

IS493 Tutorial – Project I (Defensive)- Report Template



Group#:.....

Student ID (Leader): 441101833

Student Name: FARES SALEM

Student ID: 441102081

Student Name: MESHAL ALSUBAYHIN

Student ID: 441102031

Student Name: MOHAMMED ALFOUZAN

Student ID: 441101992

Student Name: MOHAMMED ALQHTANI

Student ID: 439102359

Student Name: MOHAMMED ALSALEH

1. Cipher Overview

The HTML code in this implementation includes input areas for the plaintext, ciphertext, and key matrix(2x2). The user can enter the needed values, and the encryption and decryption operations are handled by the corresponding JavaScript functions.

The encrypt () function accepts as input the plaintext and key matrix, conducts Hill cipher encryption, and shows the resulting ciphertext. If the plaintext is unusually long, it is padded with a "x" character. To get the encrypted characters, convert the characters to numeric values (char1 and char2), multiply them with the key matrix, and take modulo 26. Finally, the ciphertext is shown.

The decrypt () function accepts as input the ciphertext and key matrix, conducts Hill cipher decryption, and displays the decrypted text.

2. Used Data Structure

We used a list data structure representing a matrix and to be specific we used two-dimensional list that made it easier to manipulate the matrix elements.

3. Error handling

We dealt with two types of errors: if the determinant is equal to 0, the code will prompt an alert message, and if the length of the matrix isn't four, the code will also prompt an alert message.

4.Code

Encoding

```
function encrypt() {
    var plaintext = document.getElementById("plaintext").value.toLowerCase().replace(/[^a-z]/g, "");
    var keyInput = document.getElementById("key").value;
    var key = parseKeyMatrix(keyInput);

    if (plaintext.length % 2 !== 0) {
        plaintext += "x"; // Pad plaintext if the length is odd
    }

    var ciphertext = "";
    for (var i = 0; i < plaintext.length; i += 2) {
        var char1 = plaintext.charCodeAt(i) - 97; // Convert to 0-based index
        var char2 = plaintext.charCodeAt(i + 1) - 97; // Convert to 0-based index

        var encryptedChar1 = (key[0][0] * char1 + key[0][1] * char2) % 26;
        var encryptedChar2 = (key[1][0] * char1 + key[1][1] * char2) % 26;

        ciphertext += String.fromCharCode(encryptedChar1 + 97); // Convert back to character
        ciphertext += String.fromCharCode(encryptedChar2 + 97); // Convert back to character
    }

    document.getElementById("encryptedText").innerHTML = "Ciphertext: " + ciphertext;
}
```

Decoding

```
function decrypt() {
  var ciphertext =
document.getElementById("ciphertext").value.toLowerCase().replace(/^[a-z]/g, "");
  var keyInput = document.getElementById("key1").value;
  var key = parseKeyMatrix(keyInput);
  var inverseKey = getInverseKey(key);

  var decryptedText = "";
  for (var i = 0; i < ciphertext.length; i += 2) {
    var char1 = ciphertext.charCodeAt(i) - 97; // Convert to 0-based index
    var char2 = ciphertext.charCodeAt(i + 1) - 97; // Convert to 0-based index

    var decryptedChar1 = (inverseKey[0][0] * char1 + inverseKey[0][1] * char2) % 26;
    var decryptedChar2 = (inverseKey[1][0] * char1 + inverseKey[1][1] * char2) % 26;

    decryptedText += String.fromCharCode(decryptedChar1 + 97); // Convert back to
character
    decryptedText += String.fromCharCode(decryptedChar2 + 97); // Convert back to
character
  }

  document.getElementById("decryptedText").innerHTML = "Decrypted Text: " +
decryptedText;
}
```

SOME HELPING FUNCTIONS

```
function parseKeyMatrix(keyInput) {
  var key = [];
  var values = keyInput.toLowerCase().replace(/^[a-z]/g, "").split("");

  if (values.length !== 4) {
    alert("Invalid key matrix. Please enter a 2x2 matrix with 4 alphabetical
characters.");
    return;
  }

  key.push([values[0].charCodeAt(0) - 97, values[1].charCodeAt(0) - 97]);
  key.push([values[2].charCodeAt(0) - 97, values[3].charCodeAt(0) - 97]);

  return key;
}
```

```

function getInverseKey(key) {
    // Calculate the determinant of the key matrix
    var determinant = (key[0][0] * key[1][1] - key[0][1] * key[1][0] + 26) % 26;

    // Find the modular multiplicative inverse of the determinant
    var determinantInverse=-1;
    for (var i = 1; i < 26; i++) {
        if ((determinant * i) % 26 == 1) {
            determinantInverse = i;
            break;
        }
    }

    // If no inverse exists, return null
    if (determinantInverse == -1) {
        alert("The key matrix is not invertible. Please enter a valid key matrix.");
        return null;
    }

    // Calculate the adjugate matrix
    var adjugateMatrix = [
        [key[1][1], -key[0][1]],
        [-key[1][0], key[0][0]]
    ];

    // Calculate the inverse key matrix using modular arithmetic
    var inverseKey = [];
    for (var row = 0; row < 2; row++) {
        inverseKey[row] = [];
        for (var col = 0; col < 2; col++) {
            inverseKey[row][col] = ((adjugateMatrix[row][col] * determinantInverse) % 26 + 26)
% 26;
        }
    }

    return inverseKey;
}

```

Our Example we used the plaintext: *information security* and key: *bdcb*

Enciphering

Encryption

Plaintext:

information security

Key Matrix:

bdcb

Encrypt

Ciphertext:

vdebyoftyepsckettfnjpt

Decryption

Ciphertext:

vdvybuftyepskktfnjpt

Key Matrix:

bdc b

Decrypt

Decrypted Text:
informationsecurityx

Instructor's example

9	4
5	7

Plaintext: CHIFFREDEHILLX

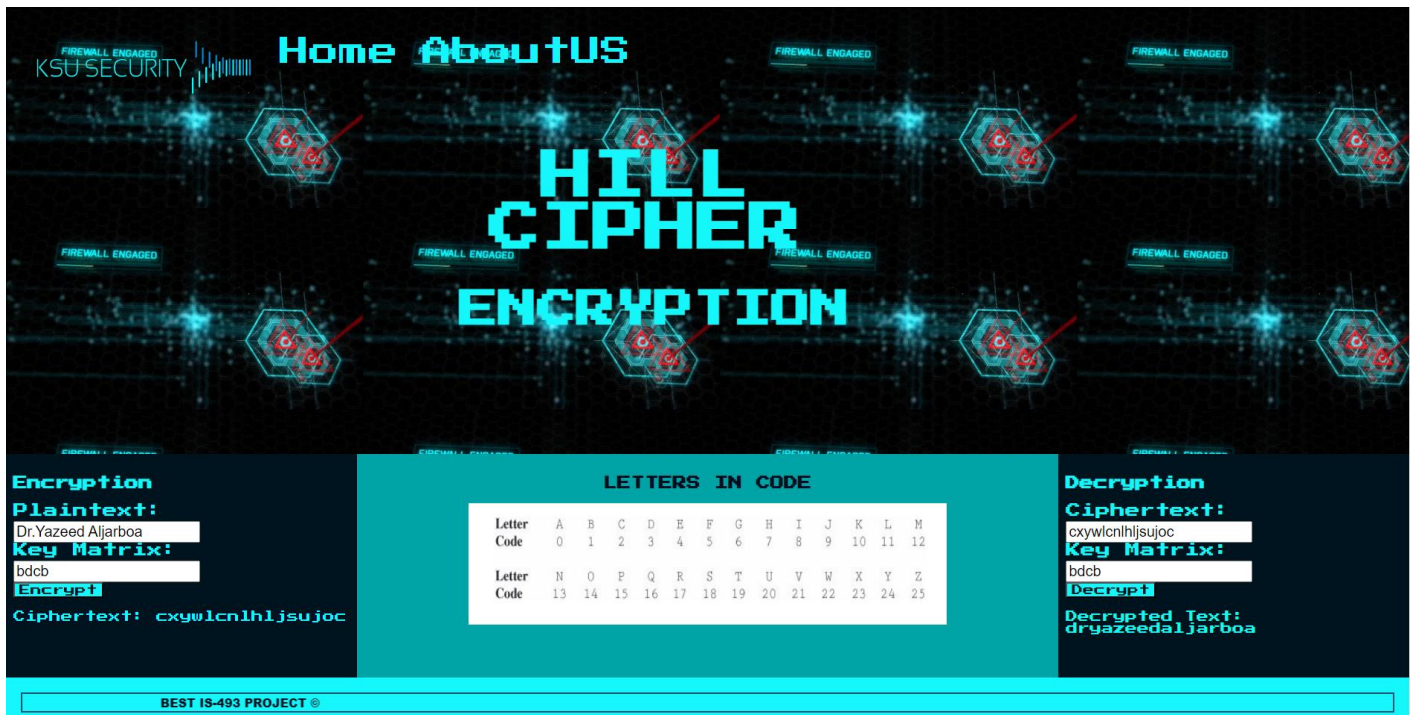
Enciphering

```
Encryption
Plaintext:
CHIFFREDEHILLX
Key Matrix:
jefh
Encrypt
Ciphertext: uhoxjowpmmniji
```

Deciphering

```
Decryption
Ciphertext:
uhoxjowpmmniji
Key Matrix:
jefh
Decrypt
Decrypted Text:
chiffredehillx
```


SYSTEM SCREENSHOTS



SYSTEM CODE

1-main.html

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>HILL CIPHER</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://fonts.googleapis.com/css2?family=Press+Start+2P&display=swap"
rel="stylesheet">
<script src="hill.js"></script>
<style>
* {
  box-sizing: border-box;
}

body {
  font-family: Arial, Helvetica, sans-serif;
}

.topnav {
  overflow: hidden;
  margin: 0;
  padding: 0;
  list-style-type: none;
}

.topnav li a {
  float: left;
  display: block;
  color: #15f7fa;
  text-align: center;
  padding: 20px 16px;
  margin: bottom;
  text-decoration: none;
  float: left;
  font-size: 40px;
  font-family: "Press Start 2P";
}

.topnav a:hover {
  background-color: #00141f;
  color: #15f7fa;
  float: left;
}

h2, h1{
  color: #15f7fa;
```

```

}
div.fixed{
position: relative;
bottom: 20;
left: 590px;
width: 500px;
font-family: "Press Start 2P";
}

/* Style the header */
.header {
padding: 30px;
text-align: center;
font-size: 35px;
background-image:url(giphy.gif);
padding: 20px;
margin:0px;
height: 600px;
}

/* Create three unequal columns that floats next to each other */
.column {
float: left;
padding: 10px;
height: 300px; /* Should be removed. Only for demonstration */
}

/* Left and right column */
.column.side {
width: 25%;
}

/* Middle column */
.column.middle {
width: 50%;
}

/* Clear floats after the columns */
.row:after {
content: "";
display: table;
clear: both;
}

/* Style the footer */
.footer {
background-color: #15f7fa;

```

```

padding: 20px;
text-align: center;
margin: 0px;
}

/* Responsive layout - makes the three columns stack on top of each other instead of next
to each other */
@media (max-width: 600px) {
  .column.side, .column.middle {
    width: 100%;
  }
}
</style>
</head>
<body>
  <div class="header">
    <ul class="topnav">
      <li><a href="main.html"></a></li>
      <li><a href="main.html">Home</a></li>
      <li><a href="about.html">AboutUS</a></li>
    </ul>
    <div class="fixed">
      <h1>HILL CIPHER</h1>
      <h2>ENCRYPTION</h2>
    </div>
  </div>

  <div class="row">
    <!-- encryption part -->
    <div class="column side" style="background-color:#00141f;">
      <h3 style="color: #15f7fa;font-family:'Press Start 2P';">Encryption</h3>
      <label for="plaintext" style="color: #15f7fa;font-family:'Press Start 2P';font-size:
20px;">Plaintext:
      <input type="text" id="plaintext" style="font-size: 20px;" >
    </label>
    <br>
    <label for="key" style="color: #15f7fa;font-family:'Press Start 2P';font-size: 20px;">Key
Matrix:
    <input type="text" id="key" placeholder="Only (2x2)" style="font-size: 20px;"></label>
    <br>
    <button onclick="encrypt()" style="font-size: 15px;font-family: 'Press Start 2P';
background-color: #15f7fa;color: #00141f;">Encrypt</button>
    <p id="encryptedText" style="color: #15f7fa;font-family:'Press Start 2P';"></p>
  </div>

  <div class="column middle" style="background-color:#00a4a6;">
    <h3 style="color: #000f1f;font-family:'Press Start 2P';text-align: center;">LETTERS IN
CODE</h3>

```

```

    <div align="center">
      
    </div>
  </div>

  <!-- decryption part -->
  <div class="column side" style="background-color:#00141f;">
    <h3 style="color: #15f7fa;font-family:'Press Start 2P';">Decryption</h3>
    <label for="ciphertext" style="color: #15f7fa;font-family:'Press Start 2P';font-size:
20px;">Ciphertext:
    <input type="text" id="ciphertext" style="font-size: 20px;"></label>
    <br>
    <label for="key1" style="color: #15f7fa;font-family:'Press Start 2P';font-size:
20px;">Key Matrix:
    <input type="text" id="key1" placeholder="Only (2x2)" style="font-size: 20px;"></label>
    <br>
    <button onclick="decrypt()" style="font-size: 15px;font-family: 'Press Start 2P';
background-color: #15f7fa;color: #00141f;">Decrypt</button>
    <p id="decryptedText" style="color: #15f7fa;font-family:'Press Start 2P';"></p>

  </div>
</div>

<div class="footer">
  <marquee direction="right"
behavior="alternate"
style="border:#234E70 2px SOLID;color: #000f1f; font-size: medium;font-weight: 900;">
BEST IS-493 PROJECT &copy;
  </marquee>
  <h1 style="color: #000f1f;padding: 0px;margin: 0px;"> MADE WITH  IN KSU</h1>
</div>

</body>
</html>

```

2-about.html

```

<!DOCTYPE html>
<html lang="en">
<head>
<title>ABOUT US</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://fonts.googleapis.com/css2?family=Press+Start+2P&display=swap"
rel="stylesheet">
<script src="hill.js"></script>

```

```

<style>
* {
  box-sizing: border-box;
}

body {
  font-family: Arial, Helvetica, sans-serif;
}

.topnav {
  overflow: hidden;
  margin: 0;
  padding: 0;
  list-style-type: none;
}

.topnav li a {
  float: left;
  display: block;
  color: #15f7fa;
  text-align: center;
  padding: 20px 16px;
  margin: bottom;
  text-decoration: none;
  float: left;
  font-size: 40px;
  font-family: "Press Start 2P";
}

.topnav a:hover {
  background-color: #00141f;
  color: #15f7fa;
  float: left;
}

h2, h1{
  color: #15f7fa;
}

div.fixed{
  position: relative;
  bottom: 20;
  left: 590px;
  width: 500px;
  font-family: "Press Start 2P";
}

/* Style the header */
.header {
  padding: 30px;

```

```

text-align: center;
font-size: 35px;
background-image:url(giphy.gif);
padding: 20px;
margin:0px;
height: 600px;
}

/* Create three unequal columns that floats next to each other */
.column {
float: left;
padding: 10px;
height: 300px; /* Should be removed. Only for demonstration */
}

/* Left and right column */
.column.side {
width: 25%;
}

/* Middle column */
.column.middle {
width: 50%;
}

/* Clear floats after the columns */
.row:after {
content: "";
display: table;
clear: both;
}

/* Style the footer */
.footer {
background-color: #15f7fa;
padding: 20px;
text-align: center;
margin: 0px;
}

/* Responsive layout - makes the three columns stack on top of each other instead of next
to each other */
@media (max-width: 600px) {
.column.side, .column.middle {
width: 100%;
}
}
</style>

```

```

</head>
<body>
  <div class="header">
    <ul class="topnav">
      <li><a href="main.html"></a></li>
      <li><a href="main.html">Home</a></li>
      <li><a href="about.html">AboutUS</a></li>
    </ul>
    <div class="fixed">
      <h1>INSTRUCTOR</h1>
      <h2>Dr.Yazeed Aljarboa</h2>
    </div>
  </div>

  <div class="row">

    <div class="column side" style="background-color:#00141f;">
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #15f7fa;">
SUBJECT:INFROMATION SECURITY-IS 493</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #15f7fa;"> CLASS
SECTION:30586</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #15f7fa;"> LAB
SECTION:30587</p>
    </div>

    <div class="column middle" style="background-color:#00a4a6;">
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #00141f;"> FARES SALEM-
441101833</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #00141f;"> MOHAMMED
ALFOUZAN-441102031</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #00141f;"> MESHAL
ALSUBAYHIN-441102081</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #00141f;"> MOHAMMED
ALQHTANI-441101992</p>
      <p style="font-size: 20px;font-family:'Press Start 2P';color: #00141f;"> MOHAMMED
ALSALELH-439102359</p>
    </div>

    <div class="column side" style="background-color:#00141f;">
      
    </div>
  </div>

```



```
<div class="footer">
  <marquee direction="right"
    behavior="alternate"
    style="border:#234E70 2px SOLID;color: #000f1f; font-size: medium;font-weight: 900;">
    BEST IS-493 PROJECT &copy;
  </marquee>
  <h1 style="color: #000f1f;padding: 0px;margin: 0px;"> MADE WITH  IN KSU</h1>
</div>

</body>
</html>
```