**Project Name : Monoalphabetic And Polyalphabetic Cipher**

**Phase 3 : Data Analysis and Evaluation**

**Student name : Nikhila Konda**

**Course Number : CS630-740**

**Instructor Name : Dr. Suhair Amer, Ph.D.**

**1. DETERMINE THE GOALS:**

The goals of this project is firstly to provide the easy way of learning the concepts for students. The reason for this undertaking is to learn about figures idea in cryptography which is Monoalphabetic Cipher and Polyalphabetic Cipher and to build up a Learning Game for understudies. The fundamental moto of this task is to comprehend the ideas in a basic and simple manner along these lines, that everybody learn in little range of time. What is more, it will stay in their cerebrum for the long time. This task is useful essentially for the understudies who concentrate High school and in college to the under alumni. Learning with the assistance of gaming instrument is certifiably not an impractical notion and it likewise upgrades the innovativeness abilities in understudies. It is simple approach to learn and recollect the ideas in the minds of understudies and perform well in tests also. By utilizing this Monoalphabetic and polyalphabetic figures idea we can program by utilizing a scratch programming. Programming just implies the specialty of creating rules (computations) to train a PC. Scratch is a block-based visual programming language and site focused on essentially at youngsters. Clients of the website can make online ventures utilizing a square like interface. The administration is created by the MIT Media Lab, has been converted into 70+ dialects, and is utilized in many pieces of the world. Scratch is not only a decent prologue to programming; it is a genuine programming language in its own right. Scratch has the important features of many programming languages, like loops (repeat blocks) and conditionals (if-then blocks). In Scratch, improvement is significant for bigger ventures since Scratch is a deciphered language. Proficient programming likewise permits you to have progressively content or a littler document size in a Scratch venture, in light of the fact that the contents would occupy less room, letting you make more use out of 50 MB. Scratch is secure, and ordinarily these individuals are immediately revealed and prohibited. Simply do not give out close to home data and report anyone who is mentioning individual data or in any case making you awkward and you ought to be fine. It merits referencing, however, that you will locate the intermittent grown-up. Scratch has the significant highlights of many programming dialects, similar to circles and conditionals . With these highlights, Scratchers can make calculations, or guidelines to finish explicit undertakings. PC researchers would state Scratch is a Turing-complete programming language, which implies it can play out all the fundamental capacities that make up calculations. In the wake of working with Scratch for some time, numerous Scratchers find that they need to keep utilizing Scratch even as they utilize other programming dialects. And providing the user-friendly interface to the students develop the skills to enhance their view of learning the subject. The purpose of this project is to study about ciphers concept in cryptography which is Monoalphabetic Cipher and Polyalphabetic Cipher and to develop a Learning Game for students. The main moto of this project is to understand the concepts in a simple and easy way so, that everyone learn in small span of time. And it will remain in their brain for the long time. This project is helpful mainly for the students who study High school and in university to the under graduates. Learning with the help of gaming tool is not a bad idea and it also enhances the creativity skills in students. It is easy way to learn and remember the concepts in the brains of students and perform well in exams as well.

**2. EXPLORE THE QUESTIONS:**

Social occasion data is an essential human movement – we use data to learn, to assist us with taking care of issues, to help our dynamic procedures and to see each other all the more unmistakably. Addressing is the way to increasing more data and without it relational interchanges can fall flat. Addressing is basic to fruitful correspondence - we as a whole ask and are asked inquiries when occupied with discussion.

1. What is the meaning of cipher in cryptography?

2. What will be the ciphered text for the input string “sanfoundry” with key string as “code” to the program of keyword cipher?

3. What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of vigenere cipher with keyword as “HELLO”?

4. What will be the ciphered text if the string “HELLO” is given as input to the code of hill cipher with keyword as “SANFOUNDRY”?

5. How to decode the monoalphabetic ciphers using the plaintext concepts?

6. What is the difference between monoalphabetic ciphers and Polyalphabetic ciphers in the cryptography module?

7. How do you differentiate between the plaintext and the cipher text relation in the ciphers concepts?

8. Explain about the Encoding and Decoding process involved in the cipher text and plain text in alphabetics?

A Monoalphabetic Substitution Cipher maps individual plaintext letters to individual ciphertext letters, on a 1-to-1 unique basis.  That is, every instance of a given letter always maps to the same ciphertext letter.  The oldest such cipher known is the Caesar cipher, where the mapping involved a simple shift within the alphabet.  For example, the following represents a Caesar cipher with a shift of 3:

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext: XYZABCDEFGHIJKLMNOPQRSTUVW

Monoalphabetic Substitution Ciphers employ a more complex approach:  Instead of using a simple shift to determine the letter mapping, they select an individual mapping for each character, where the relative position of the corresponding characters is, in general, different for all characters. So, in order to decipher a Monoalphabetic Substitution cipher, you need to determine the mapping for every character a lot more complex than just determining a single fixed shift value. Here is an example of a Monoalphabetic Substitution Cipher.  Here is a letter substitution table for such a cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
OEXPVYQNAZGCDKURHJLBIFMSWT

**3. CHOOSE THE EVALUATION METHOD:**

A few interesting points while choosing an evaluation methods are:

What data is expected to decide?

What data can plausibly be gathered and broke down?

How exact will the data be?

Will the data be tenable to top benefactors or the executives?

**Potential Evaluation Methods:**

Test

Pre and Post Test

Test Against Control Groups

Participation

Attendance

Completion

Certificates

Follow-On Tracking

Data Collection

Surveys

Questionnaires

Interviews

Checklists

Feedback forms

Financial Reports

Cost to budget

Cost per unit of service

On time on budget

Performance

Grades

Graduation

Drop in recidivism

**4. IDENTIFY THE PRACTICAL ISSUES:**

Practical issues identify with time, cash and coordinations. In some cases the best strategy for exploring a specific theme, hypothetically, must be dismissed on the grounds that it would cost a lot of cash to direct, it would be hard to do, or in light of the fact that it would require some investment to get results.

Problem 1: Everybody wants to know what it is going to cost.

Problem 2: Requirements are not clearly defined.

Problem 3: Requirements need to change for business reasons.

Problem 4: Requirements prevent changing to a more suitable solution.

Problem 5: It takes FOREVER to launch the new site.

Problem 6: A site is never really done when it is launched.

Problem 7: My fancy content management system/e-commerce site got hacked!

Problem 8: My fancy content management system has reached the end of life!

Problem 9: My site broke after an upgrade.

Problem 10: It costs too much up front!

We can let you know whether a financial plan is sensible for what you are attempting to achieve. In the event that it is tight, we can assist you with organizing highlights, and ensure the basic ones are done first before the financial plan is depleted. Necessities fill one need: they are a stake in the ground that one side can use to separate more work or more money out of the opposite side. Rather than having immovable prerequisites, we help our clients distinguish objectives and rank them by need. A site sitting on an advancement server concealed away from the general population is totally pointless. Loads of amazingly fruitful Internet new businesses began with a bad webpage individuals come to sites for the substance, the communication, the stuff that is on there. With the sorts of web ventures, we do, individuals assemble on your webpage and connect with it consistently. Most substance the executives frameworks store content in a database. Not many conventional web has disclosed to you how to back these up. Less despite everything keep a scope of reinforcements after some time or can specifically reestablish specific things that might have been erased. They cost more. I could not care less what your engineer let you know in advance that by having the option to refresh content yourself, you will not need to pay them to refresh content on your site. While that is genuine you can refresh the substance, yourself you will need to pay someone to stay up with the latest. What is more, it will cost more than having a static site. Flawlessness is costly, also inconceivable. The ideal is the foe of the great. While we make progress toward out and out greatness, the straightforward certainty is that the product we utilize is an aggregate exertion of thousands of engineers, and there are bugs.