

**IMPROVING MOBILE SECURITY OF QR CODES  
ECOSYSTEM WITH PKI AND HASH  
ALGORITHM**

*Dissertation submitted in fulfilment of the requirements for the Degree of*

**MASTER OF TECHNOLOGY  
in  
COMPUTER SCIENCE AND ENGINEERING**

By  
**HARPREET SANDHU**  
**11511084**

Supervisor  
**MR. M. VIJAYA RAJU**



**School of Computer Science and Engineering**

Lovely Professional University

Phagwara, Punjab (India)

APRIL 2017

@ Copyright LOVELY PROFESSIONAL UNIVERSITY, Punjab (INDIA)

April 2017

ALL RIGHTS RESERVED



**TOPIC APPROVAL PERFORMA**

School of Computer Science and Engineering

**Program :** P172::M. Tech. (Computer Science and Engineering) [Full Time]

**COURSE CODE :** CSE545                      **REGULAR/BACKLOG :** Regular                      **GROUP NUMBER :** CSERGD0302

**Supervisor Name :** M. Vijaya Raju                      **UID :** 14844                      **Designation :** Assistant Professor

**Qualification :** \_\_\_\_\_                      **Research Experience :** \_\_\_\_\_

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Harpreet Sandhu	11511084	2015	K1519	9463782372

**SPECIALIZATION AREA :** Software Engineering                      **Supervisor Signature:** \_\_\_\_\_

**PROPOSED TOPIC :** Improving Mobile Security of QR Code Ecosystem with PKI and Hash Algorithms.

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	7.00
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.20
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.20
5	Social Applicability: Project work intends to solve a practical problem.	6.80
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.20

PAC Committee Members		
PAC Member 1 Name: Gaurav Pushkarna	UID: 11057	Recommended (Y/N): Yes
PAC Member 2 Name: Mandeep Singh	UID: 13742	Recommended (Y/N): NA
PAC Member 3 Name: Er.Dalwinder Singh	UID: 11265	Recommended (Y/N): Yes
PAC Member 4 Name: Balraj Singh	UID: 13075	Recommended (Y/N): Yes
PAC Member 5 Name: Harwant Singh Arri	UID: 12975	Recommended (Y/N): Yes
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

**Final Topic Approved by PAC:** Improving Mobile Security of QR Code Ecosystem with PKI and Hash Algorithms.

**Overall Remarks:** Approved

**PAC CHAIRPERSON Name:** 11011::Rajeev Sobti

**Approval Date:** 26 Oct 2016

12/12/2016 2:10:52 PM

## DECLARATION STATEMENT

---

I hereby declare that the research work reported in the dissertation entitled "IMPROVING MOBILE SECURITY OF QR CODES ECOSYSTEM WITH PKI AND HASH ALGORITHM" in partial fulfillment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. M. VIJAYA RAJU. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

*Signature of Candidate*

**Harpreet Sandhu**

**RK1519B30**

## **SUPERVISOR'S CERTIFICATE**

---

This is to certify that the work reported in the M.Tech Dissertation entitled "IMPROVING MOBILE SECURITY OF QR CODES ECOSYSTEM WITH PKI AND HASH ALGORITHM", submitted by **Harpreet Sandhu** at **Lovely Professional University, Phagwara, India** is a bona fide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor  
(Mr. M. Vijaya Raju)

**Date:**

**Counter Signed by:**

**1) Concerned HOD:**

HoD's Signature: \_\_\_\_\_

HoD Name: \_\_\_\_\_

Date: \_\_\_\_\_

**2) Neutral Examiners:**

**External Examiner**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Affiliation: \_\_\_\_\_

Date: \_\_\_\_\_

**Internal Examiner**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

## ACKNOWLEDGEMENT

---

Although, only my name appears on the cover of this dissertation, a great many people have contributed to its production. I owe my gratitude to all those people who have made this dissertation possible and because of whom my graduate experience has been one that I will cherish forever. My deepest gratitude is to my advisor, **Mr. M. Vijaya Raju**. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own and at the same time the guidance to recover when my steps faltered. He taught me how to question thoughts and express ideas. His patience and support helped me overcome many crisis situations and finish this dissertation.

Notably, none of this would have been possible without the love and patience of my family. My family has been a constant source of concern, support and strength for all these years. This accomplishment would not have been possible without them.

Thank you.

**Harpreet Sandhu**  
**Reg. No. - 11511084**

# TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE NO.</b>
Front page	i
PAC form	ii
Declaration by the Scholar	iii
Supervisor's Certificate	iv
Acknowledgement	v
Table of Contents	vi
List of Tables	viii
List of Figures	ix
List of Abbreviations	x
Abstract	xi
<b>CHAPTER1: INTRODUCTION</b>	<b>1</b>
<b>1.1 QUICK RESPONSE CODES</b>	<b>1-3</b>
<b>1.2 PUBLIC KEY INFRASTRUCTURE</b>	<b>4-5</b>
<b>1.3 SECURED HASH ALGORITHMS</b>	<b>6-7</b>
<b>CHAPTER2: REVIEW OF LITERATURE</b>	<b>8-19</b>
<b>CHAPTER3: SCOPE OF STUDY</b>	<b>20</b>
<b>CHAPTER4: PRESENT WORK</b>	<b>21-22</b>
<b>4.1 PROBLEM FORMULATION</b>	<b>23</b>

<b>4.2 OBJECTIVES OF THE STUDY</b>	24
<b>4.3 RESEARCH METHADODOLOGY</b>	25-34
<b>CHPTER4: RESULTS AND DISCUSSION</b>	35-39
<b>4.1 EXPERIMENTAL RESULTS</b>	39- 44
<b>CHAPTER5: CONCLUSION AND FUTURE SCOPE</b>	45
<b>REFERENCES</b>	46-48
<b>APPENDIX</b>	49

## LIST OF TABLES

<b>TABLE NO.</b>	<b>TABLE DESCRIPTION</b>	<b>PAGE NO.</b>
<b>Table 2.1</b>	Comparison between QR code, Bar code and SQR	10
<b>Table 2.2</b>	Color QR code with HSV	14
<b>Table2.3</b>	Different Hash algorithm with properties	17



## LIST OF FIGURES

<b>FIGURE NO.</b>	<b>FIGURE DESCRIPTION</b>	<b>PAGE NO.</b>
<b>Figure1.1</b>	QR code of any data	3
<b>Figure1.2</b>	Color explanation of QR code	3
<b>Figure1.3</b>	Public key Cryptography	5
<b>Figure1.4</b>	Steps of SHA-1	7
<b>Figure2.1</b>	Compression and Multiplexing algorithm	13
<b>Figure4.1</b>	Proxy re-encryption	21
<b>Figure4.2</b>	Compression and Multiplexing	22
<b>Figure4.3</b>	Flow charts for research methodology	26
<b>Figure4.4</b>	Screenshot to test project	32
<b>Figure4.5</b>	Screenshot to test generating QR code	33
<b>Figure4.6</b>	Screenshot of generated QR code	34
<b>Figure5.1</b>	Graphical representation of decryption	40
<b>Figure5.2</b>	Front page	41
<b>Figure5.3</b>	Encryption page	41
<b>Figure5.4</b>	SHA-1 page	42
<b>Figure5.5</b>	Generating page	43
<b>Figure5.6</b>	Graphical representation of hash valuses	44

## LIST OF ABBREVIATIONS

---

1. **QR** - Quick Responses
2. **PKI** - Public Key Infrastructure
3. **SHA** - Secured Hash algorithm
4. **QRC** - Quick Response codes
5. **SQRC**– Secured Quick Response codes
6. **TTL** –Time to live
7. **RSA** - Rivest, Shamir and Ad leman
8. **ECC** - Elliptic curve cryptography
9. **PHP** - Personal home page
10. **AES** - Advanced encryption standard
11. **DES** - Data encryption standard
12. **SSL certificates** - Secure socket layer
13. **MD** - Message digest
14. **HTTPS** - Hypertext transfer protocol
15. **ASCII** - American Standard Code for Information Interchange

## ABSTRACT

---

Significance of Quick responses has been growing for the past few years because of its practical applications in mobile devices. These Codes are very frequent in uses because they are easy to use and store more data as compare to Bar codes. There are many pros of these codes like in Research fields, Online Banking, Attendance Management, Health Care, Security Application (Cryptography and Steganography), secure transportation. As per usage of these codes are frequently increases then security of these codes are also very important. So, If this security is maintained by PKI and Hash algorithm than there would be less chances of Malicious codes, who wants to attack on these QR codes. Secondly, PKI explains the cryptography techniques with exchange of public and private keys. Using Public Key Infrastructure we maintain our data security because it is very hard to detect these public/private keys for attacker. Since until this step data authentication, confidentiality and integrity is achieved with the help of generating QR codes and using PKI, after this if we apply Hash Algorithms for more security than our data should be more secured to transmission. Hash functions are used to map the data from differential length of data into fixed length data. There are some particular Hash algorithms which generates the fixed length message digest. Generating an android app with this much secure data is the main point of this topic of theses which increases the ecosystem of mobile phones. Because these codes are read and scan by android phones so they affect the security of mobile phones due to of hidden information in it. So as the Usage of mobile increases widely the security of these phones are also play wide role.

*Keywords— QR codes, Mobile phone, Compression, Android studio, Cryptography, Stagnography .*

## Checklist for Dissertation-III Supervisor

Name: \_\_\_\_\_ UID: \_\_\_\_\_ Domain: \_\_\_\_\_

Registration No: \_\_\_\_\_ Name of student: \_\_\_\_\_

Title of Dissertation: \_\_\_\_\_

---

- Front pages are as per the format.
- Topic on the PAC form and title page are same.
- Front page numbers are in roman and for report, it is like 1, 2, 3.....
- TOC, List of Figures, etc. are matching with the actual page numbers in the report.
- Font, Font Size, Margins, line Spacing, Alignment, etc. are as per the guidelines.
- Color prints are used for images and implementation snapshots.
- Captions and citations are provided for all the figures, tables etc. and are numbered and center aligned.
- All the equations used in the report are numbered.
- Citations are provided for all the references.
- Objectives are clearly defined.**
- Minimum total number of pages of report is 50.
- Minimum references in report are 30.

Here by, I declare that I had verified the above mentioned points in the final dissertation report.

Signature of Supervisor with UID

# CHAPTER 1

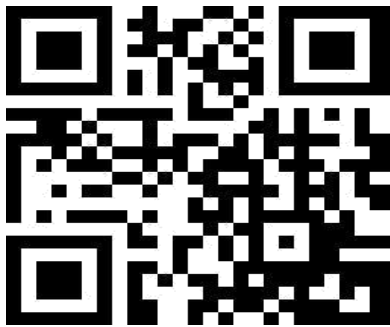
## INTRODUCTION

---

### 1.1 QUICK RESPONSES (QR CODES)

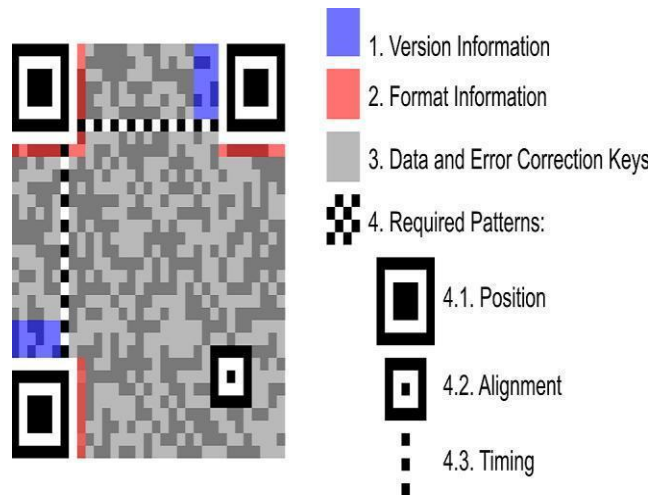
QR codes are quick response codes they responses in very few of seconds. These codes designed by Denso-Wave patented in 1994. He builds software which is scanned by mobile phones and digital cameras. The data encoded in these codes according to ISO/IEC 18004:2006. They are two dimensional so they gives more properties in storage and security in comparison with Bar codes. Because the Bar codes are one dimensional, they store information in both sides while QR codes store the data within both horizontal as well as vertical direction. They have white background and black dots on it. The special features which make these codes attractive are Error correction mechanism. Likewise they have three levels which are format error correction, mask pattern and error correction level. QR codes also play wide role in security of transmission of data [22] because they look only in black and white dots but inside them they store secure data which is hard to detect. It is not any hard and fast rule that these codes are designed only in black and white dots, Infect these codes are also present in colors. They are designed in RBG colors and some light colors effect. Colored QR codes are more secured as compare to black/white because there storage capacity is more. The wide usages of these codes are in digital marketing due their properties like potable, flexible and handy property. If we design a QR code for any data then there are total 8 possible masks for single data. Their reading property is  $360^{\circ}$ . While designing Quick responses the data is encoded with the help of Android studio. Android studio helps to give fronted and backend to design these codes. Similarly, for the process of decoding same process is followed. There are some special features which makes these codes are more valuable that is they are damage and dirt resistant. There are still sections under QR codes study which can be fulfilled in future like: there are many options to increase the security of QR codes. Because these codes hide lots of information which is not easily detect. We can design an algorithm which contains the any cryptographic techniques along with Message digest or Hash. Also we can increase the storage space of these codes using with some Steganography techniques. QR Codes can be easily generated using various web based

applications and it can be read using any Smartphone having Camera. So, encoding and decoding of the QR codes can be done using various free and open-source tools. First, I have developed a real-time application (web/mobile/desktop based) to generate and read the QR codes using either PHP or Android platform. There are some open libraries available i.e. qrlib in PHP and zxing in Java for android platform. (Required Duration: 1 month/person). Data Storage- To enhance the data storage capacity of QR Codes version1 to version40, I will use color QR code technique along with suitable compression algorithm (Huffman, ZIP, Lempel-Ziv etc) and the concept of Multiplexing can also be used. Further I try to enhance the existing color QR code model. For confidentiality- SQRCs (Secured QR Codes) are already providing small level of steganography and cryptography but that is not sufficient for brute-force attacks as attacker will always have enough time for cryptanalysis. [24] So for enhanced security, I have implemented public key encryption algorithm like ECC or RSA etc. Further I perform scrambling on the ciphered data. [26] All these algorithms can be implemented in PHP (web based) or Java (android based) platforms. after studying QR codes i have decided to work on security of QR codes. Security in QR codes: Security of QR codes is big issue because they hide the information in dots so it is tough to give more security to these. But this security is possible in many ways like providing Steganography and Cryptography. By applying Encryption/decryption technique we achieve larger security. There are many malicious QR codes which look like the same but they harm the security. Similarly there are some intended users who are unable to detect these types of attacks. Attacks possible only in case of malicious cases. There are many ways which gives the security to these codes as like by providing tracing codes, by authentication methods, by securing the information, by providing benefits in digital education system, by using AES and DES, security against malicious codes, by embedding encrypted techniques etc.



**Fig. 1.1:** QR Code of any Data

But in Second fig we can see that the knowledge given about four main sections of quick responses. That is Rendition information, organization Information, information Furthermore lapse revision Keys What's more required designs.



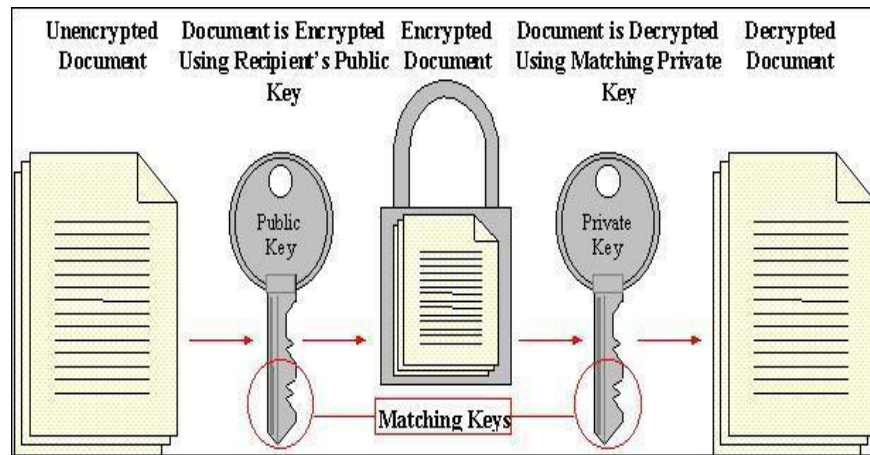
**Fig. 1.2 :** Color Explanation of QR Code

## 1.2 PUBLIC KEY INFRASTRUCTURE

PKI is basically a policy or procedure, which is used to manage, distribute and store of digital signature. As the name depicts the main motive of PKI is to transmit secure electronic data. Primarily, Public Key Infrastructure defined the cryptography techniques with the help of public and private keys whereas public key is for everyone while private key is for authenticated one. To convert the plaintext into cipher text is for handling from unauthorized user. The highlight feature in PKI is SSL certificates. SSL certificates related to encryption on websites. While sending the secure data on insecure path than digital signatures provide them security from unauthorized user. [28] We can say that PKI provides encryption on messages while an SSL certificate provides encryption on websites while transferring data on browser. Basically these certificates installed on servers for user to provide security. As the dependency on online transferring data is increasing day by day so security of these transformation is also very important. Similarly, there are many public key certificates also, which are also known as digital certificates that used for electronic communication. In General population enter encryption firstly the message is encrypted with public key which is send by sender than this cipher text is converted into decrypted form with the help of paired private key. In this way the message authentication is achieved in public key cryptography. This diagram shows the whole process of Public Key Cryptography. As you can see the first step is to take the simple unencrypted data than this data encrypted with the help of receiver's public key. We found the encrypted data. Afterward process started at receiver side. Take that encrypted data and decrypt with the help of private key. Finally we get our original data. In this we can achieve the data authentication and secrecy because the public and private key known by only sender and receiver. In the figure there is one factor which is known as matching key which is common in private and public key. Basically public key encryptions are used to secure the data and protect from third party nodes because is this case the malicious nodes are failed to detect the private and public keys. There these encryption techniques maintain the confidentiality and authenticity. These cryptographic



algorithms based on mathematical operations like integer factorization and discrete logarithms. There many types of public key encryption algorithms:- RSA and ECC . RSA used to secure the sensitive data. In RSA the integers are used from 0 to n-1 but also for some n. But basically the standard value for this is 1024 bits. Therefore the value of n should be less than  $2^{1024}$ . Thus security of this RSA is also very important. To secure this algorithm basic attacks are which are there which can attack to destroy this algorithm. Like Brute force attack, Mathematical attacks, Timing attack, Hardware fault - based attack, Chosen cipher text attack.



**Fig. 1.3:** Public Key Cryptography

### 1.3 SECURED HASH ALGORITHMS

Secured Hash algorithms are gaining more attention due to their property of data confidentiality. Data Integrity means data should be received in same format in which sender send it. SHA firstly designed by NSA in 1993 which is the version no SHA-0, after that in market the SHA-1 was came in 1995. Than SHA-224, SHA-256, SHA-384, SHA-512 come. These calculations depicted by NSA to achieve more data security after the development of MD-4 MD-5. These MD-4 and MD-5 are message digests which are by encryption on plain message. In secured hash algorithms very first step is padding, where as padding means adding extra bits in original message so that it become multiple of 512 bits. Than with encryption technique one message digest is formed which is further compared with next time entry. These algorithms designed to detect duplicate data and resist from attack. For example when we create an account on Gmail than at that time what password we given to that site, it converted into message digest at the backend. than next time when we given a password to get login the backend message digest is compared with new password which is given by user if the password is matched than you are allowed to login otherwise it shows wrong password if that new entered password is not matched with that message digest. SHA provides fixed length message which is the key point of maintaining data confidentiality. The maximum size of message in SHA is  $2^{128}$ , output message size is 256, internal bit size can extend to 512, block size is also extend up to 1024 .The basic binary operations which are performed on these secured hash algorithms are AND, OR, XOR, SHR, ROT. Different no of rounds in different versions of secured hash algorithms like in MD-5 and SHA-224 there are total 64 rounds while in SHA-0, SHA-1, SHA-256, SHA-384 and SHA-512 there are 80 rounds. The hash functions accept the value from message and convert it into fixed length and also padded some bits to the end if necessary. Cryptanalysis of hash functions are resolve the problem of collision that's why they are also called as collision resistant. These cryptanalysis works on internal structure of message. These Hash values which are produce from hash functions are maintain the integrity as well as authentication.

This figure indicates that message A, B, C, D, E are converted into fixed length messages with the help of hash algorithms. Here F defines the fixed length variables. After hashing these fixed length messages matched.

Algorithm for SHA-1 for 160 bit message:-

step 1- Increase the size of bit by adding extra bits. step 2- Increase length of message.

step 3- Get ready preparing functions.

step 4- Get ready preparing persistent.

step 5- Instate buffers.

step 6- Transforming message in 512 bit squares.

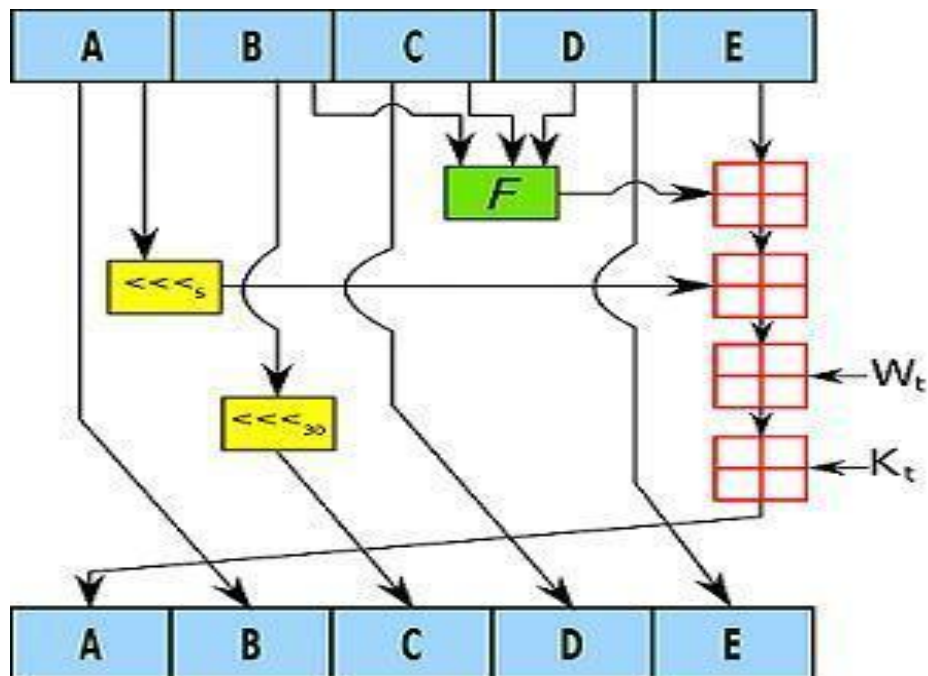


Fig. 1.4 : Steps of SHA-1

## CHAPTER 2 REVIEW OF LITERATURE

---

L. Roger Yin, Jiazhen Zhou, Maxwell K. Hsu " **Redesigning QR code Ecosystem with Improved Mobile Security**" [1] explained the life cycle of QR codes which include the basic 5 steps. Encoding, Distribution, Decoding, Action, Decommission. Encoding means the given data is transfer into another form. Distribution means data is divided into pieces. Decoding means again retransfer encoded data into original form. Action means play next operation that is given by user. Last Decommission means value in market. Author designed a new purposed model which is added one more factor before encoding that factor is data is encrypted with hash algorithm. In last, author also provides future work with gives indication to add PKI and Hash algorithm to affect the performance of QR codes. In this paper [1] they discuss about life cycle of QR codes which resolve the security issues. With this scheme security risk is decreased. In the scheme two main steps meanwhile in first step firstly the message pass to valid date then algorithms (public key algorithms) then passed to certificates after that at last the signature is generated.

- Message - that could be any text.
- Valid Date- this is a date at which message is valid.
- Algorithms - these includes all the public key algorithms.
- Certificate- these certificates are related to information and certified by public key of QR code issuer.
- Signature - the encrypted data using public key.

Saud Alotaibi, Steven Furnele, Nathan Clarke " **Transparent Authentication System for Mobile Device Security: A Review**" [2] explained the Authentication processes which are increased the mobile securities. It is an review paper which is focus on reviewing the different authentication techniques. There are some applications which are based on keystroke which means based on typing keyboard and some are based on gait based which means depend upon walking. But author compare and telling that from these

2 the touch screen is best because it depend upon touch, pressure and authenticates the original user. After that author explained sensor based which means the sensors present in android phones which detect the authenticity, and some applications are depend upon behavioral. These are also sensor based because these sensors are help to detect that the user is legitimate or not. Well it is a review paper [2] which explains that there are many applications in our mobiles that does not need any security. This paper explains the literature review of different papers on mobile security. It explains that certain applications are not come under mobile authenticity. But when we install them they told us that accept certain terms and conditions which are not necessary. At the end user gives some future direction if we decide that how to categories application in mobile phones.

Saranya K., Reminaa R. S., Subhitsha S. "**Modern Applications of QR-Code for Security**" [3] explained the applications of Quick Responses to attain the security of mobile phones. Firstly the author compared the different properties of bar codes and QR codes. Secondly the author compared the properties of QRC with SQRC. This SQRC gives better recognition, reducing redundancy and save space. Author explains the example with QR code on Aadhar card. As we all see at fronted of Aadhar card which is unique identity of everyone contains a QR code which is full of user information like name, address, sex, age and unique number. This is also helpful in detecting that data should send from authenticate device and should received by legitimate device. This is a survey paper. Like Capacity, Durability, Speed, Space and Language supported. This paper explains the different applications of QR codes and compares them with Bar codes [3]. This is a survey paper. Like Capacity, Durability, Speed, Space and Language supported. It explains the different colors of QR codes difference between QRC and SQRC where QRC are quick response codes and SQRC are secured quick response codes. When compare the properties of QRC and SQRC like capacity, durability, security, readability then it is found that SQRC is more efficient and secured than QRC.

**Table no: 2.1** Comparisons between QR Code, Bar Code and SQR

Features	QR code	Bar code	SQRC
Data Capacity	Up to 7089 numeric Digit	10-20 digits	7089 numeric digit
Security Function	No	No	Yes
Durability	Yes (max 30%)	No	Yes (max 30%)
Readability	Yes	No	Yes
Language Supported	Numeric, alphanumeric, Eric, kanji, kana	Numeric, alphanumeric	Numeric, alphanumeric, kanji, kana

Akhil N. V, Athira Vijay, Deepa S Kumar "**QR Code Security Using Proxy Re-Encryption**" [4] explains that how to detect the malicious data and malicious QR codes. The technique designed by author is proxy re-encryption serves on reduce these malevolent attacks. It explains that data should be secure if and only if data should be known to sender and receiver. After that author explains the structure of quick response code which contains the information about error correction mechanism and message placement. Author purposed a model which explains that providing encryption before encoded the string in quick response codes and decryption after decoding the QR code. This paper [4] explains the basic features of QR codes and Proxy Re-Encryption. Well Proxy Re-Encryption is nothing it is same as encryption done on any message. Transform information is secured with QR codes but this Proxy Re-encryption helps to maintain double security on that information because it is very hard to detect that what

message is converted into cipher text. These Quick Response codes contains the following six main steps - Information analysis, information encoding, slip revision coding, structure last message, module placement On matrix, information masking, organization Furthermore adaptation majority of the data.

- Information investigation analyses those information.
- Information encoding methods will encode the information under an additional structure.
- Error correction coding means to check the error and correct that error after that coding is done.
- Structure final message means design the final message.
- Module placement in matrix means placed the modules in 2d matrix.
- Data masking means prepare a mask to cover that data.
- Format and Version information explains the version of that data.

Krombholz Katharina, Fuhwirt Peter, Rieder Thomas, Kapsalis Ioannis, Ullrich Johanna, Weippl Edgar "**QR Code Security-How Secure and Usable Apps can Protect Users Against Malicious QR Codes**" [5] explains that malicious codes are also alike original ones that's why people get attacked and also some applications are in our phones that are deployed. Phishing attacks are very common for these type codes. Phishing attack is obtaining personal information from user by some malicious way.

Writer utilization http what's more HTTPS interceptor proxy on identify the correspondence the middle of outer units Furthermore cell telephones. Author gives direction that QR codes does not need any personal information of user like phone contacts, messages, gallery and some logs so to avoid the malicious attacks one should know that malicious codes demands all such things. This paper [5] focuses on the security of some usable applications from malicious codes. These Malicious QR codes are big problem. They are not easy to detect and resolve. Malicious codes are very much same as like original codes that's they are hard to detect. But the main motive of attacker or malicious codes is to destroy the security of data. In this paper they detect that Usage

of these QR codes are resolve the problem of External Communication, User Tracking, and Location data. In external Communication the QR codes does not need any external data like messages and images of mobile phone. Similarly in user tracking there is no need of any user appearance.

Mona M Umaria, G. B Jethava " **Enhancing the Data Storage Capacity in QR code using Compression Algorithm and achieving Security and Further Data Storage Capacity Improvement Using Multiplexing**" [6] focused Around expanding space of QR codes by applying layering procedure. QR code cam wood makes go about as medium from claiming offering information. Author designed a technique which explains that firstly the data is compressed in any form so that more and more data should be stored. In this paper[6] the author explains the capacity of storage in QR code. They invent new algorithm which increase the capacity of these codes and named as compression algorithm. After that they apply multiplexing on bits of data which increase more capacity of Quick response codes.

In Compression algorithm there are total 5 steps:-

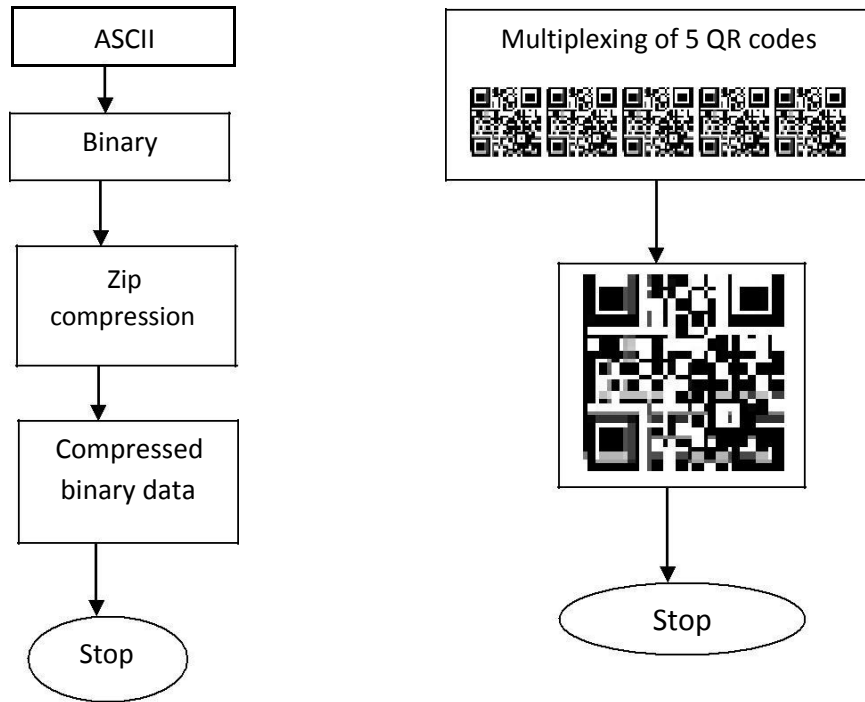
1. The text is converted into ASCII values,
2. Convert these ASCII values into binary,
3. Apply Zip compression on these binary digits,
4. Take this compressed data which is compressed binary data after that last step is to collect the data.

Afterwards, Second algorithm is Multiplexing algorithm. In this algorithm:-

1. Take simple any QR code,
2. Multiplex 5 QR codes and take as input than generate single output. With this step the data is more stored in single QR code.
3. Collect that single QR codes which is generated from above multiplexing and take that single QR code as final output.
4. Than Stop the algorithm.



Further, Author suggested as a future work that data is converted into codeword's than in some special characters after that in last apply multiplexing (five QR codes multiplex in one code). Compression algorithm and Multiplexing is given as following:







**Fig. 2.1:** Compression and Multiplexing Algorithm

Nutchanad Taveerad , Sartid Vongpradhip "**Development of Color QR code For Increasing Capacity**" [7] focused on various features of Bar codes and QR codes in Detail. Author explained if we choose color QR codes instead of black/white than it should more secure and store more data. It will also help to increase the capacity. Simple quick response code store 1 bit in each module but color code store 16 colors in 4 bit. Author purposed a model in which they used 8megapixel camera for encoding and java platform for decoding. In this paper [7] the author explains the capacity and efficiency of color QR codes. As we studied that there are many properties of black/white quick response codes. But in this paper we can see that these color QR codes are also very interesting. The simple 2d structure of QR codes contains two main

parts function pattern and encoding region. But the author used HSV in his model. This HSV is Hue, Saturation and Value where Hue explains the no of colors from 0<sup>0</sup> to 360<sup>0</sup> Color explains the range of color like red start from 0<sup>0</sup> and so on, Similarly Saturation explains the amount of gray in all colors. Here Value depicts the brightness of any color. In black/white where the color capacity of 100 modules, but in color ones that capacity may be 360 n particles. At the end the author wants to say that with his research of color QR codes have great accuracy and readability and also there is different decoding process because the scanner firstly read the image color than decode the QR code.

**Table no: 2.2** Color QR Code with HSV.

Image	Device	Source	Accuracy(%)
	Mobile devices	Camera	75
	Personal Computer	File	100
	Mobile devices	Camera	100
	Personal Computer	File	100

B Karthikeyan, Abhilash Choudary Kosaraju, Sudeep Gupta S " **Enhanced Security in Steganography using encryption and Quick responses code**" [8] focused on confidentiality of data. This paper is collection of Cryptography and Steganography . The author purposed a model in which first step at sender side is encryption second is encoding third is scrambled that QR code fourth is exchange least significant bit and at last apply Steganography and found stego-image. Similarly, for receiver side take that stego-image descramble it and decode it and at last decrypt the data. In this paper [8] the author explains the security of Steganography with using QR codes and encryption techniques. The word Steganography depicts the image processing. The author has given two models first for sender and another for receiver. These steps are increasing the security very well because it is very hard to detect these encrypted data's and also quick responses for that. The model for sender side in this paper having 6 steps.1 is taking any message. 2 is encrypted that message with the help of AES -128. 3 is converted that encrypted data into QR code which means encoding is done at here.4 is scramble that encoded data into any form so that security increases.5 is hide most significant bit(MSB) with least significant bit(LSB).6 is create an stego-image with this secured data. Similarly, the model for receiver side is also having 6 steps.1 is take that stego-image from sender.2 is extract the original image from stego-image.3 is descramble that image into original.4 is scan the QR code. 5 is decryption which means using AES-128 message will be decrypted.6 is collecting the original message. At the end the author also given some indications for future work like there may be security enhanced with adding some modification in modules.

Moldovyan Nikolay, Berezin Andrey, Kornienko Anatoly, Moldovyan Alexander "**Bi-Deniable Public-Encryption Protocols Based on Standard PKI**" [9] focused on providing security from both type of attacks like active and passive. Uses some protocols which are not used shared keys. Author purposed a model in which they are using digital signature of sender and receiver instead of sharing keys. Digital Signature are used to authenticate the data. To achieve the authentication is highlight feature of this paper. In

this paper firstly they provide authentication with digital signatures than encryption/ decryption is applied. This paper [9] is on public key encryption with using of standard of PKI. Author first of all explains that a sender and receiver share their data with using of secret sharing key which is very much insecure. That's why Author purposed a model in which first step is to generate personal signature of sender. After that generate a hash function of that signature. Than using secret key mod of that function is done which is considering as a second part of signature. Then comparison is done if the both values are same then receiver take as original message otherwise it will be consider as message send by malicious node.

Priyanka Vadhera, Bhumika Lall **“Review Paper on Securing Hashing Algorithms and its Variants”** [10] reviewed different types of SHA and compared MD-4 and MD-5. Author try to give whole information about secured hash algorithms and also give comparison of their properties. According to message size, words per bit, rounds in different variants, binomial operations and collision occurred in which variant of SHA. The maximum size of message in SHA is  $2^{128}$ , output message size is 256, internal bit size can extend to 512, block size is also extend up to 1024 .The basic binary operations which are performed on these secured hash algorithms are AND, OR, XOR, SHR, ROT. Different no of rounds in different versions of secured hash algorithms like in MD-5 and SHA-224 there are total 64 rounds while in SHA-0, SHA-1, SHA-256, SHA-384 and SHA-512 there are 80 rounds. In this paper [10] the author explains the different SHA algorithms. SHA means secured hash algorithm. Basically it is review paper which explains the different functions of different variants of SHA. SHA is a hash function but it is secured form. There is no collision found and total 64 rounds after that hash is generated. Afterwards SHA-384 and SHA-512 explained. In these algorithms steps output and structure are same also there is no collision found. But no of steps in these algorithms are 80. Author firstly makes comparison between these algorithms after that give a purposed model. This purposed model explains the efficiency, time consuming, amount, collision and bit wise operations of these algorithms. In SHA-0 there are only

160 bits are used and also many shortcomings, therefore SHA-1 come in market. In SHA-1 there also 160 bits but it correct the errors of SHA-0 with simple one bit wise rotation. After that SHA-224 come in this 224 bits used and in 256 there are 256 bits are used but there structures are identical. In end author give his profile.

**Table no: 2.3** Different Hash Algorithms with Properties.

Algorithm Variants	Output	Internal state size	Block size	Max Message Size	Round	Collision
MD5	128	128	512	$2^{64}-1$	64	Yes
SHA-0	160	160	512	$2^{64}-1$	80	Yes
SHA-1	160	160	512	$2^{64}-1$	80	Theoretical attack
SHA-224	224	256	512	$2^{64}-1$	64	No
SHA-256	256	256	512	$2^{64}-1$	64	No
SHA-384	384	512	1024	$2^{128}-1$	80	No
SHA-512	512	512	1024	$2^{128}-1$	80	No

Faten Chaa bane, Maha Charfeddine, William Puech and Chokri ben Amar "**A QR code based audio watermarking technique for tracing traitors**"[11] Explanation of different techniques of watermarking. This paper designed an encoded identifier which is a parallel sequence of two tracing codes: Boneh Shaw and Tardos codes into QR-code. This approach is not for reducing complexity value but also for improves two stage tracing ability and also enhanced security after sender send its data through QR codes. Also shows the graph of time in results with well qualified values.

Mete Eminagaoglu, Ece Cini, Gizem Sert, Derya Zor "**A two factor authentication system with quick response codes for web and mobile application**"[12] Explains the authentication system with web and some android applications. the main motive of this paper to identify two way authentication with the help of QR codes. also create an environment that could be more user friendly. they focused on one time password which would help to authenticate the device with the similarity of today . they have used RSA and ECC and gives future direction to use SSL certificates. at the end author gives his acknowledgment.

Vladimir Hajduk, Martin Broda, Ondrej Kovac, Dusan Levicky "**Image stenograph with using QR code and cryptography**" [13] explains the basic concept of Steganography . The main motive of this paper is to design an image Steganography with high level security. they want to say that main relation between security and capacity is compression model. if we apply compression before encoding an quick response than there must increase capacity and security. Efficiency of the designed methodology was measured by Peak Signal-to-Noise Ratio (PSNR) and achieved results were compared with other Steganography tools.

V. Ramya, G. Gopinath "**Review on quick response in the field of information security**" [14] Explanation of usage of information security in quick responses . This paper described about full details of QR codes, their Structures and the current state-of-the-art, it means how the Quick Response Codes are used in the field of Information security. Our examine Additionally looks at those Different intangibility aspects for example, such that top sign should clamor Ratio, intend square Error, Normal Difference, greatest Difference, Normalized outright slip In light of pixel quality built information concealing method and the discoveries are introduced.

Dan chia-Tien Lo, Kai Qian, Wei Chen "**Mobile security education on portable labs**"

[15] Explains the different types of education system security in portable labs. Versatile platforms empower learners should take in done an advanced connection when they would utilized as educating support devices to PC science (CS) or majority of the data engineering organization (IT) training. Meanwhile, mobile security is an important topic in security curricula partly due to the popularity of consumer mobile devices and a shift in computing landscape towards mobile devices' apps development. Due to the rapid demand and popularity of mobile devices [2-3], Those security of portable registering is indispensable of the developing guard of clients Furthermore for what's to come about our social, monetary What's more political frameworks.

## **CHAPTER 3**

### **SCOPE OF STUDY**

---

Quick Response codes due to its security features and storage capacity the most important usage in today's Era is data authentication and confidentiality. These codes are scanned by android phones and also we know the usage and demand of these mobile phones are increasing day by day. In Achieving secured data transformation one should surely feel helpful with the usage of these QR codes. Because these codes are medium of secured and authenticated communication.

The scope of security in mobile phones of QR codes ecosystem with using PKI and Hash algorithms is to maintain a secured data communication and gives a platform to applications of android phones [17] which are very much important in our daily life. As the technology increases and shortage of time is also becoming a big issue, to resolve these type of problems the QR codes are very much helpful.

It is feasible to carry out the proposed work with the facilities available in-house. QR Codes can be easily generated using various web based applications and it can be read using any Smartphone having Camera. So, encoding and decoding of the QR codes can be done using various free and open-source tools.

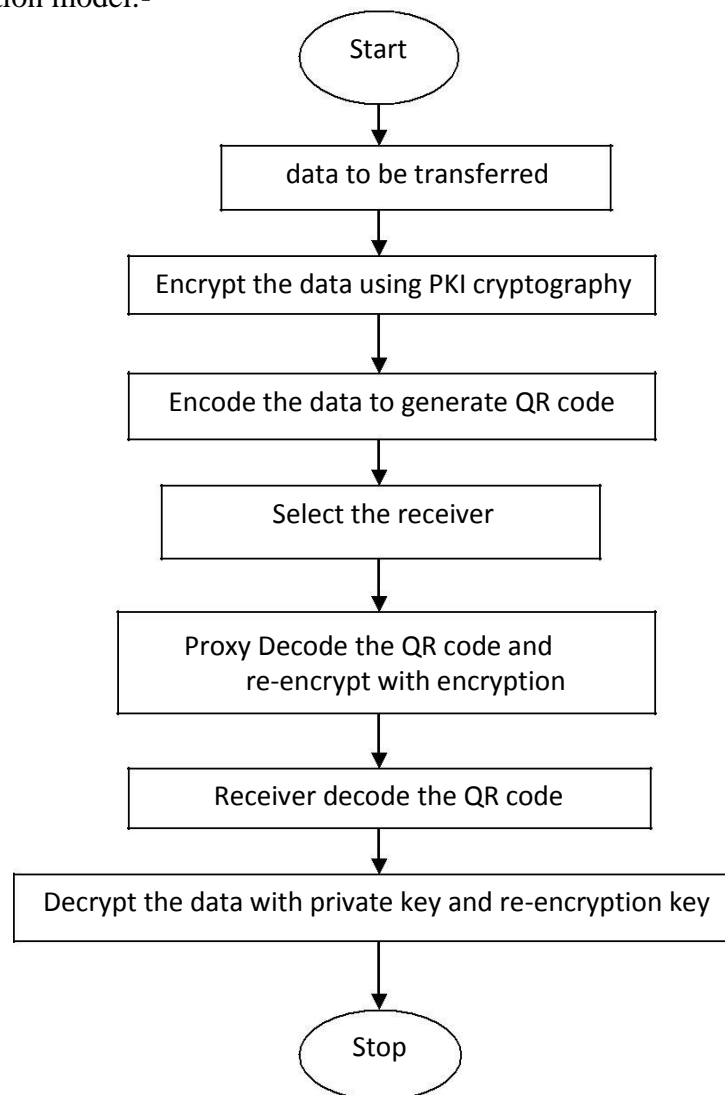


## CHAPTER 4 PRESENT WORK

---

From researching all about QR codes and security related it i have studied four models which are existed models related to QR codes. they can be come under related work of this thesis work. they are as follows:- Proxy re-encryption model, Model for data compression, Model for Multiplexing and Model for Stego images.

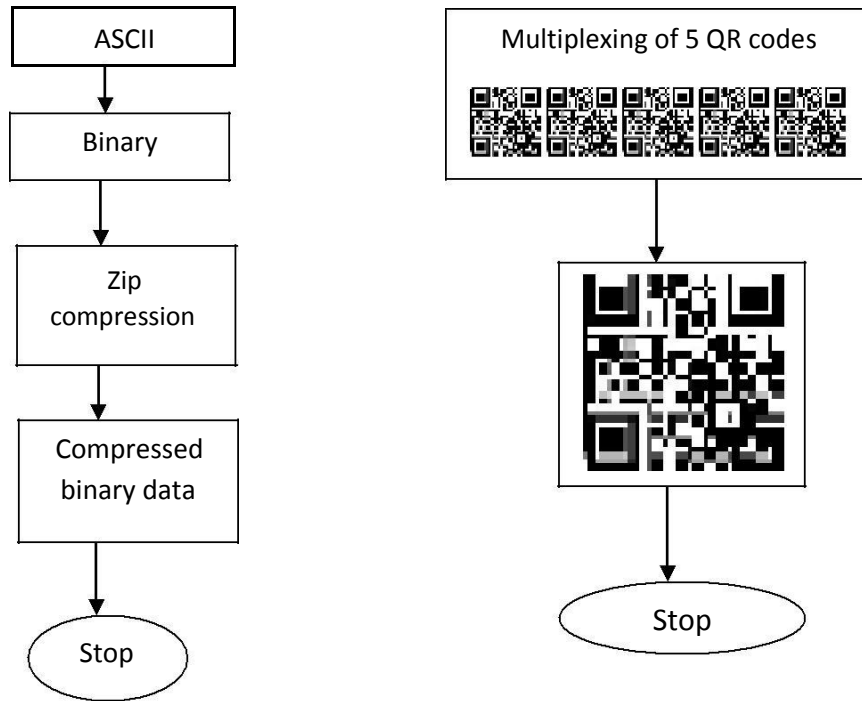
Proxy re-encryption model:-



**Fig. 4.1:** Proxy Re-Encryption

In this model author simply purposed an model in which first message is encrypted with pki than encode it in quick response code than select the receiver and after that proxy selects that message and re-encrypt with encryption. at last receiver receives and decode and decrypt it.

Model for data compression and model for multiplexing:-



**Fig. 4.2:** Compression and Multiplexing.

At last the fourth model is stego-image [19] model:-

In this model there are different outputs and inputs for sender and receiver. like-wise for sender side:-

- Take simple message.
- Encrypt with AES.
- Encode this encrypted into QR code.
- Scramble this encoded data.
- Hide most significant value to least significant value.
- Finally found the stego image.

Similarly for receiver side:-

- Take that Stego image.
- Extract that image.
- Descramble the extracted image.
- Scan that QR code.
- Decrypt the message.
- Found original message.

#### **4.1 PROBLEM FORMULATION**

After Studying all above existed models i have done lots of research on QR codes and its security than i decided to do increase mobile security [25] with these QR codes with the help of PKI and Hash algorithm. there is one thing different which i have achieved during my implementation work is database. i have included the concept of database which is worked at backend and stored all the information regarding hash and encryption/decryption.

What is the difference between base paper and our paper?

In base paper there is a concept of valid date and certification. they have set the date of message validity. It works as last date at which the specific message is encrypted or decrypted but after this date the message will not considered as valid.

After valid date there is a concept of algorithm may contain public key algorithms for authentication.

Afterwards they used the concept of signature. this signature is simply digital signature which are designed electronically. at last they design they QR code which contains the encoding and decoding process.

But in our purposed technique there is concept of converting the given message into ASCII values afterward encrypted it with PKI and then it is secured with Hash algorithm SHA1. after that we create an QR code which is encoding process and decode it with that app.

## **4.2 OBJECTIVES OF STUDY**

After studying enormous security and storage features of Quick Response codes it is observed that despite of wide range of applications but there are also some area which defines more properties which are under research and maintenance. The objective of the study is to design a technique to nullify any malicious attack on the mobile phone [23] information with the help of malicious QR codes, which is done by the help of PKI and Hash Algorithms. Further objectives are summarized below:-

1. Basic functionality of QR code life cycle.
2. Exploring the security in Quick Responses and issues related to malicious QR codes attacks .
3. Study the working of Mobile phone applications, Public Key Cryptography, Hash Algorithms.
4. Develop an android platform to read and scan Quick Response codes with the secured data which is get from PKI and Hash algorithm as output and test through simulation.

### **4.3 RESEARCH METHODOLOGY**

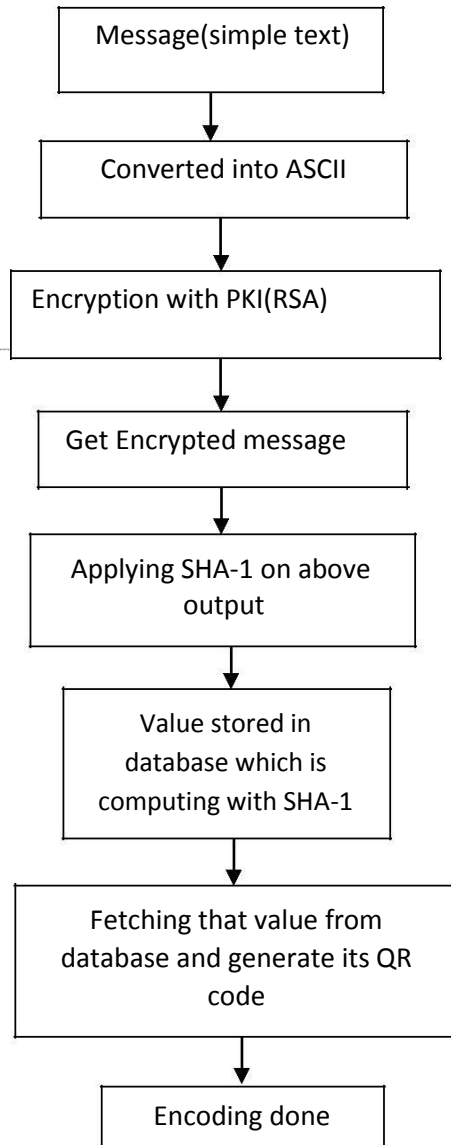
In this chapter we are discussing about the methodology in such way that reader should understand that in what way the author design his research implementation. Research Methodology is what? Research Methodology is simply author's Analysis regarding Research, Motivation in Research, Significance of Research, Research Process and

Hypothesis. Let's start one by one. Research Analysis is study of different papers and books that author completed to define his new research topic. Motivation in research is simply the work efficiency that has to complete your work. Significance of Research is usage and effectiveness of your work we can say that what is the importance of your work or research. Process is simply your Flowchart of work and pseudo code of your research. Hypothesis is simply mean by your expectation from research. In every report and research the Research Methodology is play very wide role because due to this point the reader should clear and get detailed knowledge about author's research plan. Firstly, we are discussing about sender side.

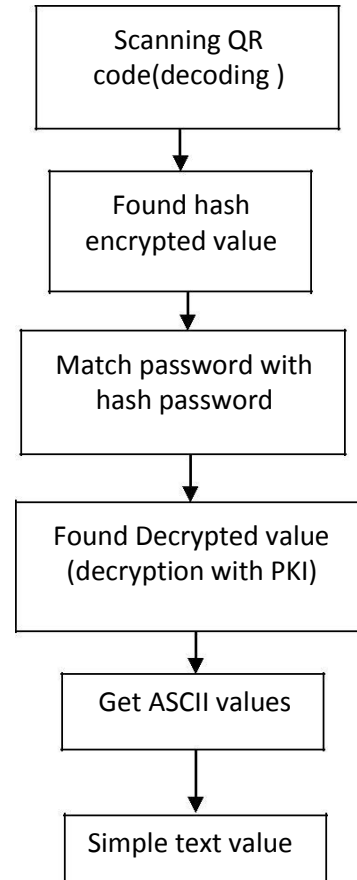
In my Research Methodology At sender side firstly take original message which may be any text and alphabets. Than in second step converted it into ASCII value just for data security. After that apply PKI which may be RSA or ECC and Hash Algorithm any Secured Hash Algorithm for data authentication and confidentiality. Afterwards take that encrypted data as a input and encoded it with programming in Android Studio. Last step of sender side is to take that input and generate an QR code in android studio.

Similarly, At receiver side firstly take encoded data(QR code) and converted it into decoded form(Scanned QR code). After that decrypt with applying PKI and Hash Algorithm for converting it into ASCII value. Afterwards take that ASCII value which is found from decrypted data and converted it into original message. Hence Encryption/Decryption take place.

Flow chart Direction for sender side:-



Flow chart direction for receiver side:-



**Fig. 4.3:** Flow Charts for Research Methodology.

PKI and Hash Algorithms are used to achieved data authentication and confidentiality. Afterwards, use android studio to design the application with above input.

#### **4.3.1 RESEARCHING**

After purposed model our next step is research which includes all research i have done on QR codes, PKI, Security, Mobile phones, Hash algorithms and android studio. this section contain all the sites and books which i have prefer to complete my work.

The main useful library is ZXING library. all the coding and designing section is dome with the help of this library. ZXING is open source for bar codes and QR codes in Java coding.

The main aim of this research is to enhance the security of QR codes using PKI and Hash algorithm. I believe this research will result into rapid increase of application domains of QR Codes specially for smart cities [27] where one needs to store bulk data with confidentiality.

After researching on topic one question is arise in my mind that Is it feasible to carry out the proposed work with the facilities available in-house? If yes, please mention how the project/research work shall be carried out?

Yes it is feasible to carry out the proposed work with the facilities available in-house. QR Codes can be easily generated using various web based applications and it can be read using any Smartphone having Camera. So, encoding and decoding of the QR codes can be done using various free and open-source tools. First, I will develop a real-time application (web/mobile/desktop based) to generate and read the QR codes using either PHP or Android platform. There are some open libraries available i.e. qrlib in PHP and zxing in Java for android platform. (Required Duration: 1 month/person). Data Storage- To enhance the data storage capacity of QR Codes version1 to version40, For confidentiality- SQRCs (Secured QR Codes) are already providing small level of stenography and cryptography but that is not sufficient for brute-force attacks as attacker

will always have enough time for cryptanalysis. So for enhanced security, I have implemented public key encryption algorithm like RSA. All these algorithms can be implemented in PHP (web based) or Java (android based) platforms.

After studying QR codes I have decided to work on security of QR codes. Security in QR codes: Security of QR codes is a big issue because they hide the information in dots so it is tough to give more security to these. But this security is possible in many ways like providing Steganography [21] and Cryptography. By applying Encryption/decryption technique we achieve larger security. There are many malicious QR codes which look like the same but they harm the security. Similarly there are some intended users who are unable to detect these types of attacks. Attack possible only in case of malicious cases. There are many ways which give the security to these codes as like by providing tracing codes, by authentication methods [16], by securing the information, by providing benefits in digital education system, by using AES and DES, security against malicious codes, by embedding encrypted techniques etc.

#### **4. 3.2 TOOL FOR STUDY (ANDROID STUDIO)**

For Implementation and complete my research work We will use Android studio. Android studio is a tool used for programming and creation of android phones applications. As my topic is security in android phones so this tool is very much effective for output and throughput. As we know Java language is base of Android studio so Java language is also used to complete this research. Programs of PKI and Hash algorithms are also taken in Java language.

Android studio is a platform which gives you the opportunity to design a android applications. For Implementation and for my complete research work, we are using Android studio. Android studio is a tool used for programming and creation of android phones applications. As my topic is security in android phones so this tool is very much effective for output and throughput. As we know Java language is base of Android studio



so Java language is also used to complete this research. Programs of PKI and Hash algorithms are also taken in Java language. In addition, Android studio supports java language so if we encrypt and decrypt our message in java programming than it should increase the efficiency of our work. When we design our android application we used that encrypted data which increases the data authentication, confidentiality and Authorization. As studied the research paper on QR codes, mobile security, public key infrastructure and hash algorithms the net conclusion is found that secure data transformation is the main key feature which is noticeable point. But all the paper taken the simple alphabetic text as input to encode in the formation of QR codes. Android studio helps to take Android application that input easily and encode it into a QR code formation.

Usage of Android studio :- Android studio is a tool used for programming and creation of android phones applications. [29] As my topic is security in android phones so this tool is very much effective for output and throughput. As we know Java language is base of Android studio so Java language is also used to complete this research. Programs of PKI and Hash algorithms are also taken in Java language. In addition, Android studio supports java language so if we encrypt and decrypt our message in java programming than it should increase the efficiency of our work. When we design our android application we used that encrypted data which increases the data authentication, confidentiality and Authorization.

#### **4. 3.3 USING RSA IN ANDROID**

When we are using RSA encryption technique in android studio than whole coding is done in java files. these coding part done at backend. it means whole encryption/decryption is done at backend. User can see only frontend designing part only if any user interested to see coding than he must clear java at backend. In this we can achieve the data authentication and secrecy because the public and private key known by only sender and receiver. In the figure there is one factor which is known as matching key which is common in private and public key. Basically public key encryptions are used to secure the data and protect from third party nodes because is this case the

malicious nodes are failed to detect the private and public keys. There these encryption techniques maintain the confidentiality and authenticity. These cryptographic algorithms based on mathematical operations like integer factorization and discrete logarithms. There many types of public key encryption algorithms:- RSA and ECC. RSA used to secure the sensitive data. In RSA the integers are used from 0 to n-1 but also for some n. But basically the standard value for this is 1024 bits. Therefore the value of n should be less than  $2^{1024}$ . Thus security of this RSA is also very important. To secure this algorithm basic attacks are which are there which can attack to destroy this algorithm. Like Brute force attack, Mathematical attacks, Timing attack, Hardware fault-based attack, Chosen cipher text attack.

#### **4. 3.3 USING HASH ALGORITHM IN ANDROID STUDIO**

Similarly, When we are using Hash algorithm hashing technique in android studio than whole coding is done in java files. these coding part done at backend. it means whole hashing is done at backend. User can see only frontend designing part only if any user interested to see coding than he must clear java at backend.

These algorithms designed to detect duplicate data and resist from attack. For example when we create an account on Gmail than at that time what password we given to that site, it converted into message digest at the backend. than next time when we given a password to get login the backend message digest is compared with new password which is given by user if the password is matched than you are allowed to login otherwise it shows wrong password if that new entered password is not matched with that message digest. SHA provides fixed length message which is the key point of maintaining data confidentiality. [30] The maximum size of message in SHA is  $2^{128}$ , output message size is 256, internal bit size can extend to 512, block size is also extend up to 1024 .The basic binary operations which are performed on these secured hash algorithms are AND, OR, XOR, SHR, ROT. Different no of rounds in different versions of secured hash algorithms like in MD-5 and SHA-224 there are total 64 rounds while in SHA-0, SHA-1, SHA-256,

SHA-384 and SHA-512 there are 80 rounds. The hash functions accept the value from message and convert it into fixed length and also padded some bits to the end if necessary. Cryptanalysis of hash functions are resolve the problem of collision that's why they are also called as collision resistant. These cryptanalysis works on internal structure of message. These Hash values which are produce from hash functions are maintain the integrity as well as authentication [16].

### 4.3.4 TESTING

Firstly, we have done only simple QR code generation and scanning and According to our research methodology the given text is encrypted with public key encryption and that it goes to hash page for input and creating an password at frontend and saving it at backend database. Now we have covered all the points of purposed algorithm. we are able to send our value in database and fetching from there for generating QR code. In final output it shows the QR code which is itself stored in mobile phone gallery which is generated from hash algorithm and fetch itself when we click on generate QR code button. Screenshot regarding simple generating and scanning QR code.

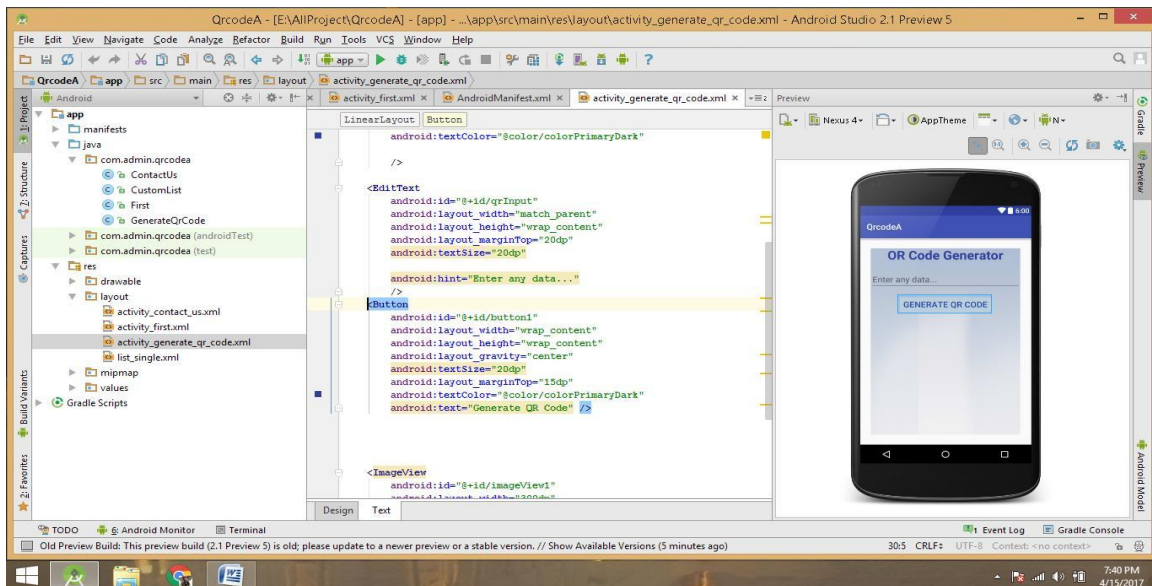
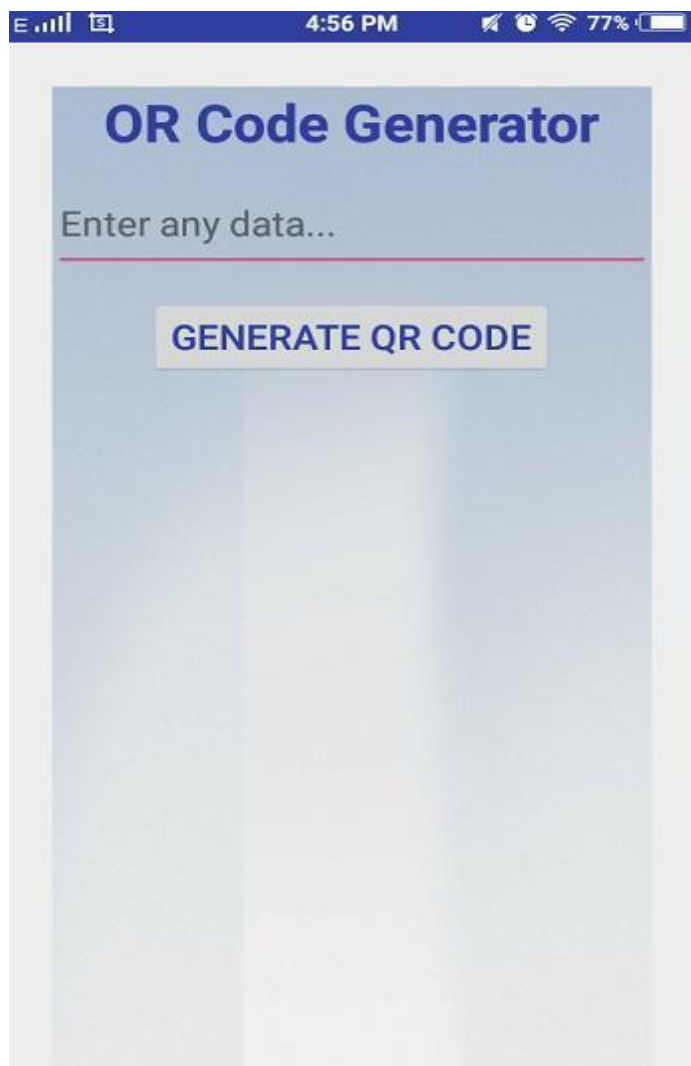
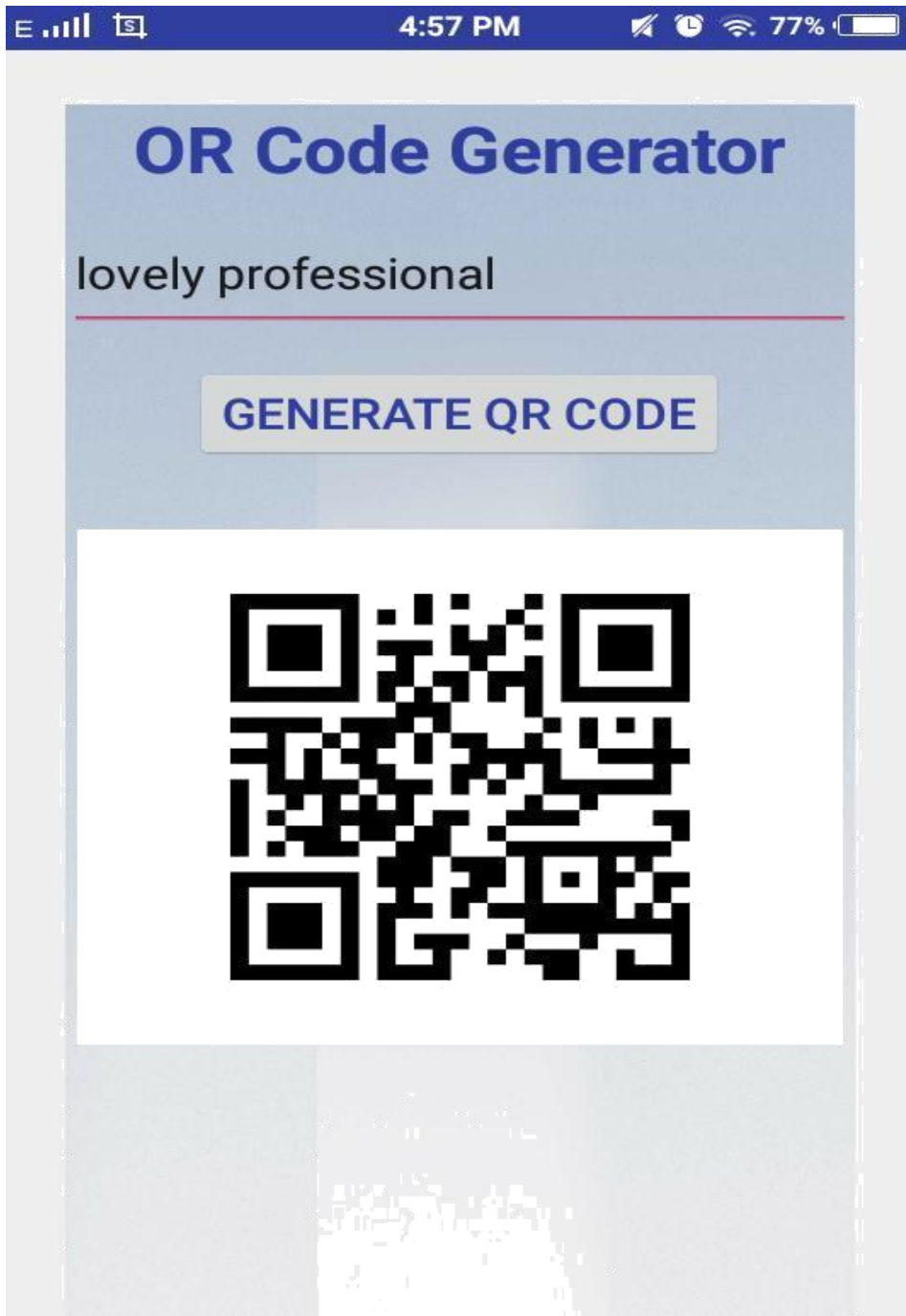


Fig. 4.4 : Screenshot to Test Project.

In this image it shows simply generate an QR code and scan it. Firstly it opens the first page at where we have two list items which are generating and scanning but works as button. then there is another two buttons which are about us and contact us. First button is generating QR code which works as generate the string in black and white pixels in square format. Second button is scanning QR code which works as give same that string in input format.



**Fig. 4.5:** Screenshot to Test Generating QR Code.



**Fig. 4.6:** Screenshot of Generated QR Code.

## **CHAPTER 5**

### **RESULTS AND DISCUSSION**

---

#### **5.1 SOFTWARE ANALYSIS**

After doing research methodology the main facing problem is selection of the software, when once system requirement is under stable then checks that whether a particular software package fits the requirements or not. After Starting Choice further security will be necessary with determine those allure from claiming specific programming compared for other hopefuls. This area initial summarizes the provision prerequisite address et cetera infers additional point by point comparisons.

Those essential point of Investigation may be will get an acceptable seeing of the necessities of the system, the thing that precisely may be fancied from the programming What's more the thing that the imperatives on the result are. Investigation prompts the genuine detail.

Investigation includes interviewing customers and the wind clients. An key and only Investigation will be gathering majority of the data regarding the exhibit framework. The investigator must know what data together, the place on discover it, how will gather information it, the thing that should make from claiming it. The legitimate utilization of devices to gathering data is those enter to fruitful examination. With accomplish this, the 1st major issue is with get necessary data. Those second real issue about examination [18] will be how on sort out the majority of the data got something like that that those data make assessed to culmination and consistency.

For our suite, our team has interviewed a lot of people working there in the different branches of the organization. We ask them about their work in the current system of the organization. We have gathered a lot of information regarding their work for the organization.

We have reviewed the manual records maintained by them and the different documents of the organization. We have collected all these information and sorted them according to

the needs of the modules. We organized all the information in a proper way to remove inconsistencies.

Android Studio provides wizards and templates that verify your system requirements, such as the Java Development Kit (JDK) and available RAM, and configure default settings, such as optimized default Android Virtual Device (AVD) emulation and updated system images. This document describes additional configuration settings you may want to use to customize your use of Android Studio. After the initial Android Studio installation and setup, use the SDK Manager to verify and update the tools, platforms, packages, and other components used by your apps. You can also use the **File > Settings > Appearance & Behavior > System Settings > Updates** to configure the SDK Manager to automatically prompt whenever updates are available.

## 5.2 JAVA

**Java** is pure object oriented general purpose programming language that is totally class base specifically designed to have as few implementation dependencies as possible. It intended to provision developers "write once, run projects toward whatever stage that help java without the have for recompilation. Java provisions are normally aggregated on byte code that might run on whatever java virtual machine (JVM) in any case for workstation structural engineering.

1. Java files- these files are used to coding which stores the no of classes. (src) By default, it includes an Main Activity.java source file which contains activity class that runs when your app is launched using the app icon.
2. Res- it contains all the resources which include:
  - a. Draw able folder(images, designs)
  - b. layout files(.xml files)
  - c. Values which contains colors files, string files etc. these files are used for designing purpose which is a part of whole app design.
3. Gen- This section contains the .R file, a compiler-generated file references all the resources results in your project.

4. Android manifest- it contains the app name, icon, all permissions and activity services.
5. Gradle- it contains all the libraries and SDK version.

### **5.3 ALGORITHM**



For contact page

1. start an package as example harpreet;
2. import android support version app on activity;
3. import android operating sys bundle;
4. set public class content activity.
5. start void on create.
6. set content view and layout activity on contact us page .



for main page

1. start an example harpreet kaur qr code.h
2. import android app action bar.
3. import android app activity
4. import android content and bundle.
5. list the view function as view.
6. start widget list view.
7. start widget text view.
8. import an site on intent integrator.
9. view the results

It simply shows that what so ever button we are using is coded like this. it contains text view and list view which helps to view the text and list under the section of entry at encoded time.



- For generating page
  1. Start the first page on app activity.
  2. Action button on generate qr code.
  3. Similarly button on scan qr code.
  4. create an database as db helper
  5. This db helper saves the generate and scan operation.

It is helping to generate an QR code and scan an QR code button which appears at front of the project. Db helper helps to retain it in database.

- For encryption page
  1. Firstly create an bundle which saves info.
  2. Create saved instance state.
  3. Set content layout activity first page.
  4. Db helper get the data on application context.
  5. Set qr Code Generate (Button) with View By Id (R.id.button1);
  6. set qr Code Scanner (Button) with View By Id (R.id.button2);
  7. Finally create an listener which checks whole operation.
  8. Click on public view.
  9. It will start the first activity.

It is helping to generate an first page which contains the encryption button which starts the process of encryption. and move to next step which is hash algorithm page.

- For scanner page
  1. Firstly create an bundle which saves info.
  2. Create saved instance state.
  3. Set content layout activity scanner page.

4. db helper get the data on application context.
5. set qr Code Scanner (Button) with View By Id (R.id.button2);
6. Finally create an listener which checks whole operation.
7. Click on public view.
8. It will start the scanner activity.

For checking the device of scanner:-

1. Set prompt as scan.
2. Integrate as set camera id.
3. Integrate as set beep enable if it is false.
4. Integrate as set bar code image enable if it is false.
5. Start to initiate scan operation.

It is helping to scan an QR code and its button which appears at front of the project. Db helper helps to retain it in database.

For checking it is null:-

1. Initiate the request code as given
2. Parse this request into results .
3. If the content is null then output will be ==.
4. If the length is very long then show the results.
5. But if recent value is saved in db helper.
6. Make an toast which is sum of result and recent string value.
7. Finally show the results.

It is helping to cancel the query of QR code and its button which appears at front of the project (like cancel).

## 5.4 IMPLEMENTATION

Regarding Implementation:- Main pages in manifest in android. There designing part in java pages and backend coding in res pages in android studio is done till now. According to our research methodology the given text is encrypted with public key encryption and that it goes to hash page for input and creating an password at backend in database. we have covered all the points of purposed algorithm. we have covered that point and our output which is generated from hash algorithm is stored in database and fetch itself when we click on generate QR code button.


For example:-

Let's take a message 'abc'

1- Converted it into ASCII - 001002003

2- Encrypted it with RSA(PKI) - pu9pZ0aYnUH5EqrFFBKfw==

3- Compute with sha(password)

4- Generate QR code- 

5- Scan this QR code.

6- Output is- 001002003.

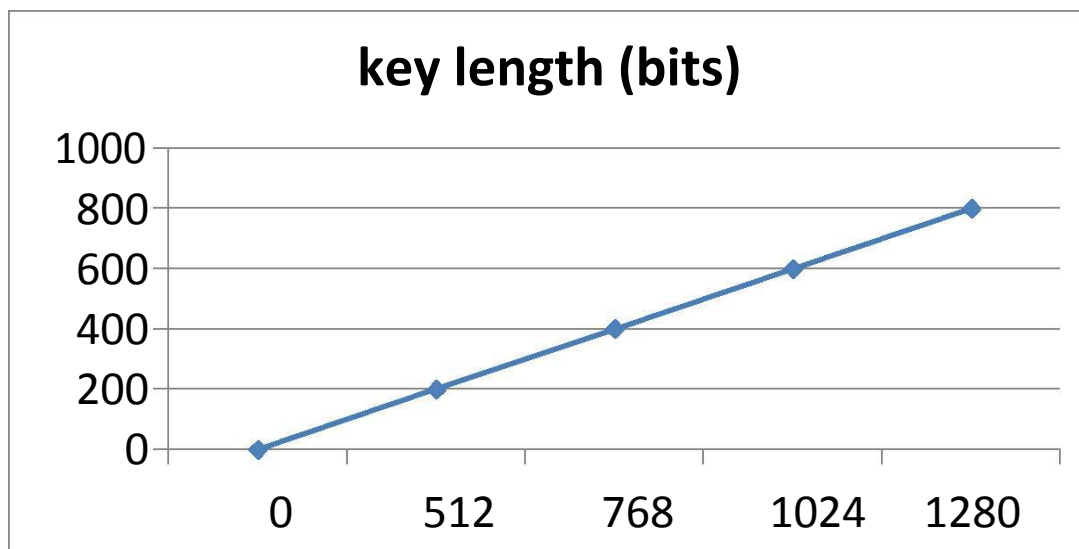


Fig. 5.1: Graphical Representation for Decryption.

In this graph the x quadrant shows the value of key length which is measured in bits while in the side of y quadrant it shows the decryption time which appears 200 difference with in. this graph values shows that if the key length is increase than the decryption time is also increased with in upward direction. suppose an example if we take the value of private key length is 0 than on the other side decryption time is also 0 but if we take the value of key is 512 than the graph must increase in upward direction with the value of 200.

Screenshots regarding research:-

1.

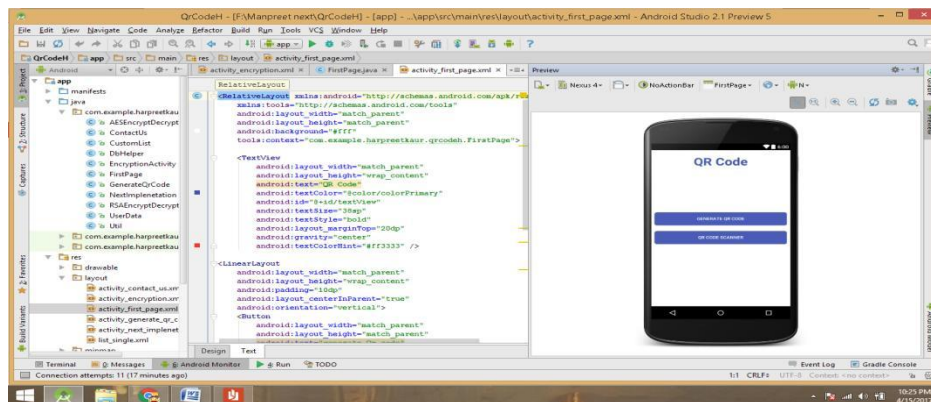


Fig. 5.2: Front Page.

It is first page description which contains the two buttons of generating and scanning QR code, with its coding part.

Pseudo code for front page:-

1. Create a bundle and saved instance state.
2. Set content view in layout. activity page which is first page.
3. With the help of database create an application context().
4. This db helper creates final activity into this.
5. Create an QR code generate button and saves as button 1 and give view function.
6. Create an QR code scan button and saves as button 2 and give view function.
7. Take an listener function which call by these button and view the function.

2.

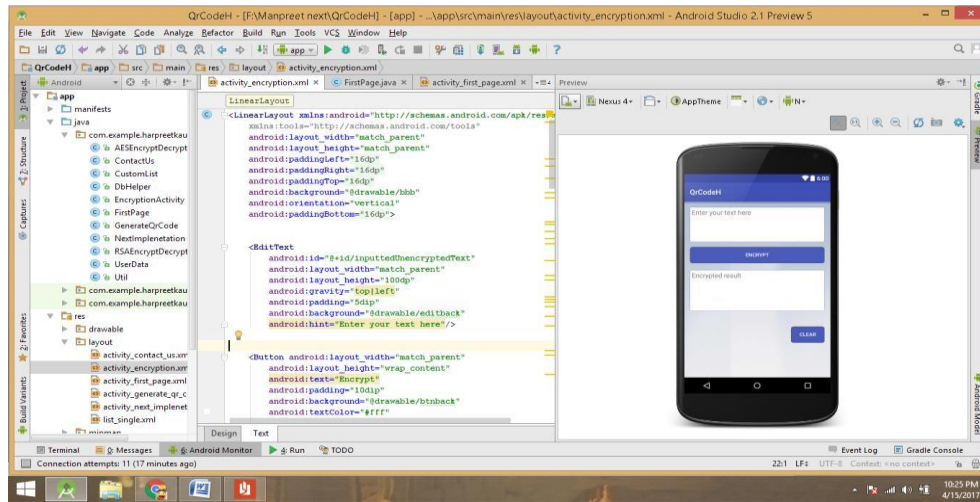


Fig. 5.3: Encryption Page.

Second screenshot it contains the encryption of string with the help of RSA in android studio. It contains the string area and encrypted area which shows the output. one clear button is there which contains the ability to clear out all the data. In this we can achieve the data authentication and secrecy because the public and private key known by only sender and receiver. In the figure there is one factor which is known as matching key which is common in private and public key. Basically public key encryptions are used to secure the data and protect from third party nodes because in this case the malicious nodes are failed to detect the private and public keys. These encryption techniques maintain the confidentiality and authenticity.

Algorithm for encryption page:-

1. Click on public void.
2. It gives the intent of first page class and encryption page class.
3. Start main activity.

3.

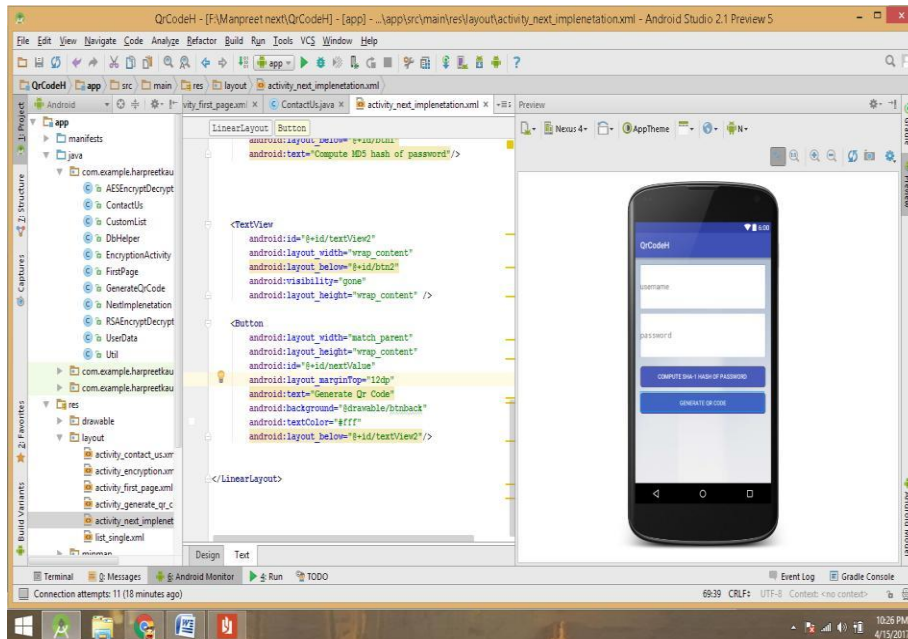


Fig. 5.4: SHA Page.

Third screenshot it contains the information regarding SHA-1 coding in android studio. which basically defines the two sections one is data and another is password. in string or data box there must be encrypted data which is output of PKI and the password must contain that password which is further matched with future password from receiver side. These algorithms designed to detect duplicate data and resist from attack. [20] For example when we create an account on Gmail than at that time what password we given to that site, it converted into message digest at the backend. than next time when we given a password to get login the backend message digest is compared with new password which is given by user if the password is matched than you are allowed to login otherwise it shows wrong password if that new entered password is not matched with that message digest.

4.

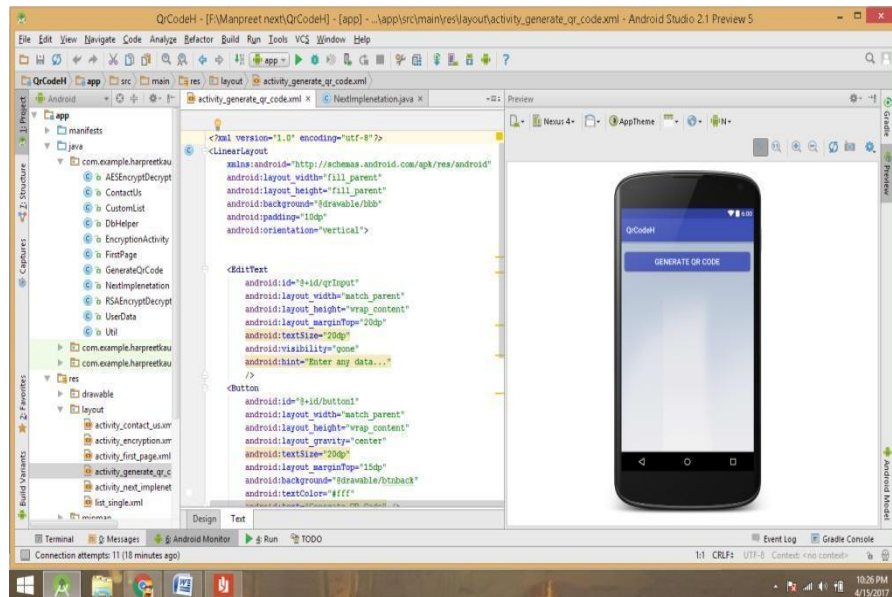
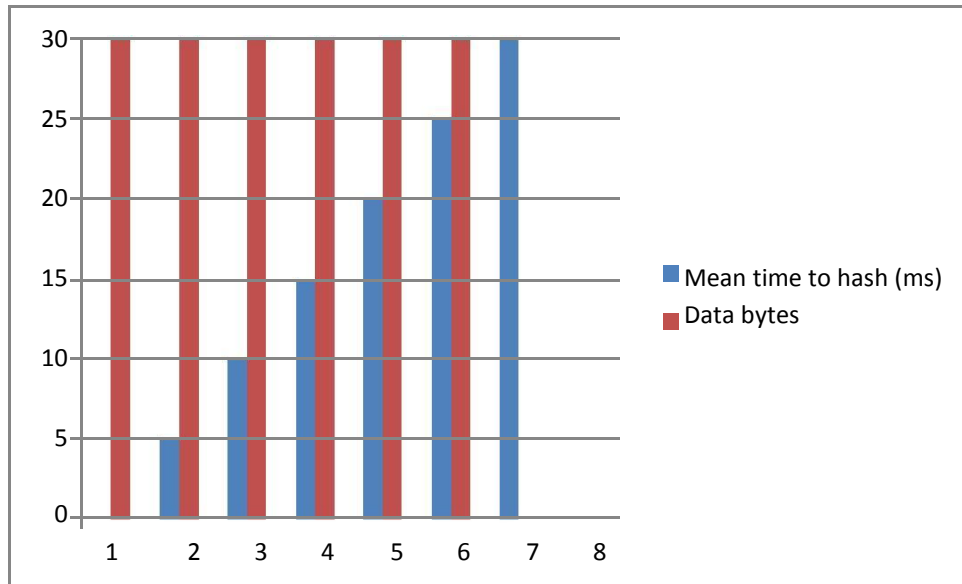


Fig. 5.5: Generating Page.

The data encoded in these codes according to ISO/IEC 18004:2006. They are two dimensional so they give more properties in storage and security in comparison with Bar codes. Because the Bar codes are one dimensional, they store information in both sides while QR codes store the data within both horizontal as well as vertical direction.

5.



**Fig. 5.6:** Graphical Representation of Hash Values.

In this graph the x quadrant shows the value of data bytes which is measured in bytes while in the side of y quadrant it shows the mean time to hash (ms) which appears in 5 points difference with in. this graph values shows that if the data length is increased than the mean time is also increased in upward direction. suppose an example if we take the value of data length is 4096 than on the other side mean time to hash is also increased with 5 points but if we take the value of data is 8192 than the graph must increase in upward direction with the value of 10.



## **CHAPTER 6**

### **CONCLUSION AND FUTURE WORK**

---

As Studied the Research paper on QR codes, Mobile Security, Public Key Infrastructure and Hash algorithms the net conclusion is found that secure data transformation is the main key feature which is noticeable point. In This Paper, Quick Response codes add lots of data which is in secret form so the usage of QR codes is very much important. If this security is achieved with the help of Cryptography and some hashing techniques than data transformation should also very much secure. In this research we will try to increase mobile ecosystem security using PKI and apply any Hashing technique. Then for more security we will generate QR codes are own application in android studio with above secured data then the security of these codes will increased and also they increased the efficiency, integrity, authentication, confidently and also TTL(time to live) value too.

Future Direction- After reviewing all above papers it is clearly confirm that there are many options to increase the security of QR codes. Because these codes hide lots of information which is not easily readable. In future directions we can plan an calculation which holds any cryptographic techniques along with Steganography techniques. Also we can increase the storage space of these codes using with color code techniques and compression techniques.

## **LIST OF REFERENCES**

### **I. BOOKS**

- [1] Stallings William "Cryptography and System Security (Standards What's more act)" commissioned adaption from the united states edition, sixth version distributed Eventually Tom's perusing Pearson instruction 2014.
- [2] Stallings William "Cryptography and Network Security (Principles and Practice)" Indian edition published by Dorling Kindersley, Sixth Edition India Pvt. Ltd. Copy right 2011.
- [3] Stallings William "Cryptography and Network Security( Principles and Practice)" First Indian Reprint 2003 Third edition, This edition is manufactured in India and is authorized for sale only in India, Bangladesh, Pakistan, Nepal, Srilanka and the Maldives.
- [4] Stallings William "Cryptography and Network Security (Principles and Practice) " Fourth Edition, Copyright 2006 by Pearson Education, Inc. This edition is published by arrangement with Pearson Education.

### **II. RESEARCH PAPERS**

- [1] L. Roger Yin, Jiazhen Zhou, Maxwell K. Hsu " Redesigning QR code Ecosystem with Improved Mobile Security" 2015 IEEE 39th Annual International Computers, Software & Applications Conference.
- [2] Saud Alotaibi, Steven Furnele, Nathan Clarke "Transparent Authentication System for Mobile Device Security: A Review" The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)
- [3] Saranya K., Reminaa R. S., Subhitsha S. "Modern Applications of QR-Code for Security" 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.
- [4] Akhil N. V, Athira Vijay, Deepa S Kumar "QR Code Security Using Proxy

- Re-Encryption" 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].
- [5] Krombholz Katharina, Fuhwirt Peter, Rieder Thomas, Kapsalis Ioannis, Ullrich Johanna, Weippl Edgar "QR Code Security-How Secure and Usable Apps can Protect Users Against Malicious QR Codes" 2015 10th International Conference on Availability, Reliability and Security.
- [6] Mona M Umaria, G. B Jethava " Enhancing the Data Storage Capacity in QR code using Compression Algorithm and achieving Security and Further Data Storage Capacity Improvement Using Multiplexing" 2015 International Conference on Computational Intelligence and Communication Networks.
- [7] Nutchanaad Taveerad , Sartid Vongpradhip "Devlopment of Color QR code For Increasing Capacity" 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems.
- [8] B Karthikeyan, Abhilash Choudary Kosaraju, Sudeep Gupta S " Enhanced Security in Steganography using encryption and Quick responses code" This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.
- [9] Moldovyan Nikolay, Berezin Andrey, Kornienko Anatoly, Moldovyan Alexander "Bi- Deniable Public-Encryption Protocols Based on Standard PKI" This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.
- [10] Priyanka Vadhera, Bhumika Lall "Review Paper on Securing Hashing Algorithms and its Variants" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358
- [11] Faten Chaa bane, Maha Charfeddine, William Puech and Chokri ben Amar "A QR code based audio watermarking technique for tracing traitors" 2015 23rd European Signal Processing Conference (EUSIPCO).
- [12] Mete Eminagaoglu, Ece Cini, Gizem Sert, Derya Zor "A two factor

authentication system with quick response codes for web and mobile application" 2014 Fifth International Conference on Emerging Security Technologies.

- [13] Vladimir Hajduk, Martin Broda, Ondrej Kovac, Dusan Levicky "Image stenograph with using QR code and cryptography" 26th Conference Radioelektronika 2016, April 19-20, Košice, Slovak Republic.
- [14] V. Ramya, G. Gopinath "Review on quick response in the field of information security" IEEE - International Conference on Advances in Engineering and Technology-(ICAET 2014).
- [15] Dan chia-Tien Lo, Kai Qian, Wei Chen "Mobile security education on portable labs" 978-1-4799-8454-1/15/\$31.00 ©2015 IEEE.
- [16] Partiksha Mittra, Nitin Rakesh "A Desktop Application of QR code for Data Security and Authentication".
- [17] L. Roger Yin, Zhuo Zhang, Mitchum Senior, Nicholas Baldwin "Perceived Security Risks of Scanning Quick Response Codes in Mobile Computing with Smart Phones".
- [18] Saroj Goyal, Dr. Surendra Yadav, Manish Mathuria "Exploring Concept of QR code and its Benefits in Digital Education System" 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India
- [19] Sayantan majumdar, Abhishek maiti, Asoke nath " New Secured Steganography Algorithm using Encrypted Secret Message inside QR<sup>TM</sup> Code: System implemented in Android Phone" 2015 International Conference on Computational Intelligence and Communication Networks.
- [20] Chaitya B. Shah, Drashti R. Panchal "Secured Hash algorithm-1: review paper" Volume2,IssueX,Oct2014 ISSN 2320-6802 .
- [21] B Karthi keyan, Abhilash choudary kosaraju, Sudeep Gupta S "Enhanced Security in Steganography using Encryption and Quick response code" IEEE WiSPNET 2016 conference.

- [22] Milan Schmittner, Mathias Hollick "X castor: secure and scalable group communication in adhoc networks" 978-1-5090-2185-7/16/\$31.00 c 2016 IEEE.
- [23] Ailin Zeng "Discussion and research of computer network security" Journal of Chemical and Pharmaceutical Research, 2014, 6(7):780-783.
- [24] Jie shan "Analysis and research of computer network security" Journal of Chemical and Pharmaceutical Research, 2014, 6(7):874-877
- [25] Sutapa sarkar, Brindha M. "High Performance network Security using NIDS Approach" I.J. Information Technology and Computer Science, 2014, 07, 47-55 Published Online June 2014 in MECS (<http://www.mecspress.org/>) DOI: 10.5815/ijitcs.2014.07.07
- [26] Ranjan Pal, Leana Golubchik and Konstantinos Psounis, Pan hui "Will Cyber- Insurance Improve Network Security? A Market Analysis".
- [27] David Anderson Karl Reiners, Charmaine Barreto "Post-Secondary Education network Security: Results of Addressing the end user Challenge" Proceedings of INTED2014 Conference 10th-12th March 2014, Valencia, Spain.
- [28] Anupriya Shrivastava et al, "Network Security Analysis Based on Authentication Technique" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 11-18.
- [29] Priyanka Sharma al. "Reviewing MANET Network Security Threats" International Journal of Recent Research Aspects, ISSN: 2349-7688, Vol. 1, Issue 2, Sept. 2014, pp. 25-30
- [30] Rajeev Sobti, DR. G. Geetha "Analysis of SHA-3 Final round candidate Algorithm and Design of Variant to skein hash family".

## APPENDIX

### Used Abbreviations:-

- 1) **QR** - Quick Responses- They are two dimensional so they gives more properties in storage and security in comparison with Bar codes.
- 2) **PKI** - Public Key Infrastructure- PKI is basically a policy or procedure, which is used to manage, distribute and store of digital signature. As the name depicts the main motive of PKI is to transmit secure electronic data.
- 3) **SHA** - Secured Hash algorithm- In secured hash algorithms very first step is padding, where as padding means adding extra bits in original message so that it become multiple of 512 bits. Than with encryption technique one message digest is formed which is further compared with next time entry.
- 4) **QRC** - Quick Response codes- These contains same steps as QR but in coded form.
- 5) **SQRC**– Secured Quick Response codes- They are also same as QR Codes but they are in secured forms. therefore they are called as secured QR codes.
- 1) **TTL** –Time to live- It is a time period at which they arrival packet is alive. after this time the packet or data is discarded.

### Glossary

Xing library - The main useful library is ZXING library. all the coding and designing section is dome with the help of this library. ZXING is open source for bar codes and QR codes in Java coding.

The main aim of this research is to enhance the security of QR codes using PKI and Hash algorithm. I believe this research will result into rapid increase of application domains of QR Codes specially for smart cities where one needs to store bulk data with confidentiality.

## Features of bar code, QR code and SQRC:-

1. Bar code:- Full form - bar code , Data capacity - Up to 10-20 numeric digit, Readability- no.
2. QR code:- Full form - quick response code, Data capacity- up to 7089 numeric digit, Readability- yes.
3. SQRC:- Full form - secured quick response code, Data capacity- up to 7089 numeric digit, Readability- yes.

