Jaypee institute of information technology,noida

2011

**The Cipher Machine -Hitchhiker’s Guide to Cryptography**

Web Minor project

SUBMITTED BY-

Sumit Nangia(9103531)

Arihant Banthia(9103548)

Ayush Jain(9103553)

Batch-B-5

Phase One Report

TABLE OF CONTENTS

ACKNOWLEDGEMENT …………………….……………………………………………..3

ABSTRACT………………...………..……………………………………………………....4

ANALITICAL REVIEW……………………………………..…………………….……….

1. SOURCES USED…………..…………………………………………………………...5

1.1.VIEW……………………….……………………………………………………………7

1.2. CONTRIBUTION………….………………………….………………………………...8

REQUIRMENT ANALYSIS AND DESIGN………………………………………………...

2.0. REQUIRMENTS………………………………………………………………………...9

2.1.USE CASE DIAGRAMS.…………………………….………………………………….11

2.2CLASS DIAGRAMS………..…………………………………………………………….15

2.3.UML……………………………………………………………………………………….23

2.4.ACTIVITY DIAGRAM………………..………………………………………………….24

2.5.STRUCTURE DIAGRAM…………………………………………………..……………27

2.6.STATE DIAGRAMS………………………………………………………...……………28

2.7.ER DIAGRAMS………………………………………………………………..…………29

2.8.SEQUENCE DIAGRAMS…………………………………………………..……………31

ALGORITHMS……………………………………………………………………………………

3.0.ALGO USED………………………………………………………………………………..32

DESIGN VIEW……………..…….………………………………………………………………..

4.0. ALL DESIGNS………………………………………………………………………….....35

MAPING WITH SOFTWARE ENGINEERING…………………………………………………

5.0.DETAILED REQUIRMENT ENGEERING……………………………………………….37

5.1.PROCESS MODAL USED…………………………………………………………………39

TEST CASES…………………………………………………………………………………..40

CONCLUSION AND FUTURE WORK……………………………………………………….42

WORK DIVIDATION…………………………………………………………………………..43

BIBLIOGRAPHY……………………………………………………………………………….44

**ACKNOWLEDGEMENT**

Our first experience of project has been successful, thanks to the support staff of many friends & colleagues with gratitude. We wish to acknowledge all of them. However, we wish to make special mention of the following-:

First of all we are thankful of our project guide **Mrs. Mukta Goyal** under whose guideline we were able to complete our project. We are wholeheartedly thankful to her for giving us his valuable time & attention & for providing us with a systematic way for completing our project in time.

We must make special mention of our project in charge for their co-operation & assistance in solving the technical problems. We would also wish to express our gratitude to our lab mentor & all lab maintenance staff for proving us assistance in various problems encountered during course of our project.

We are also very thankful to our faculty who gave us an opportunity to present this project.

SUMIT NANGIA

ARIHANT BHANTIA

AYUSH JAIN

**ABSTRACT**

The process of learning is changing and evolving continuously. The place of black board is taken by the projectors; books have turned into e-books. A very convenient way which has evolved over time is to teach anybody through internet. We are developing a website related to the e learning which teaches the concepts of cryptography.

E-learning is about information, communication, education and training. Regardless of how trainers categorize training and education, the learner only wants the skills and knowledge to do a better job or to answer the next question from a customer.

**Cryptography** is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

This website would consist of complete explanation ofcryptography through tutorials, slides, videos, questions, answers and other web learning based features. Beside this for making it interesting it would also have quizzes and puzzles based of cryptographic theme. Login feature would help user to see his/her profile. This website thus consists of application of cryptography as well.

**SOURCES USED FOR FORMULATION**

We studied several months for the e learning and cryptography. We read many research papers and books for the related topic. We search many related sites and blogs for e learning and cryptography. Some of them are listed below-

1. **Research papers-**

**a)** CryptoToolJ: An Extensible Cryptology Tool for

Historical Ciphers

b) design and development of e learning contents for e security solutions cdac noida.

1. **Books-**
2. *Cryptography: theory and practice by Douglas Stinson*
3. A course in cryptography by RAFELL PASS
4. **Blogs links**
5. <http://cryptoblog.wordpress.com/>
6. <http://martinralbrecht.wordpress.com/>
7. <http://cipher-text.blogspot.com/>f
8. **projects**
9. stunnal
10. strip

**languages used for coding are**-

1. HTML 5
2. CSS/CSS3
3. JAVA SCRIPT
4. PHP

**Software used for coding**-

Dreamweaver , google chrome, notepad, photoshop, wamp server.

**ANALTICAL REVIEW**

After reading all the materials and performing researches on the topic we found some nonrelated things to the topic and some related things to the topic. Cryptography is begin used from several of years in many forms. It is used mainly for hiding the content or information. It is being thought in many of the universities. It is good to give information about this newly chapter to the students. For giving this material we need a good server that is internet in present days. For this we choose to form a site which will train the students for the cryptography. It may be used in universities also as a online study material.

For the selection of material as we searched many of sites and other sources we found very useful videos and pdfs as well.

Direct application of the cryptography must be seen to the user so we will use applications also.

For a good design HTML and CSS may be used in the site. PHP would be used for the database.

**CONTRIBUTION OF THE PROJECT**

1. **Competence Quality of education**

The most integral feature of the project is improvement in the quality of education. Aim of the project is to faster the entire concepts of present education system. It teaches the course of cryptography through a unique approach.

1. **Self actualization**

Advancement of support system focusing on intrinsic psychological needs. When a person would be understanding a particular concept through various modes of learning i.e. e books, videos, tutorials, photos, presentations, then it would provide him a better insight into his own self.

1. **Enhancement of accessibility and quality of basic facilities**

Education is the basic need of human being and by promoting learning through the medium of online learning increase the accessibility. It gives user the access of learning at their own pace and in their own comfort zone.

1. **Conservation of physical environment**

It is a kind of e learning. It consists of presentations and e books so it could save paper and environment.

**REQUIRMENTS**

1. **Accessibility-**

Education is the basic need of human being and by promoting learning through the medium of online learning increase the accessibility. It gives user the access of learning at their own pace and in their own comfort zone.

1. **Ease of learning**-

Teaching methodology should be kind of easy so a new comer can learn things fast and accurately. For this images, books, videos, pdfs, ppts, suggestions required.

1. **Appearance**-

Appearance will be in manner that one can find anything quickly. It would not be kind of fearing to new comer. Use funky look and attractive colors.

1. **Security**-

Admin must be known of who is using site and for how much time. For this include login function.

1. **Language-**

Site must be in other language also so that all can read it.it must have Hindi version.

1. **Mobile utility**-

Site must be open on the mobile phones.

1. **All info at one place-**

Site must have all related info at one place. This must have important links, books, news.

1. **Views-**

Site must have comments and suggestions of other users. It would have friends circle.

1. **Social networking**-

It must be linked to Facebook, Twitter, Youtube so all can see. It would have a blog also.

1. **Ease of joining-**

Joining form should be ease and fast.

1. **Feedback-**

For improving the site we need feedback so it have a feature of feedback.

**USE CASE DIAGRAMS**

logged user

Un logged user

admin

admin

extend

System

<<include>>

Blog reader

**CLASS DIAGRAMS**

**The following classes are included in the project-**

1. Blog
2. Videos
3. About us
4. Join
5. Login
6. Logout
7. Cipher 1
8. Cipher 2
9. Cipher 3
10. Hash function
11. Quizzes
12. Contact us
13. Feedback
14. Registered user
15. Unregistered user
16. Blog reader

The detailed class diagram of each class is on next page.

1. **Blog**

Blog

* Name
* Passwords
* City

+ content

* Add content
* Delete content
* update

1. **Videos**

Videos

+ videos snapshot

+ videos links

+ videos content

* Delete
* Add
* Update

1. **About us**

About Us

+ content of site

* Resourses used
* Add
* Delete
* Update

1. **Join**

Join

* Name
* Password
* Age
* Nation
* Gender

+Validate username

+validate password

-Save password

-save username

-save age

+ send confirmation message

1. **Login**

Login

-username

-password

* Check username
* Check password

+ remember me

+forget password

* Open account

1. **Logout**

Logout

* Username
* Time spend
* Save updates
* Save time
* Logout message

1. **Ceasar Cipher**

Ceasar cipher

+ input

+output

+ shift

+ convert to ascii

+add shift

+convert to string

1. **Rail fence cipher**

Rail fence cipher

+ input string

+no. of rows

+ no. of column

+ output

+ 2D array formation(row and columns)

+ divide each element into the row and column

1. **One time pad ciphers**

One time pad cipher

+ string

+alphabet

+output

+alphabet to number

+ string to nos.

+ shift of alphabet no.

+convert to string again

1. **Quizzes**

Quizzes

+ questions

-user Answers

+Time

* Right answer

-time constraint

-check answers

+ show marks winned

1. **Contact us**

Contact us

+ name

+adders

+email id

+ blogs

* Add
* Delete
* Update

+ visible

1. **Feedback**

Feedback

-name

-email id

-message

+ Send

+ Reply

-Apply

1. **Register user**

Registered user

* Name
* Password
* Age
* Gender
* Used time
* Nation
* Delete account
* Change password
* See details
* See used time

1. **Unregistered user**

Unregister user

+ visiter counter

+ login

+ access videos

+ access sitmap

1. **Blog reader**

Blog reader

* Name
* Password

+ location

* Join
* Comment
* contact

**UML DIAGRAM**

This show the relationship between classes they have.

Login

Join

Logout

\*

\*

User

Feedback

Contact

Blog reader

registered user

Unregistered user

**ACTIVITY DIAGRAM**

OPEN THE SITE

Study material

quiz

Feedback

See useful links

Login

Join

CONTACT US

SITE MAP

FAQs

USE CIPHERS AND HASH FUNCTION

WIKI SEARCH

SEE ABOUT US

SEE HINDI VER

SEE BLOG

WATCH VIDEOS

Join

Reenter password

Enter password

Enter username

Again enter

Enter pwd again

Reenter pwd

Go to next

nation

sex

age

username

Login

password

Login success ful

Not match reenter

Feedback

Enter e mail id

Write message

Send

Ciphers and hash functions

Result display

submit

Enter text to be processed

submit

Answer the question

Quizzes

**STATE DIAGRAMS**

USERNAME/PWD MATCHING

CHECKING USERNAME AND PWD

INTIAL STATE

OPEN THE SITE

INITATE THE FUNCTIONS

NOT

HAVE

LOGIN

CHECK IF HAVE A/C OR NOT

ONLOAD

NOT HAVE

RE ENTER

MATCH

NOT LOAD

JOIN STATE

LOADING JOINING FORM

LOGIN SUCCESS

ACCESS ALL MATERIAL

FAILED STATE

RETRY TO RELOAD

Display message of wrong answer

wrong

Show marks obtained

right

Answer check

Check ans.

In time

out

Failed

Try next time

Answer quizzes

Checking time

quizzes

JOINED

SAVE

NO

ENTER PERSONAL DETAILS

SAVE DETAILS

YES

ENTER PASSWORD

CHECK FOR PWD CONSTRAINT

YES

ENTER USERNAME

CHECK FOR USERNAME VALIDATION

LOAD

**ER DIAGRAMS**

Database contains many tables and queries.some of the tables are given below.

1. User
2. Passwords
3. Username
4. Marks
5. Ids
6. No. of visitors
7. Question and answers
8. Time user spent
9. Feedback

User

login

quizzes

Feedback

feedback

Question and answers

password

**SEQUENCE DIAGRAMS**

**LOGIN-**

LOGIN

PASSWORD

USERNAME

USER

check

PWD

USERNAME

Site access

**QUIZ**

USER

SYSTEM

QUESTION

ANSWER

**JOIN**

PASSWORD

USERNAME

CHECK

CHECK

USERNAME

USER

NEXT LEVEL

JOINED

PWD

**ALGOS USED**

1. **USERNAME PASSWORD MATCH**-
2. Enter username
3. Enter password
4. Open table password
5. If password == username
6. Login successful
7. Else
8. Not login.
9. **Blank the text input** –

obj.style.color=""

obj.style.fontStyle=""

if (obj.value=="Search wikipedia.org")

{

obj.value=""

}

1. **Check the length of username and password**-
2. Username=username
3. Password=password
4. var value = $(this).val();
5. if( value.length<4 || value==field\_values[$(this).attr('id')] )
6. alert("Invalid Username or Password");
7. else
8. show next level.
9. **Check password and username match websites theme or not**
10. var value = $(this).val();

var check=str.match(/the/gi);

var check1=str.match(/cip/gi);

var check2=str.match(/mac/gi);

else if(value!=check || value!=check1 || value!=check2){

$(this).addClass('error');

$(this).effect("shake", { times:3 }, 50);

alert("Username or Password doesn't match website's theme");

1. Else show next level.
2. **Check email format**
3. var emailPattern = /^[a-zA-Z0-9.\_-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,4}$/;
4. var fields = $('#second\_step input[type=text]');
5. var error = 0;
6. fields.each(function(){
7. var value = $(this).val();
8. if( value.length<1 || value==field\_values[$(this).attr('id')] || ( $(this).attr('id')=='email' && !emailPattern.test(value) ) ) {
9. $(this).addClass('error');
10. **Ceaser Cipher**
11. User input the string need to encrypt
12. Convert string to the ASCII value
13. Store it into a string
14. Add 3 to all the ASCII values
15. Convert this array to the string
16. Write the final string.

1. **Rail fence cipher**: The algorithm of Rail fence cipher requires breaking of the string inputted by the user into various rails or horizontal array of characters. In this algorithm’s implementation, the string and number of rails to be considered is given by the user and then on the basis of number of rails the string is broken and decrypted diagonally. Till the characters of the initial array become equal to the number of rails the alphabets of the string goes vertically down and horizontally right, later on the positioning of the alphabets in the string follows the pattern of vertically up and horizontally right.
2. **One Time pad Cipher:** This cipher requires the user to enter the string as well as the alphabet which acts as decryption tool. The alphabet which user enters is replaced by its corresponding number in the alphabet table. The original string entered by the user is then later shifted to the right by that corresponding number, character by character. If the choice of decryption alphabet is made random and a string is considered instead of a single alphabet, then one time pad is practically an unbreakable cipher.

**DESING OVERVIEW**

1. **Interface design-**

The interface design is very light, and colorful. It is related to the education. It is very ease to use for the new comer. It have quick links and footer also.

1. **Content design**-

The content is to suitable for the new comer and students. It have videos, pdfs, ppts, and direct application for the convenience. It have question and answers also for the test. It have quizzes for the performance in the time limit. It have useful links from the other sites also.

1. **Navigation design**-

The navigator bar is related to the educational theme. It have sticky notes kind theme. It move when mouse overs on it. It have initial required data and information.

1. **Architecture and component design**-

The each and every component of the site is designed with considering all the requirements. The architecture consist of educational theme.

1. **Aesthetic design-**

Aesthetic design is the application of the branch of philosophy of aesthetics to cultural constructs. Site have social sites link in very good manner. It have related required aesthetic design.

**DETAILED SOFTWRE REQUIREMENTS**

Requirements gathering is the most important part of the developing a project. 71% failure of the project occur due to the poor requirements. for our project we gather information using many requirement elicitation techniques. we read many books, online forums, research papers and visit many websites for the project.

All the requirements are given listed below as per the class-

1. Student-

For a student it is necessary that all the material he/she find is easy to read and access. Site must not have very complicated to view. It must have application of cryptography so that student may know the use of it.

1. Learner-

For a first time learner it must server all the importance of the chapter and use of it. It must have pictures, video, application etc. it must have pdfs, and ppts in it.

1. Admin-

It must be changeable easily so that new features can be add to it. It must be updatable.

1. Security-

Site must consist of the security feature, it must have login system. Admin and user must have different powers to edit it.

1. All at one place-

Site must consist of all the information at one place. It must have news feeds from other sites. One can must be able to search topic on other related sites.

1. System-

Site must be able to run on any browser and operating system. Site must consist of low memory space on disk. It must be open on the mobile phones.

1. Language barrier-

Site must have Hindi or any other language version also.

**PROCESS MODEL**

Any software is developed under a process model. Selection of a right process model leads to be good goal and time saving.

As per the topic our requirements are so volatile so we have to make changes at every step many times.

**Incremental model** –

We preferably use incremental model for development. Incremental model deliver its output without making change in it between working. Output is shown to the user and then again changes make in the code. this save the time of develop. It give chance to moving on and on. Feedback on previous level is used in later phases.

**RAD model-**

In some phases we also applied the RAD model. RAD model include the changes in the already developed material as per the requirement. We use many videos, pictures and research paper in project. We read them and make necessary changes in them get our requirement.

**TEST CASES**

A **test case** in software engineering  is a set of conditions or variables under which a tester will determine whether an application  or software system is working correctly or not. Here we will use BLACK BOX TESTING at this stage because at present state we have no complete project that include database and other functions. At this stage some test case may be come out to be negative cause of non completion of that particular part.

Some test cases applied are given below-

1. **Browser testing**-

We run code on google chrome, internet explorer, firefox. It ran correctly on google chrome but IE have some less features to be run. It runs on firefox very fast and use all functionality.

1. **Username and password matching**-

Code run perfectly for matching algorithm. we would include it to php in later phases.

1. **Wiki search**-

Searching on Wikipedia done correctly. It need a better web speed only.

1. **Ciphers** –

Input given by the user display the right output corresponding.

1. **Constraints**-

Constraints on username and password working well.

1. **Other-**

Other requirements like learning, good study material, sufficient material, teaching method etc. are begin fulfill till date.

**CONCLUSION AND FUTURE WORK**

Till now we completed the basic layout of site. It have useful functions and applications till date. We required it to be very pretty and secure. For this purpose we would include PHP and CSS 5 in it in later phases.

It would have Hindi version also. It would be find out on the other social sites also. PHP database would be prepared for the user info and other content.

It may have live online lectures and many downloadable material in future work. It can be very fine tool for teaching in schools and collages later. It can be hosted online.

**WORK DIVISION AMONG GROUP MEMBERS**

We worked together in a well behaved and helping environment. Each of the member was contribute at best in the project.

Detailed work division is below-

1. Sumit nangia(9103531)-

Planning, requirements elicitation, requirement analysis, designing, coding of important logics, report writing.

1. Arihant bhantia(9103548)-

Requirements elicitation.

1. Ayush jain(9103553)-

Planning, requirement elicitation,requirement analysis, designing, coding of important logics, report writing.

**BIBLIOGRAPHY**

1. A course in cryptography by RAFELL PASS
2. <http://cryptoblog.wordpress.com/>
3. <http://martinralbrecht.wordpress.com/>
4. <http://cipher-text.blogspot.com/>
5. [www.google.com](http://www.google.com)
6. [www.w3schools.com](http://www.w3schools.com)