

MID PROJECT REVIEW REPORT

CrypticalEnigma CTF Gamestation

PROJECT TITLE	CRYPTICAL CTF
PROJECT DESCRIPTION	Cryptographic CTFs by generating a unique CTF flag code for each solved challenge. Crptical CTF can run it in a special configuration that allows Capture-the-Flag (CTF) events to be used. This will bring some extra motivation and fun competition to a security training or workshop for the participants.
PROJECT MEMBERS	IT17185394 – Dissanayake D.M.K.H. IT18108750 – Aththanayaka A.M.R.E.
COMMENCEMENT DATE	JULY,2020
SCHEDULED END DATE	OCTOMBER,2020

Video Link - <https://mysliit.sharepoint.com/:f:/s/Cryptical-CTF2020/Epwt81vXuH5Ai86WBTBXztwB9Q85oWD-KM1oxCppSd9cEQ?e=9lla8g>

SUMMARY OF PROGECT

Cryptical is an educational remote base platform for learning and practicing offensive and defensive coding. Cryptical system will be introduced the banking and financial sector employees. Basically it includes set of guidelines and applications for all vulnerabilities and attacks which exist various encryption system (symmetric and asymmetric), Digital signatures, Message authentication codes and certified encryption systems.

Our main objective in this project is to offer the banking and finance sector employees who want to learn and practice cryptography, to play for crypto tasks and to test their knowledge for cryptography. Employees Cryptical Assessment supervised and conducted by the IT professional in the company, Cryptography techniques have long been used in the banking industries to ensure the security of monetary transactions including the security of **ATM cards transaction, passwords, electronic commerce and other transactions**. Each attack is complemented by example of “Capture the Flag” competitions and their own notes. People that are already familiar can use Cryptical system as a tool to solve challenges based on a particular vulnerability. The project is aimed at bridging the gap between theoretical and applied cryptography by analyzing how different Cryptical systems work their internals the conception mathematics and analytical skills etc.

Cryptical domain cover the ten CTF challenges and sub tasks. Also Cryptical system provides the group base and individually assessments for the employees.

Challengers	Task Duration(min)
1.Block Ciphers	90min
2.RSA Encryption	90min
3.Message Authentication Code (MAC)	60min
4.Discrete Logarithm Problem	60min
5.ElGamal Encryption	60min
6.Authenticated Encryption	60min
7.Elliptic Curves	30min
8.Digital Signatures	30min
9.Identification	30min
10.Define Key Exchange	30min
Total Task Duration	9 hour

AUDIENCE OF THE PROJECT

- Our system will be introduced the banking and financial sector employees. Because Cryptography techniques have long been used in the banking industries to ensure the security of monetary transactions including the security of ATM transactions, passwords, electronic commerce and other transactions. Our main objective in this project is to offer the banking and finance sector employees who want to learn and practice cryptography, to play for crypto tasks and to test their knowledge for cryptography. Employees Cryptical Assessment supervised, conducted by the IT professional in the company.

TOOLS AND TECHNIQUES ARE USED IN THE PROJECT

- IDE (Integrated development environment)
 - eclipse - Eclipse is an environment for integrated development used in computer programming. It includes a base workspace and an extensible environment customization plug-in framework. And very powerful development environment for java
- apache server
 - Apache Tomcat – it is best production ready web container. Also a web server mainly for web development projects
- Language
 - java, css, jsp, html, js
- Evaluation
 - Web based online game station platform.

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

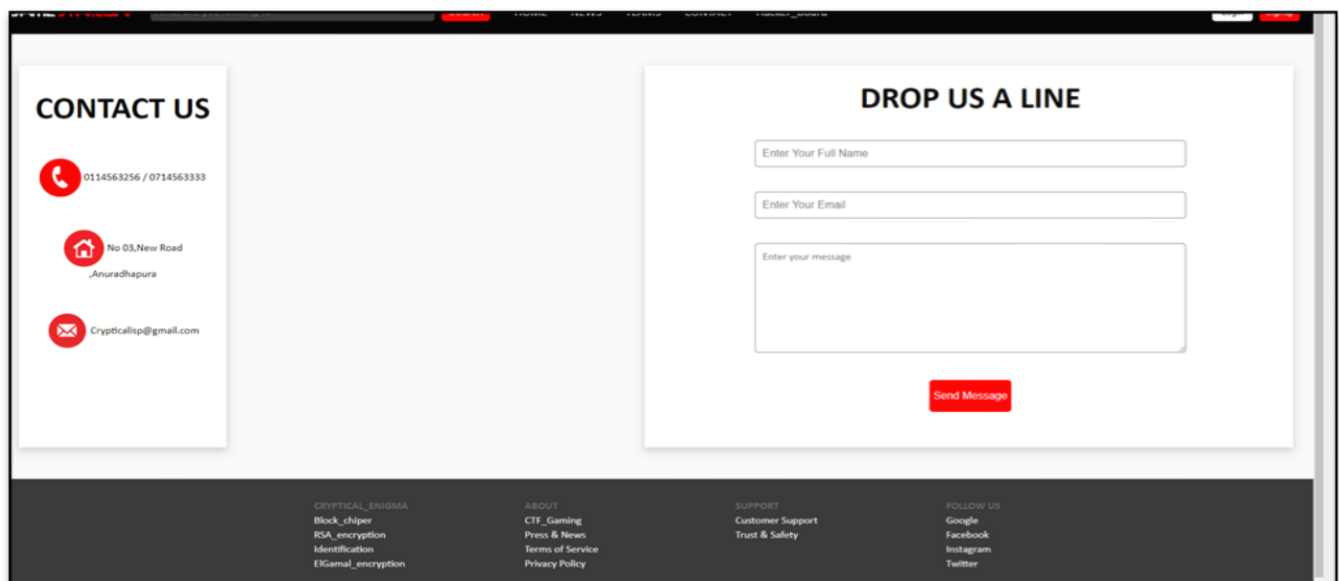
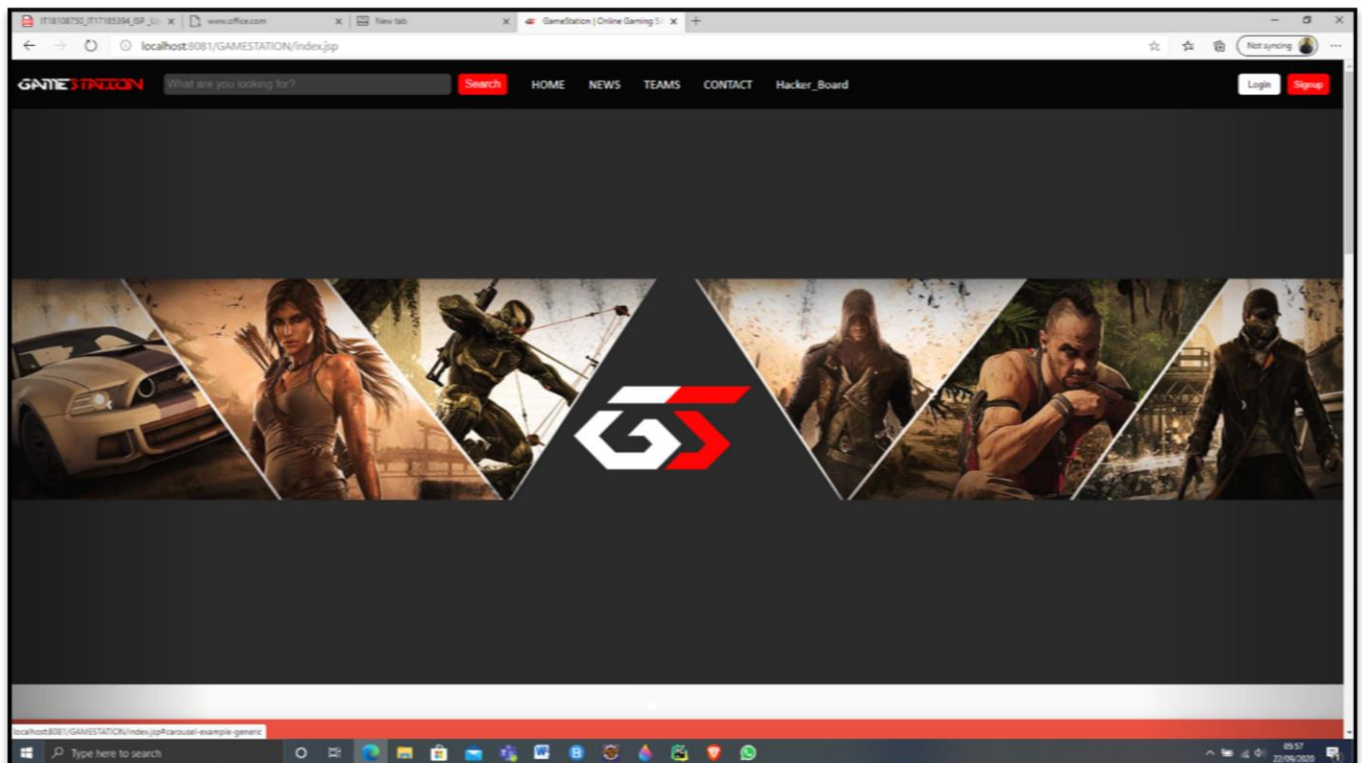
SUMMARY OF PROGECT PROGRASS

Elements	Include Sub Elements	Complete Percentage
.Home page	Search bar,login,singup Challengers, background About,contact,Teams, Hacker board, News (header & footer)	90%
.News page	Updated CTF news and include the trial videos	90%
Teams page	Team member details, Players trial videos & customer care details	90%
Contact Us	Message ,Phone, Address	90%
.Hacker Board	Team members time duration Members Scores & Analysis Details	65%
Challengers Levels.	Three levels are completed out of ten.	40%
Login	CTF players details	90%
Sign Up	CTF players details	90%
Profile	CTF players details	90%
Other Elements		60%
Project Complete Percentage		65%

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

SCREENSHOTS OF THE ENVIRONMENT IN THE PROJECT



MID PROJECT REVIEW REPORT

CRYPTICAL CTF

Register

First Name: sam

Last Name: sliva

Gender: ☒ Male ☐ Female

Country: United States

Gaming Platform: PlayStation

Username: kik123

Password: *****

Confirm Password: *****

Email Address: ispcryptical@gmail.com

Passwords Match!

Reset Submit

GAMESTATION What are you looking for? Search PLAY NOW NEWS CONTACT Cryptical01 Logout

kalpa Hashan
Cryptical01

ID	P1001
Platform	PC
From	Sri Lanka
Gender	Male
Type	user

Edit Profile

Favourites

Oops! Your list is empty.
But it doesn't have to be.

Join our play area now and add CTF to your favourites.
Keep Playing!

Play Now

CRYPTICAL_ENIGMA
Block_chiper
RSA_encryption
Identification
Cryptical_Enigma

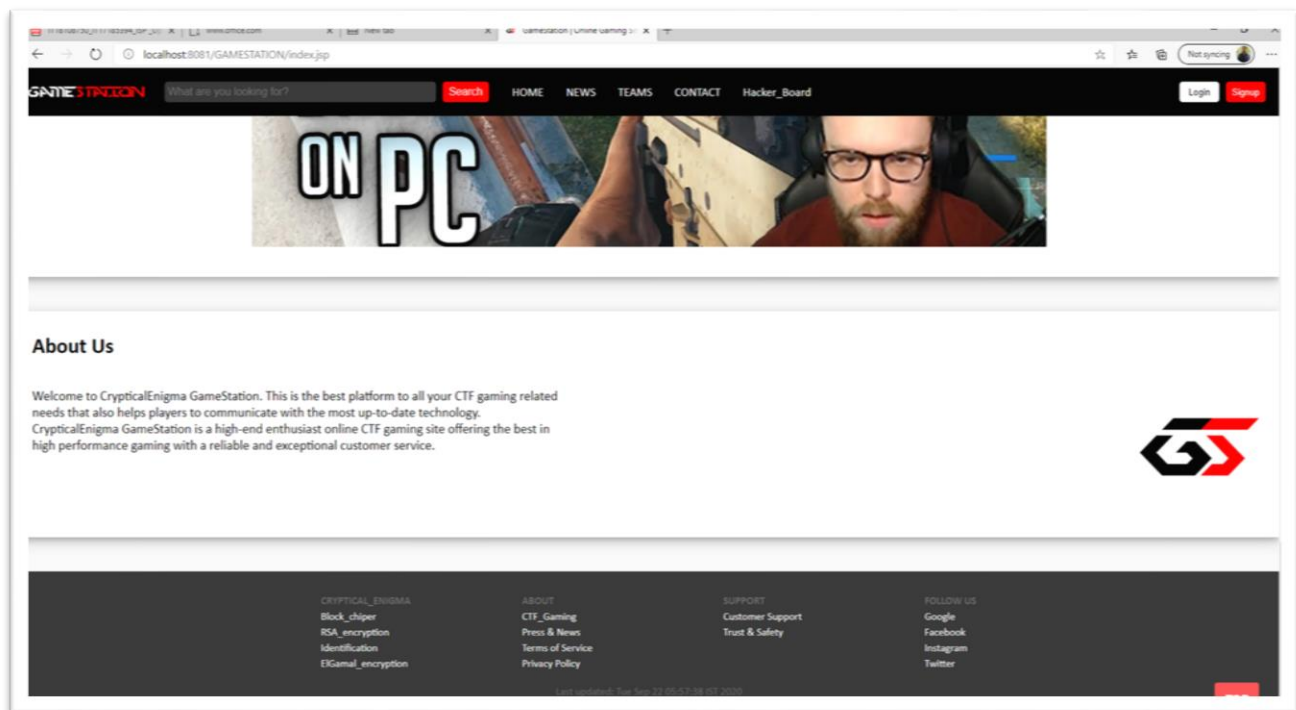
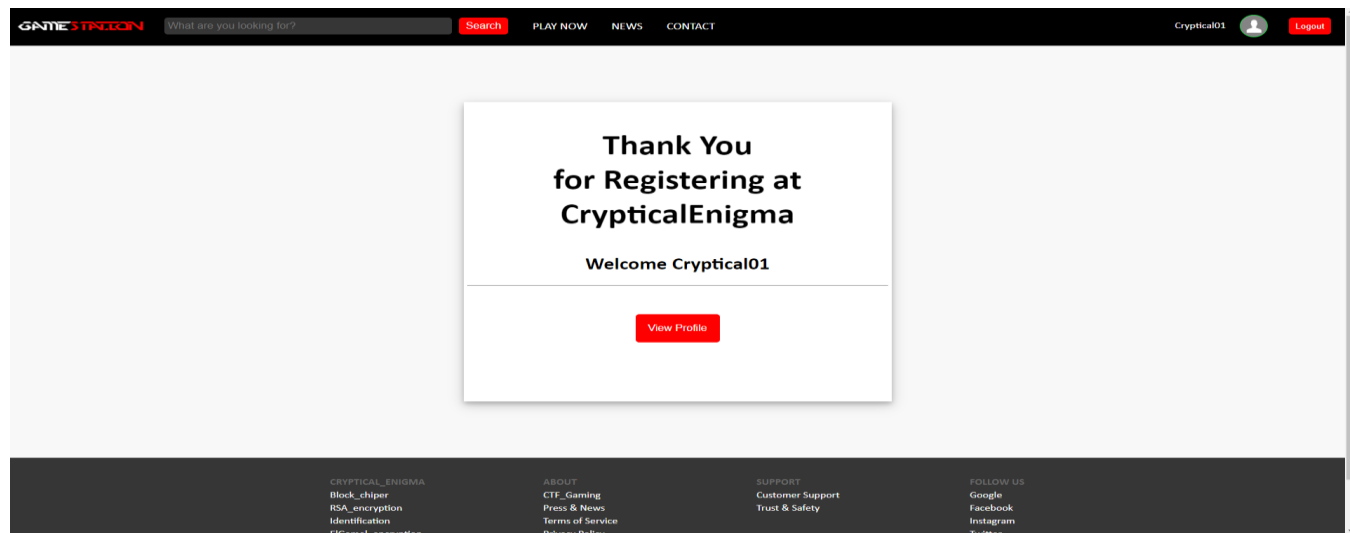
ABOUT
CTF_Gaming
Press & News
Terms of Service
Privacy Policy

SUPPORT
Customer Support
Trust & Safety

FOLLOW US
Google
Facebook
Instagram
Twitter

MID PROJECT REVIEW REPORT

CRYPTICAL CTF



In our CTF event infrastructure;

We implement the “HACKER BOARD” to manages the statues of the CTF includes:

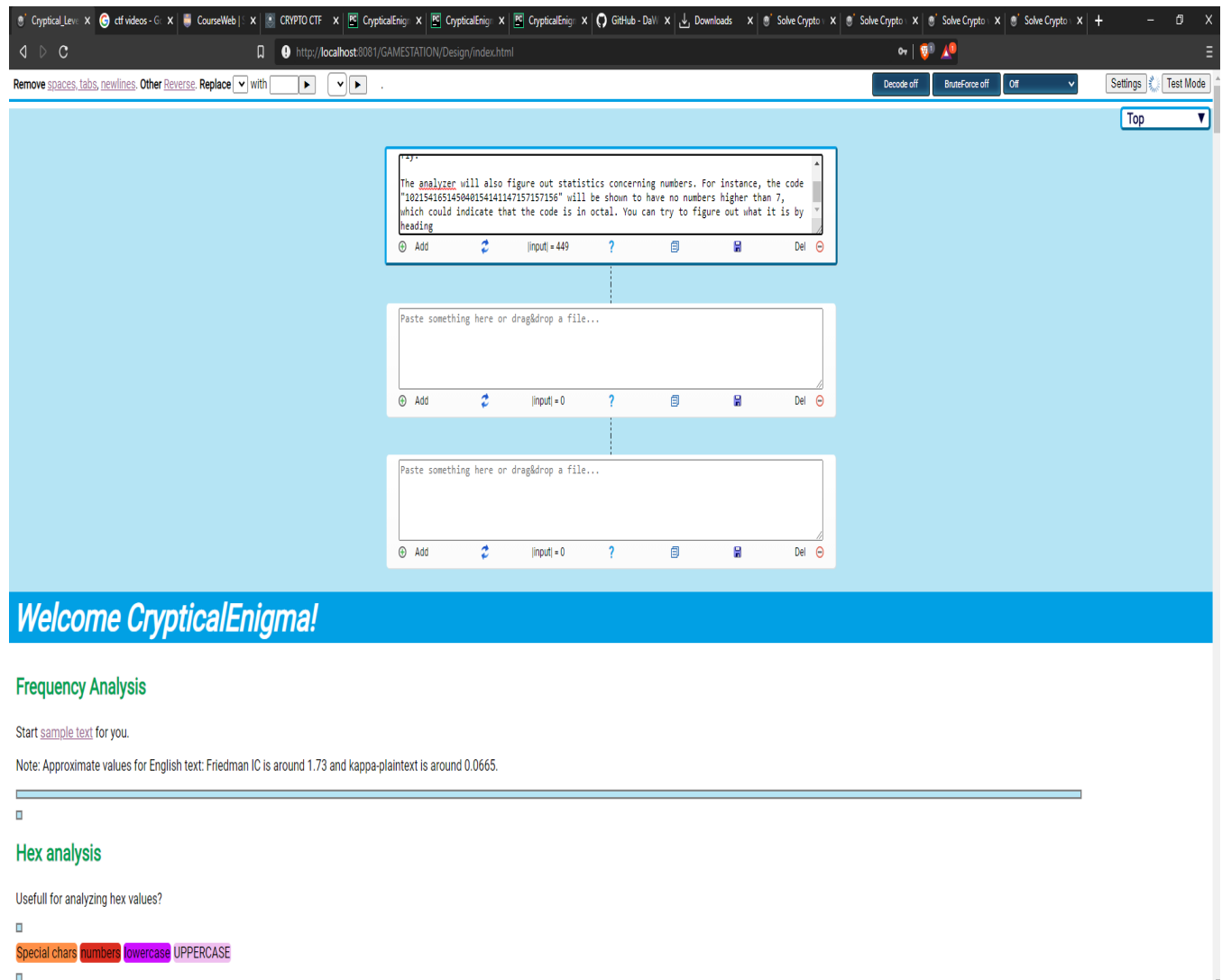
- teams and users’ registration dialogs

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

- User management board / teams participating in the event
 - The open / solved hacking challenges and their score value challenge board
 - Which challenges have already been solved and by whom
- In addition to that each participant have their own CRYPTICAL ENIGMA CTF instance.

Challengers Output



Remove spaces, tabs, newlines. Other Reverse Replace with . Decode off BruteForce off Off Settings Test Mode

Top

The analyzer will also figure out statistics concerning numbers. For instance, the code "102154165145040154141147157157156" will be shown to have no numbers higher than 7, which could indicate that the code is in octal. You can try to figure out what it is by heading

Paste something here or drag&drop a file...

Paste something here or drag&drop a file...

Welcome CrypticalEnigma!

Frequency Analysis

Start [sample text](#) for you.

Note: Approximate values for English text: Friedman IC is around 1.73 and kappa-plaintext is around 0.0665.

Hex analysis

Usefull for analyzing hex values?

Special chars numbers lowercase UPPERCASE

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

Remove spaces, tabs, newlines Other Reverse BinInverse BinReverse Replace 7 ▾ ▼ with ▸ ▶ Low : 4 < 16.7 @ input reverse() baconian()

Run online toolset? /autoexec/play/runonline/ Decode on Bruteforce on Almost Certain ▾ Settings Test Mode

Top ▾

```

'''
.....
.....
.....
.....
.....
'''

```

⊕ Add ↺ |input| = 280 ? 📄 🗑 Del ⊖

```

input.inverse()

01110100001010000101001011100110110001100110000101100110101010010111001101101101101
1011100110110001111001011001101110110010011010000110010101011011101101100110
010101110010110100001100000101101000110000101110011001010110110111011011011
1101100100

```

⊕ Add ↺ |input| = 280 ? 📄 🗑 Del ⊖

```

input.binary()

GWOP W ZORIEH HVOZ, BITP RO HEXTIP QVH GL ZUL RYH, FVRRO WIO ENOP, FIQ OPTACKRIC, NDMH'C
HXOXMNDI EPUTROP HR GL CXVL VKEP, GXCXOPMPO, GXCXBWTPG, GXCVCPOCJHRQ GACC VHRTXCLXQW,
XH GWQZ YL CVMZ GP OREI...

```

⊕ Add ↺ |input| = 202 ? 📄 🗑 Del ⊖

xor(password) xor(secret) xor(pass) xor(test) xor(code) xor(key) xor(cyberlympics) xor(token) xor(wgcode) rem_all_spaces&newl Pivot over password ▾ ▶

```

input.xor(test) - Desperate Guess

32'ST2S..7;<T(*)=I$B=1#T&"$9.= "ST4*<T"?T.T.22T&X?%&&4$==4$1,"#ZT#$%T4#
,&+&8 T9!$9$K$""#+@($.$3'&3559&E4BT&+"")$9 , #2T"+479""##95"XT"+763$ $4_T3=-
4#;7(1&E4,7&$'97'9&!8%=$XT=>7%="=5(57??)T355&K?:ZK

```

⊕ Add ↺ |input| = 202 ? 📄 🗑 Del ⊖

Remove spaces, tabs, newlines Other Reverse, BinInverse, BinReverse Replace 1 with [] Low - 5 < 29 6 @ input spiritDVD() reverse() Run online lookup2 (auto search for fair voice)

Decoded on BruteForce on Almost Certain

Add |input= 280 ? Del

input.binary()

```
GHQP W ZORIH HYOZI, RITP RO HXZTP QYH GL ZML RYHI, FVBRQ WIQ EXOP. FWQ OPTXXCRIC, MDWHI'C  
WVOXHDI' ZIPTRGP HR GL CXVL XKEP. GXCHDPHIPQ, GXCBBHTPO, GXCYIQPOCHRAXX GXCC VIRTHQCRLQXI,  
XN QXQI'H CVRZ GP QRZL...
```

Add |input= 202 ? Del

input.xor(test) - Desperate Guess

```
32"$T25.;7<t(")=IS&1#T&"S9.= "$T4"<t"?T.23$<X?#%&&45#=#451,"#2T#$%T4#  
,&k&=&.T9!S9S&#=""#0(S.53"!3SS9E4BT&""$P, "2T"+7D"#95"XT"+763$ $4_T3=@.  
+4#;7(1&%E4,7&S"97"9&!8%=$XT->T&="<S(5777)T35&87;ZZK
```

Add |input= 202 ? Del

dnfkmglkglkjffherfghgvjhvbv

Add |input= 30 ? Del

Input.playfairLookup() - Unknown

dnfkmglkglkjffherfghgvjhvbv

Add |input= 30 ? Del

Paste something here or drag&drop a file...

Add |input= 0 ? Del

input.bin_7bit_ascii() - Desperate Guess

```
x?^_^/<^ y~?QnC=uoc@_IV(e=c</>/g"ByBTR0o]BXko&(NE-BAut=c-o
```

Add |input= 60 ? Del

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

```
14 public class ContactService implements IContactService {
15
16     public void addContact(Contact contact) {
17
18         String addContactQuery = "INSERT INTO contact VALUES(?,?,?,?)";
19
20
21         try {
22             // add data to contact table
23             PreparedStatement ps = DBConnection.getDBconnection().prepareStatement(addContactQuery);
24
25             ps.setString(1, contact.getMessageID());
26             ps.setString(2, contact.getName());
27             ps.setString(3, contact.getEmail());
28             ps.setString(4, contact.getMessage());
29
30             ps.executeUpdate();
31
32         } catch (ClassNotFoundException | SQLException e) {
33
34             e.printStackTrace();
35         }
36     }
37
38
39     public void deleteMessage(String messageID) {
40
41         String deleteMessageQuery = "DELETE from contact WHERE MessageID = ?";
42
43
44         try {
45             PreparedStatement ps = DBConnection.getDBconnection().prepareStatement(deleteMessageQuery);
46
47             ps.setString(1, messageID);
48
49             ps.executeUpdate();
50
51
52         } catch (ClassNotFoundException | SQLException e) {
53             // TODO Auto-generated catch block
54             e.printStackTrace();
55         }
56     }
57
58
59     // retrieve contact from DB
60     public ArrayList<Contact> getMessages(){
61
62         ArrayList<Contact> contactList = new ArrayList<Contact>();
63
64         String getMessagesQuery = "SELECT * FROM contact";
```

```
3 public class User {
4
5     private String userID;
6     private String firstName;
7     private String lastName;
8     private String gender;
9     private String country;
10    private String platform;
11    private String userName;
12    private String password;
13    private String email;
14    private String type = null;
15    public boolean valid;
16
17
18    public void setUserID(String userID) {
19        this.userID = userID;
20    }
21
22    public String getUserID() {
23        return this.userID;
24    }
25
26    public void setFirstName(String firstName) {
27        this.firstName = firstName;
28    }
29
30    public String getFirstName() {
31        return this.firstName;
32    }
33
34    public void setLastName(String lastName) {
35        this.lastName = lastName;
36    }
37
38    public String getLastName() {
39        return this.lastName;
40    }
41
42    public void setGender(String gender) {
43        this.gender = gender;
44    }
45
46    public String getGender() {
47        return this.gender;
```

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

```
9<html>
10<head>
11
12<%
13    response.setHeader("Cache-Control", "no-cache, no-store, must-revalidate");
14
15    User user = (User) session.getAttribute("currentSessionUser");
16
17    String confirm = (String) request.getAttribute("confirmString");
18
19    String confirmAddOrRem = (String) request.getAttribute("confirm");
20
21    ArrayList<String> arrayList = new ArrayList<String>();
22    IGameService iGameService = new GameServiceImpl();
23
24    if(user == null){
25
26        response.sendRedirect("login");
27    }
28
29    %>
30
31    <% if(user !=null) { %>
32
33    <title> <%=user.getUserName()%> | GameStation </title>
34
35    <% } %>
36
37<style>
38
39    h1{
40        color:black;
41        text-align: center;
42        font-size: 30px;
43        margin: 0px;
44    }
45
46    body{
47
48        margin: 0px;
49    }
50
51    .mainArea{
52        width: auto;
53        min-height: 700px;
54        margin-top: 100px;
55    }
56
57    .sideBar{
58        width: 260px;
59        height: 560px;
```

MID PROJECT REVIEW REPORT

CRYPTICAL CTF

```
17
18
19     .mainImage{
20         width: auto;
21         text-align: center;
22         height: 500px;
23         background-image: url(images/banner.jpg);
24         background-size: cover;
25         background-repeat: no-repeat;
26         background-position: center center;
27         margin-top: 70px;
28     }
29
30     .gamers{
31         width: auto;
32         text-align: center;
33         color: white;
34         background-color: #e74c3c;
35         box-shadow: 0 4px 8px 0 rgba(0, 0, 0, 0.2), 0 6px 20px 0 rgba(0, 0, 0, 0.19);
36         height: auto;
37         margin-top: 50px;
38         margin-bottom: 50px;
39         padding: 40px;
40     }
41
42     .subContent{
43         background-size: contain;
44         background-repeat: no-repeat;
45         background-position: center center;
46         transition: transform 0.1s;
47     }
48
49     .subContent:hover{
50         transform: scale(1.1);
51     }
52
53     .gamers a{
54         transition: color 0.2s;
55     }
56
57     .gamers a:hover{
58         color: #FFB900;
59     }
60
61     .about{
62         width: auto;
63         height: 300px;
64         text-align: left;
65         background-color: white;
66         box-shadow: 0 4px 8px 0 rgba(0, 0, 0, 0.2), 0 6px 20px 0 rgba(0, 0, 0, 0.19);
67         margin-top: 50px;
68         margin-bottom: 50px;
69         padding: 20px;
70         padding-top: 10px;
71     }
72
73     .aboutContent{
74         width: 800px;
75         height: 200px;
76         font-size: 20px;
```