

Software used: Code::blocks version 17.12

Operating System: Windows.

Header files required are:

1) `#include <stdio.h>` -> used to perform standard input and output functions.
2) `#include <stdlib.h>` -> used for standard library utilities.
3) `#include <string.h>` -> used to access all the string functions in the string library to make use of inbuilt functions of string for better coding.

For this project we need to understand and be thorough with the need and use of functions, how to create functions and how to call functions in C programming, followed by using different types of functions such as void functions or return type functions etc.

Also there is a need to be well verse with the in-built string functions that are available in the string library of the C language in the header file "#include<string.h>"

CHAPTER 3

Test Plan

3.1 Features to be tested

FEATURE	DESCRIPTION
To check if the plain text letters are correctly spilt in two letters.	The letters in pain text or cipher text have to be split into two letters exactly referred as a diagram according to algorithm.
If a matrix of 5x5 has been formed according to rules of the algorithm.	A matrix of 5x5 is formed and filled first with alphabets of the keyword and followed by the rest of the alphabets.
To check if repeated letters are replaced with X or O etc.	If the plain text consists of any repeated letters, then before forming a pair an extra alphabet like an X or O etc is added to avoid repetition in the cipher text with can be detected.

Table 3.1: Features to be tested.

CHAPTER 4

Test cases

TEST CASE ID	SCENARIO	DATA/INPUT
1	Checking if the plain text letters are split exactly in a pair (diagram/two letter).	1. MONKEY MO NK EY 2. SYSTEM SY ST EM
2	To check if repeated letters in data is replaced with X or O etc.	1. BALLOON BA L**X** LO ON
3	Test for large keyword.	1. Indian Premier League 2. Joint implementation opportunities
4	Check for cases where two letters are in same row/column.	
5	Checking if the 5x5 matrix is filled first with keyword and followed by leftover alphabets.	
6	Testing for various random inputs	1. Keyword: Monarchy Plain text: Balloon Cipher text: ibsupman

Table 4.1 Test cases.

CHAPTER 5

Expected Results

TEST CASE ID	RESULT TO BE EXPECTED
1	Keyword: “MONARCHY “ Plain text: “MONKEY “ Letters split as follows: MO NK EY Cipher text: “NORGGC”
2	Keyword: “MONARCHY” Pain text: “BALLOON “ Letters split as follows: BA LX LO ON Cipher text: “IBSUPMAN”
6	Keyword: “KEYWORD” Plaintext : “COME TO THE WINDOW ” CO ME TO TH EW IN DO WX Cipher text:“LCNKZKVFYOGQCEBX”

Table 5.1: Expected results.

References

[1] Noaman, Salam. (2017), “*Adaptive playfair cipher Crypto algorithm.”*

[2] Khan, Salman. (2015), ”*Design and Analysis of Playfair Ciphers with Different Matrix Sizes*”. International Journal of Computing and Network Systems. 3. 117 - 122. 10.12785/ijcnt/030305.

[3] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.4325&rep=rep1&type=pdf

[4] Choudhary, Jitendra & Ravindra, Kumar & Gupta, & Singh, Shailendra. (2013). “*A GENERALIZED VERSION OF PLAY FAIR CIPHER.”,* COMPUSOFT: International Journal of Advanced Computer Technology.