Computer Security

Mini Project – Playfair and Caesar Ciphers (web)

By student: Abdallah Mamdouh Mohamed Alhaddad
Abdelrahman Khaled Ahmedfouad
Arafa Arafa Abd El-Mawgod
Amr Khaled Eid Ali
Youssef Ahmed Abbas
Mina samy alfons

Presented to: Dr. El Sheshtawy
T.A. Heba Osama
T.A. Aya Khaled

Chapter 1: Introduction

1. Introduction:

With the increasing development of computer and communications technology growth and increasing needs and development of information systems security. The problem of security must be approached with greater caution. With the development of computer and communication technologies have developed numerous tools to protect files and other information. A set of tools, procedures, policies and solutions to defend against attacks are collectively referred to as computer network security. It is necessary above all to define and learn about the concepts of attack, risk, threat, vulnerability and asset value. During the design and implementation of information systems should primarily take into account a set of measures to increase security and maintenance at an acceptable level of risk. In any case, there is a need to know the risks in the information system. Sources of potential security problems are challenges and attacks, while the risk relates to the probable outcome and its associated costs due to occurrence of certain events. There are numerous techniques help protect your computer: cryptography, authentication, checked the software, licenses and certificates, valid authorization... This paper explains some of the procedures and potential threats to break into the network and computers as well as potential programs that are used. Guidance and explanation of these programs is not to cause a break-in at someone else's computer, but to highlight the vulnerability of the computer's capabilities.

Chapter 2: Classical Encryption Techniques

2. Classical Encryption Techniques:

There are two basic building blocks of all encryption techniques: substitution and transposition.

2.1 Substitution Techniques:

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. Ex: Caesar cipher, Playfair cipher, Polyalphabetic ciphers, Vigenère cipher

2.2 Transposition Techniques:

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. Ex: Rail fence, Row Transposition Ciphers

2.1.1 Playfair Cipher:

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In Playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

2.1.1.1 The Playfair Cipher Encryption Algorithm:

- The Algorithm consists of 2 steps:

i. Generate the key Square (5×5):

The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I. The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

ii. Algorithm to encrypt the plain text:

The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. For example:

Plaintext: "ME"

Encrypted Text: CL

Encryption: M >>> C

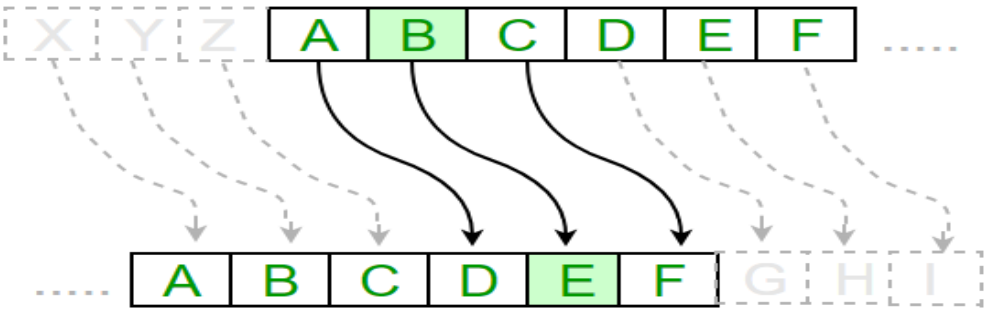
E >>> L

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

2.1.2 Caesar Cipher:

Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials. Thus, to cipher a given text we need an integer value, known as shift which indicates the number of positions each letter of the text has been moved down. The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

- **Encryption Phase with shift (n):** **$E_n(x)=(x+n) \bmod 26$**
- **Decryption Phase with shift (n):** **$D_n(x)=(x-n) \bmod 26$**



2.1.2.1 Algorithm for Caesar Cipher:

A String of lower-case letters, called Text.

An Integer between 0-25 denoting the required shift. For example:

Plaintext: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Shift: **23**

Cipher: **XYZABCDEFGHIJKLMNOPQRSTUVW**

Chapter 3: Implementation

3. Implementation:

3.1 The programming languages used:

HTML (Hypertext Markup Language):

is the most basic building block of the Web. It defines the meaning and structure of web content. Other technologies besides HTML are generally used to describe a web page's appearance/presentation (CSS) or functionality/behavior (JavaScript). "Hypertext" refers to links that connect web pages to one another, either within a single website or between websites. Links are a fundamental aspect of the Web. By uploading content to the Internet and linking it to pages created by other people, you become an active participant in the World Wide Web.HTML uses "markup" to annotate text, images, and other content for display in a Web browser.

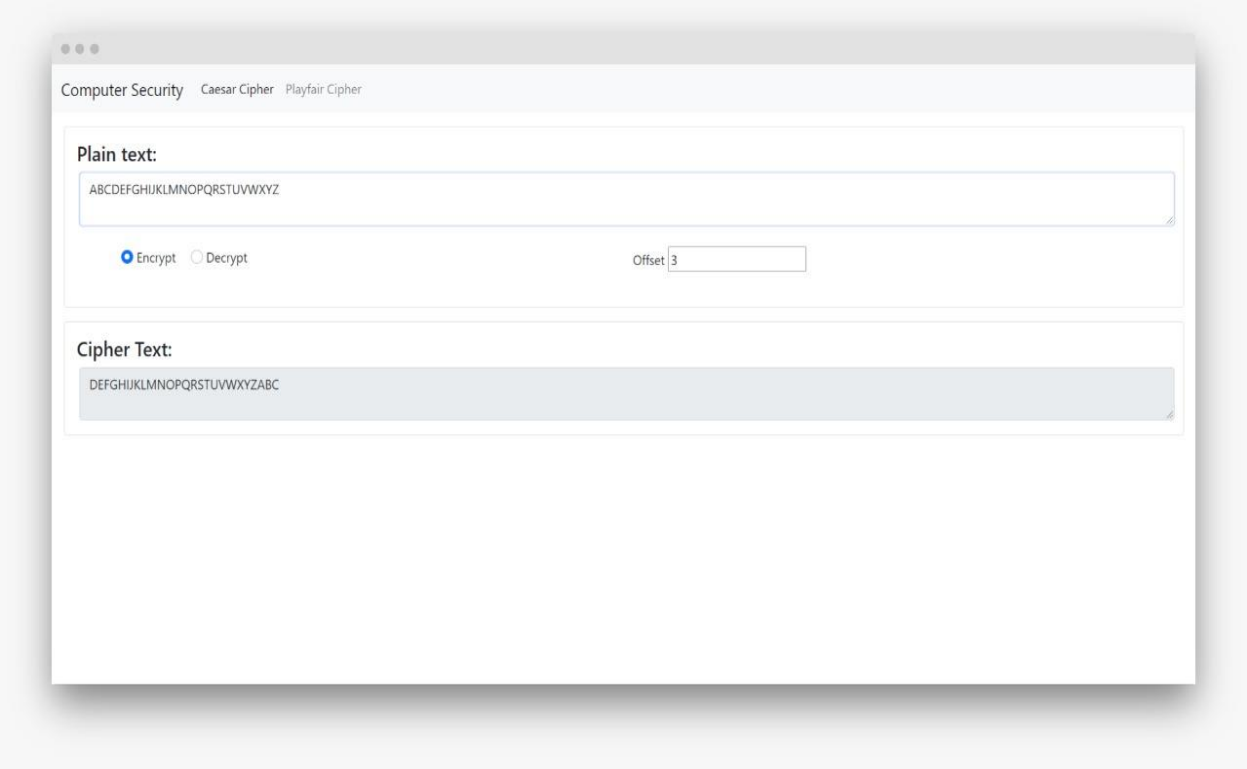
CSS (Cascading Style Sheets):

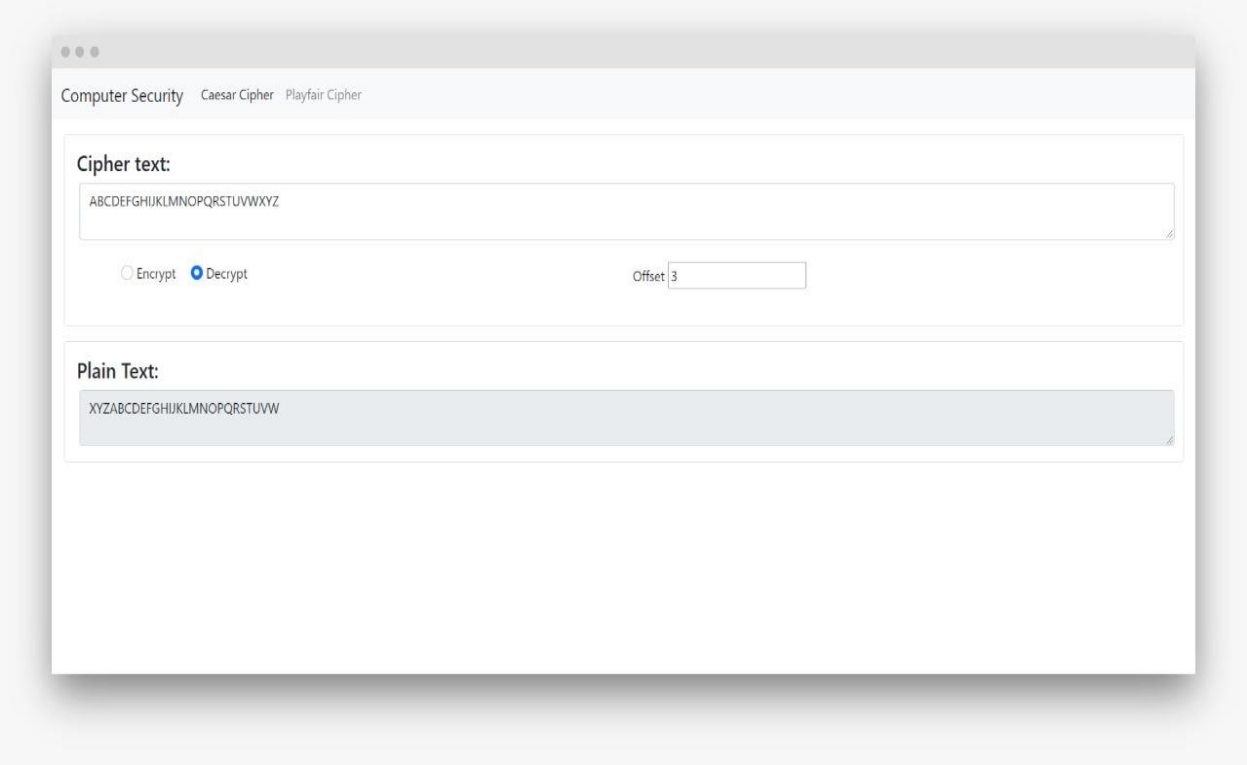
is a simple design language intended to simplify the process of making web pages presentable.CSS handles the look and feel part of a web page. Using CSS, you can control the color of the text, the style of fonts, the spacing between paragraphs, how columns are sized and laid out, what background images or colors are used, layout designs, variations in display for different devices and screen sizes as well as a variety of other effects.CSS is easy to learn and understand but it provides powerful control over the presentation of an HTML document. Most commonly, CSS is combined with the markup languages HTML or XHTML

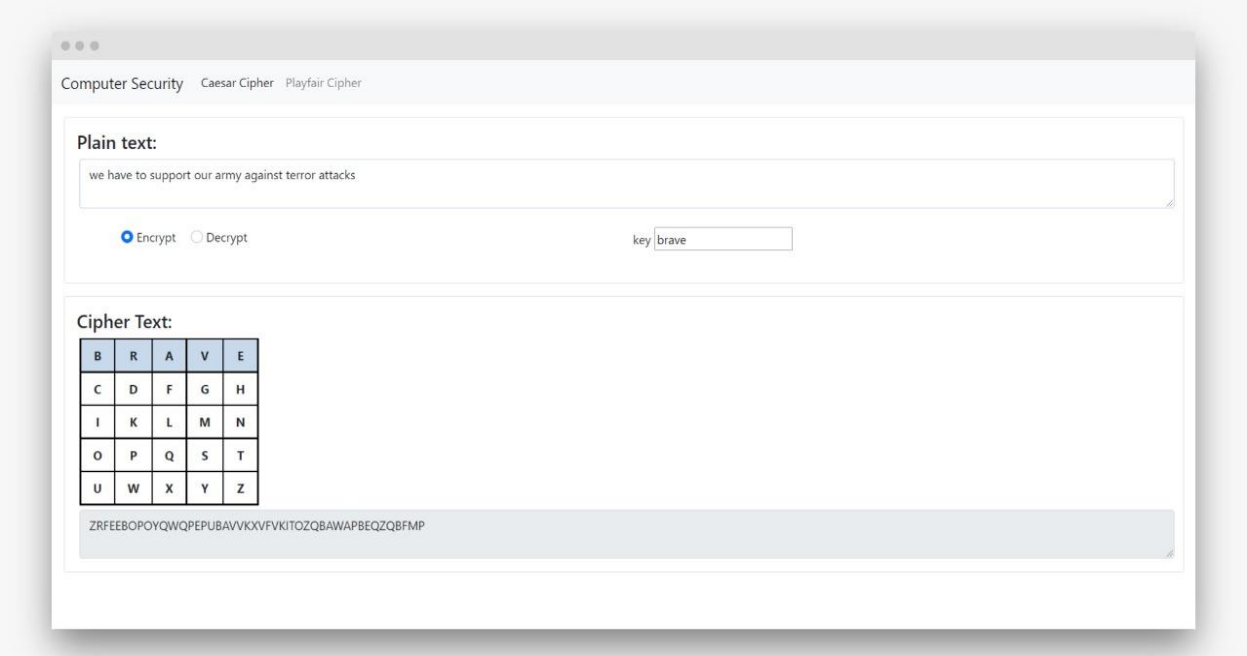
JS (JavaScript):

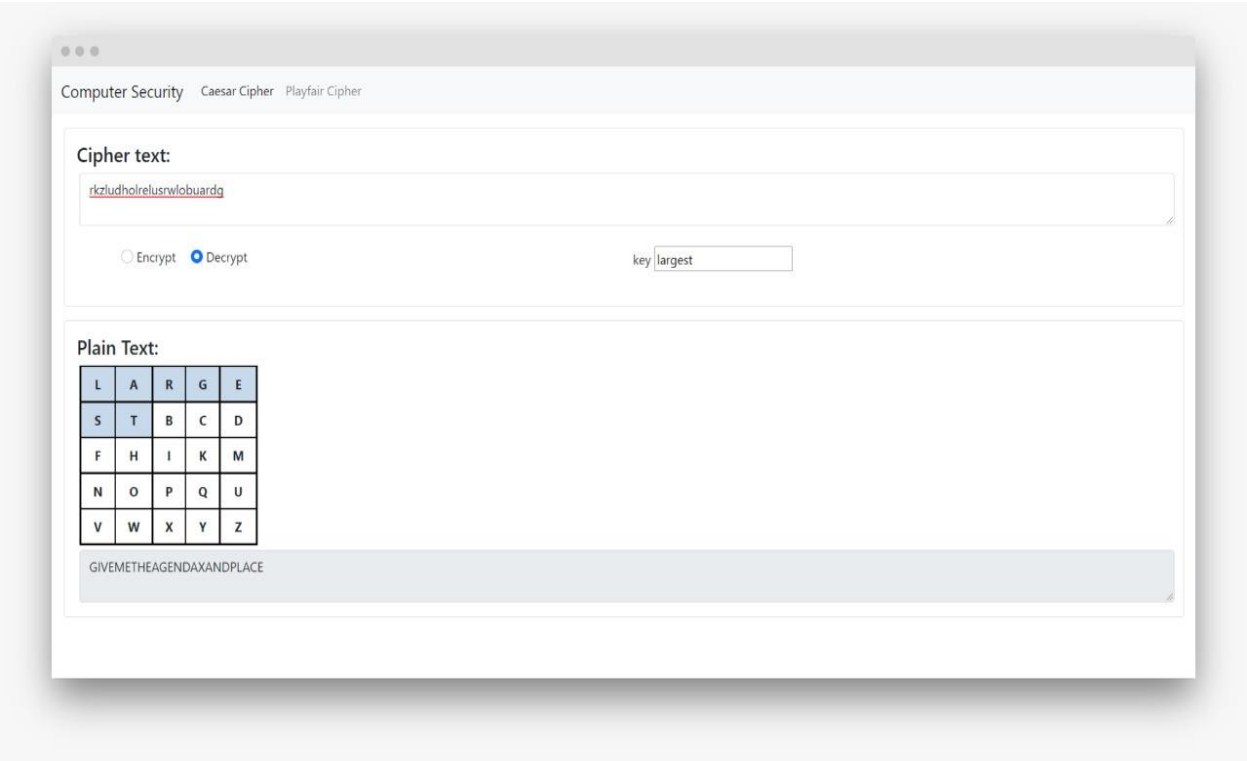
is a dynamic programming language that's used for web development, in web applications, for game development, and lots more. It allows you to implement dynamic features on web pages that cannot be done with only HTML and CSS.

3.2 GUI (graphical user interface):









Link: https://github.com/AbdallahAlhaddad/playfair-caesar-cipher