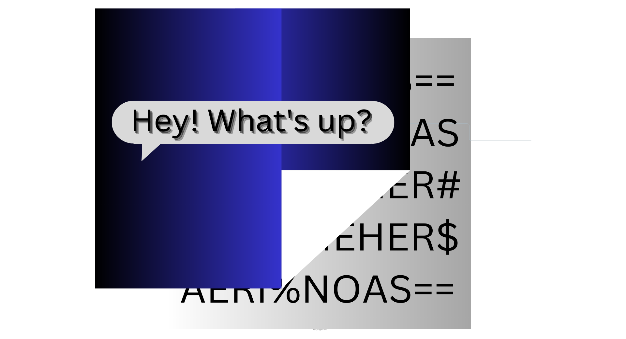
**INVENTION DISCLOSURE FORM**

**A. GENERAL INFORMATION:**

1. **TITLE OF THE PROPOSED INVENTION:**

**Cryptic (Messenger + Learning Platform): A platform where a common user gets to learn about the cryptography and how it works in messaging apps through the means of simulation.**

****

1. **DETAILS OF APPLICANT/S:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Full Name/s | Nationality | Complete address | Type:  Legal Entity or Start Up or Natural Person(s) |
| 1 | Harsh Rahul | Indian | 643/1 Pedi Ghat, Nemawar, Sub-dist: Khategaon, Dist: Dewas | Start Up |
| 2 |  |  |  |  |

1. **DETAILS OF INVENTOR/S:**
2. **IS/ARE THE APPLICANT/S ALSO THE INVENTOR/S: YES / NO**
3. **IF NO, PLEASE PROVIDE FOLLOWING DETAILS OF THE INVENTOR/S:**

|  |  |  |  |
| --- | --- | --- | --- |
| # | Full Name/s | Nationality | Complete address |
| 1 | Harsh Rahul | Indian | 643/1 Pedi Ghat, Nemawar, Sub-dist Khategaon, Dist-Dewas |
| 2 |  |  |  |

1. **DATE OF THE PROPOSED INVENTION (EARLIEST CONCEPTION DATE OF THE PROPOSED INVENTION):**

DATE: 09/04/2023(DD/MM/YYYY)

**B. QUESTIONNAIRE:**

**1. FIELD AND GENERAL DESCRIPTION OF THE PROPOSED INVENTION**

**DESCRIBE THE FIELD OF TECHNOLOGY. WHAT ARE THE APPLICATIONS IN WHICH THE PROPOSED INVENTION CAN BE EMPLOYED?**

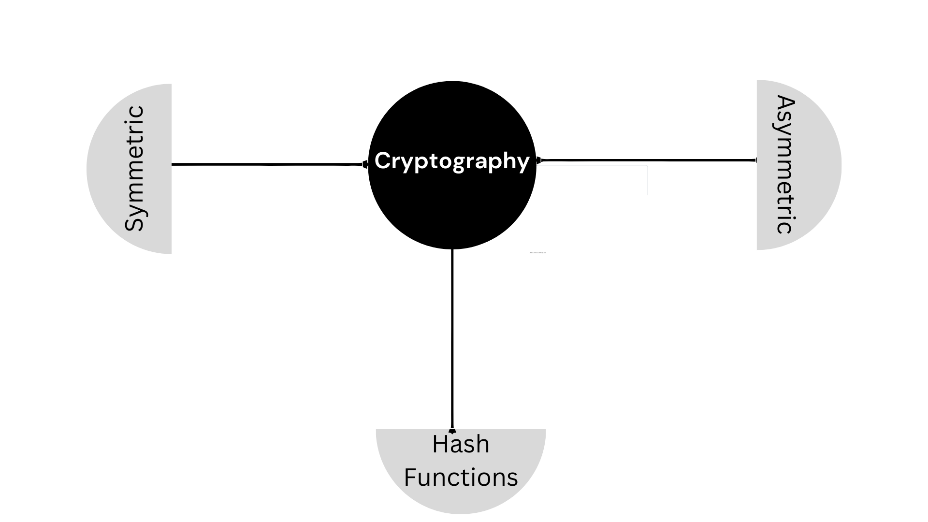
Cryptography is the process of converting the text in the form of cipher text which doesn’t make any sense without converting it back to the normal text with corresponding technique.

There are two types of Cryptography:

1. Symmetric Key Cryptography: This type of cryptography uses same key for the process of encryption and decryption known as SECRET Key.

2. Asymmetric Key Cryptography: Asymmetric key cryptography uses two different keys for encryption and decryption namely Public key and Private Key. The public key of the receiver is shared over the internet and the sender then encrypts the message using the public key of receiver which could only be decrypted using the private key of the receiver.

3. Hash Functions: Hash functions are mathematically calculated functions which takes input of any size and convert to string of a certain size, it is easy to calculate the hash of a function but near impossible to go back to original data using the hash of it.



*There are many sub types of both types of cryptographic algorithms which will cover a whole book but the main idea lies in those only algorithms which later on will become the most important components of this application/software/web application.*

In order to provide a safe and distinct communications, there’s a need of alternative options other than the ones present right now which should be provided to the user so that a monopoly doesn’t get created and users don’t have to rely on one application which uses a technology which the user isn’t even aware of.

To provide an alternative source of communication and multiple options for transferring the text or media this app should provide the information about the cryptographic techniques and how they work and consecutively provide the choice of encryption technique in which they want to communicate.

**2. EXISTING TECHNOLOGY**

**DESCRIBE ALL EXISTING PRIOR ART (PATENTS / NON-PATENT REFERENCES) THAT YOU ARE AWARE OF. ALSO, PROVIDE DETAILS OF DEVICE/S, MACHINE/S, PROCESS/ES ETC. KNOWN IN THE INDUSTRY IN THE FIELD OF APPLICATION OF THE PROPOSED INVENTION.**

There are many applications which uses end to end encryption technology to encrypt messages and media for communication which uses a combination of both symmetric and asymmetric algorithms in order to set a connection.

First a connection is set using the public key of the receiver then the sender encrypt the secret key using that public key which can be decrypted using the private key of the receiver then the shared secret key is used for the later messages that would be transferred between them.

And other than that there are also many individual websites and learning platforms which are really helpful in gaining knowledge about different algorithms.

**3. DRAWBACKS / PROBLEMS / CHALLENGES IN THE PRIOR ART THAT THE PROPOSED INVENTION ADDRESSES**

**DISCUSS ALL POSSIBLE DRAWBACKS / PROBLEMS / CHALLENGES ASSOCIATED WITH THE EXISTING TECHNOLOGY IN RESPECT OF WHICH THE PROPOSED INVENTION AIMS TO A PROVIDE SOLUTION. HOW THESE PROBLEMS WERE ADDRESSED BEFORE THE PROPOSED INVENTION WAS CONCEIVED?**

Every communication provider uses its own certain choice from all the available cryptographic methods for encrypting the text or the media files and user have no choice other than believing in the service provider and keep on using the service and all companies which provide these services use same method for every user.

So if the method becomes anyhow vulnerable everyone present on internet using the service would become vulnerable to that threat and that has the risk of breaching of data of billions of people in a couple of minutes.

And presently no application or software or any website provide real time knowledge of the algorithms by applying it to the messages or data.

**4. SOLUTION PROPOSED BY THE PROPOSED INVENTION**

HOW DOES THE PROPOSED INVENTION OVERCOME THE DRAWBACKS / PROBLEMS / CHALLENGES ASSOCIATED WITH THE EXISTING TECHNOLOGY?

The proposed application/software/web-application is a combination of a learning platform and a messenger where the user could understand an algorithm and apply to his/her message or data in real time and on top of that he can chat using the technology(algorithm) of his choice with

User first get to see the integrated graphics showing the working of a particular algorithm and understand the basics of that algorithm and if he wants to see the calculations behind it he/she can also see that

As all the present applications uses only single technology and the users don’t know about any of the present technology this is where this mobile application/software/web application come up in the play with multiple options of encryption technique provided to every individual user to communicate using the method of his own choice because everyone might have different need and on top of that user get to know the logic and working of all the available algorithms in the mobile application/software/web application.

Each algorithms has their own strengths and weaknesses and based on the needs of the user one can choose which algorithm does we like to use, there are several choices putted on the dish for the user to choose from, like symmetric key cryptography, asymmetric key cryptography, hash functions, digital signatures and key exchange algorithms.

There is no guarantee that the one method would never be compromised ever, in that case the people using different algorithms will 100% be safe.

**5. DETAILED DESCRIPTION OF THE PROPOSED INVENTION**

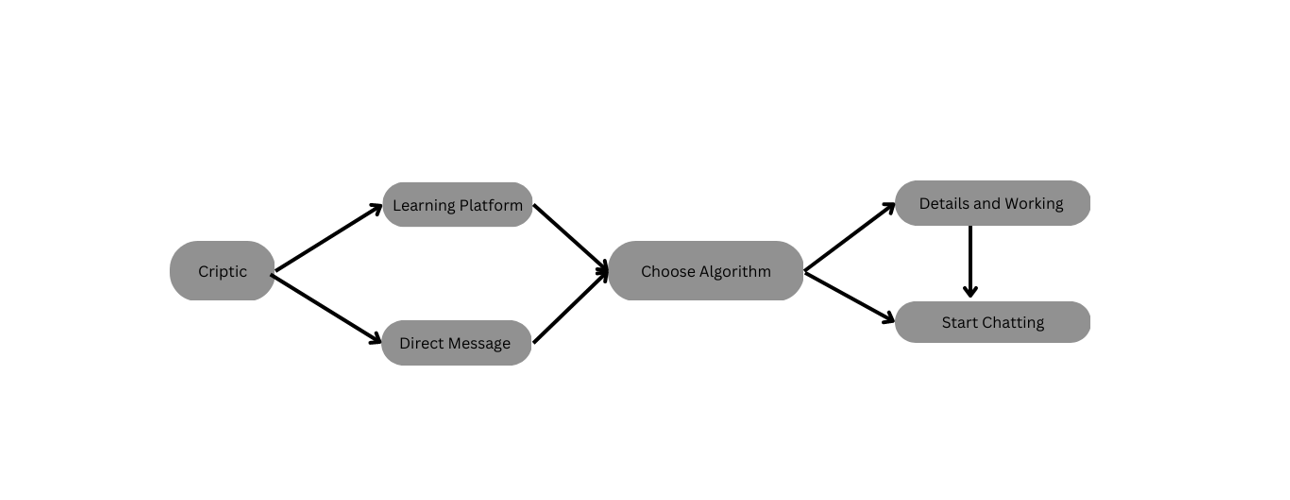
**DESCRIBE THE PROPOSED INVENTION AND ITS WORKING IN DETAIL. FOR EXAMPLE, DOES THE INVENTION RELATES TO A PRODUCT** **/ PROCESS / MACHINE / SYSTEM ETC. IN CASE OF A PRODUCT / MACHINE / SYSTEM OR THE LIKE, WHAT ARE THE DIFFERENT COMPONENTS AND HOW THEY ARE INTERLINKED TO PERFORM THE PROPOSED INVENTION? IN CASE OF A PROCESS, DESCRIBE VARIOUS STEPS INVOLVED TO PERFORM THE PROPOSED INVENTION. THIS DESCRIPTION SHOULD BE ELABORATE SO TO ENABLE A SKILLED PERSON TO PERFORM THE PROPOSED INVENTION AFTER READING THIS DESCRIPTION.**

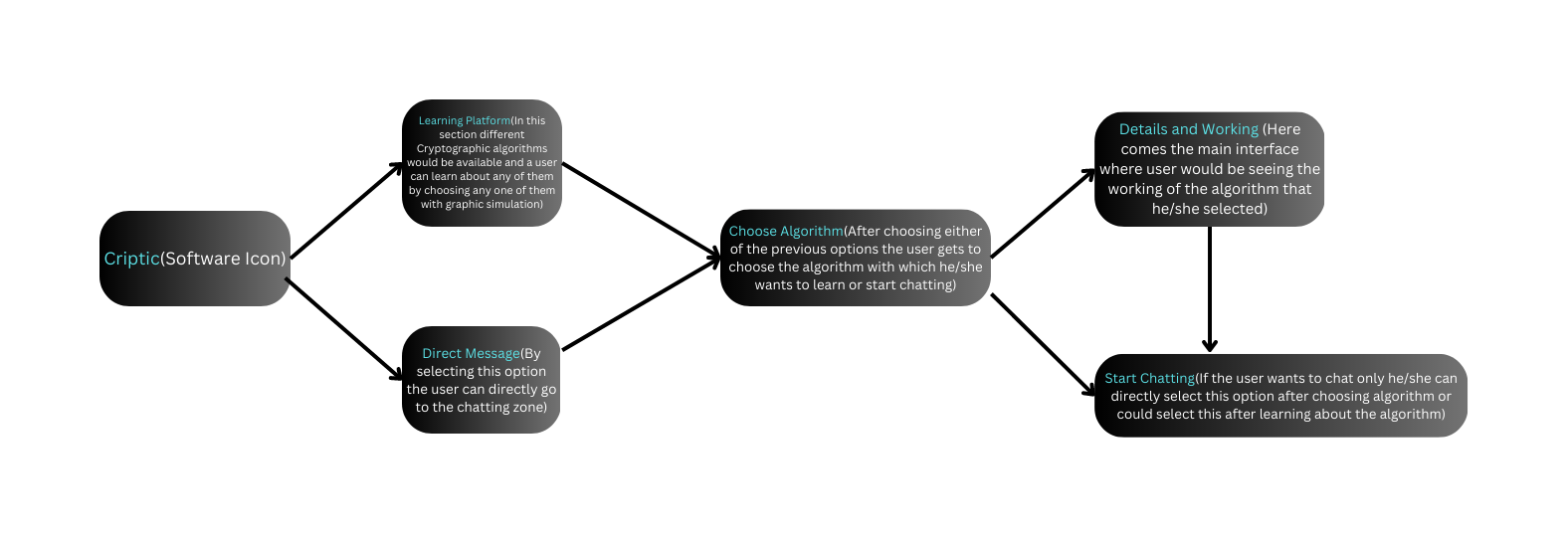
Criptic when opened provides two options to the user whether they want to chat or learn after choosing any of them, the user gets to choose the algorithm on which he wants to perform the action of his choice like details and working of the algorithm with graphic or he may directly start to chat.

The basic working of this messenger is just like a normal texting or communication application that uses some type of encryption technology for converting the text into cipher text and the receiver receiving it decrypt this with the respective technique but the difference that this mobile application/software/web application should provide is the method of encrypting the text.

**6. DRAWINGS / FLOW CHARTS / BLOCK DIAGRAMS / CIRCUIT DIAGRAMS**

PROVIDE DRAWINGS, PREFERABLY LINE DRAWINGS, FLOW CHARTS, BLOCK DIAGRAMS, CIRCUIT DIAGRAMS ETC. WHICH BEST DEPICT THE PROPOSED INVENTION. THE DRAWINGS SHOULD BE ABLE TO DEPICT VARIOUS COMPONENTS / IMPORTANT STRUCTURAL FEATURES OF THE PROPOSED INVENTION. IN CASE OF A PROCESS, A FLOW CHART DEPICTING ITS VARIOUS STEPS SHOULD BE PROVIDED.





**7. NOVEL / INVENTIVE FEATURES**

ACCORDING TO YOU, WHAT ARE THE MOST IMPORTANT FEATURES / ELEMENTS OF THE PROPOSED INVENTION

THE MOST IMPORTANT FEATURES OF THIS INVENTION ARE: THE CHOICE OF ALGORITHMS WHICH THIS APPLICATION/SOFTWARE/WEB APPLICATION PROVIDE TO CHAT WITH AND THE PLATFORM ALSO PROVIDE TEACHING ABOUT THOSE ALGORITHMS

**8. UTILITY OF THE PROPOSED INVENTION**

PLEASE MENTION CURRENT IMMEDIATE APPLICATIONS OF THE PROPOSED INVENTION AND POSSIBLE USES.

This app will help the user understand better about the cryptography and how the conversation actually work behind the application with the help of graphical animations using different algorithms

**9. ADVANTAGES**

LIST ALL POSSIBLE ADVANTAGES OF THE PROPOSED INVENTION OVER EXISTING TECHNOLOGY.

1.This will help people know about the cryptography.

2. Generate a wave of interest in the field of cryptography and cybersecurity in general.

3. This will help in making students ready for the cybersecurity vacancies all over the world.

( The threat of data theft and hacking is increasing day by day so making people take interest in cybersecurity is very important.)

4. Awareness about cybersecurity in common people

**10. ALTERNATE EMBODIMENTS**

PLEASE PROVIDE ALTERNATE WAYS / METHODS OF ACHIEVING THE PROPOSED INVENTION

N/a

**11. Hardware Used**

**The use of a server is required to operate the running processes and store all the data related to the software, all the data of the end user and the cryptographical operations which are going to be performed on the data entered by the user.**

**The server could be cloud based or it could be on-premises**

**12. LIST OF PREFERRED KEYWORDS PERTAINING TO THE PROPOSED INVENTION**

* **Cryptography**
* **Encryption/Decryption**
* **Hash functions**
* **Cryptographic Algorithms**