ENCRYPTING THE EMAIL USING RSA

ANUPAM KUMAR THAKUR
18BIT0003

10. Write a program with necessary GUI to encrypt any given file or data using strong asymmetric encryption algorithm such as RSA and compare it with another method.

You can communicate your email Without any worry of being attacked as it is end to end encrypted

THE PROBLEM

#when the mail is sent it may or may not be encrypted

#Gmail is still not truly end-to-end encrypted, where only the communicators can read the contents of the email

email was not designed with *any* privacy or security in mind

Amazingly, email sent using those wide-open methods still (mostly) works.but it is prone to attecker

#

PROBLEM

How to communicate securely

SOLUTION

#ENCRYPTED DATA IS SENT TO FIREBASE DATABASE WITH THE RSA PUBLIC KEYS

ANYONE TO WHOM THE AUTHOR WANT TO SHARE THE MESSAGE HAVE TO DOWNLOAD THE APP

#APP WILL DECRYPT THE FILE AND AND DISPLAY THE MASSAGE THAT THE

#GIVEN MESSAGE IS ONLY DECRYPTED BY THE PERSON HAVING KEYS
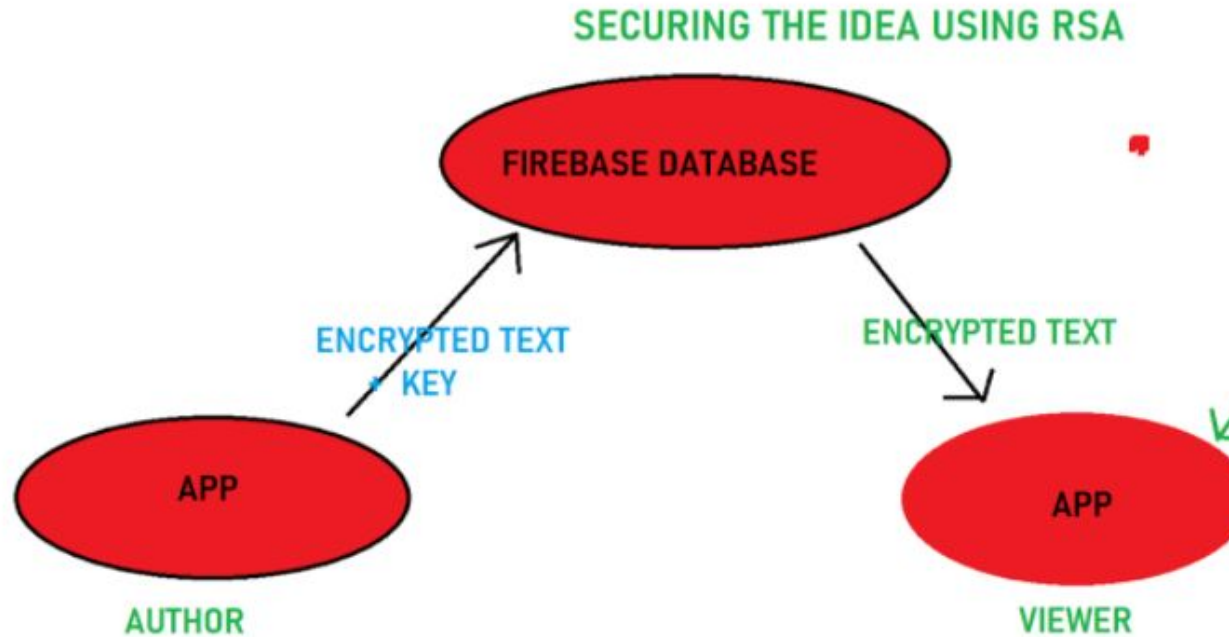
MESSAGE WILL SHOWN TO USER

SOLUTION

#WE HAVE ALSO SECURED THE GROUP MAIL WHEN ONE PERSON SEND MAIL TO MANY PEOPLE

#SO IN OUR SYSTEM THE APP WILL RECIEVE THE PUBLIC KEY FROM ALL

THE RECEIVER AND THEN THE SAME MAIL WILL BE ENCRYPTED USING DIFFERENT KEYS SO EVEN IF ONE RECIEVER SYSTEM COMPROMISED THE OTHERS WERE REMAIN PROTECTED

SOLUTION

SECURING THE IDEA USING RSA

LANGUAGE

FRONT END : ANDROID STUDIO,JAVA

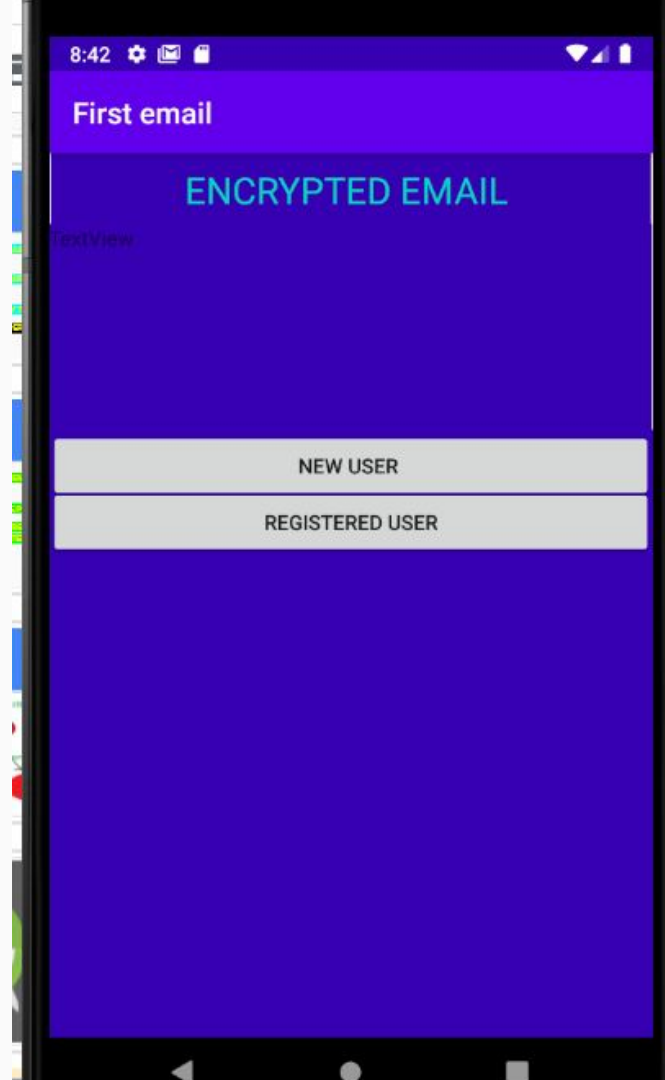BACK END: FIREBASE ,LOCAL STORAGE

ENCRYPTION: RSA AND DES

Welcome page

it has two button
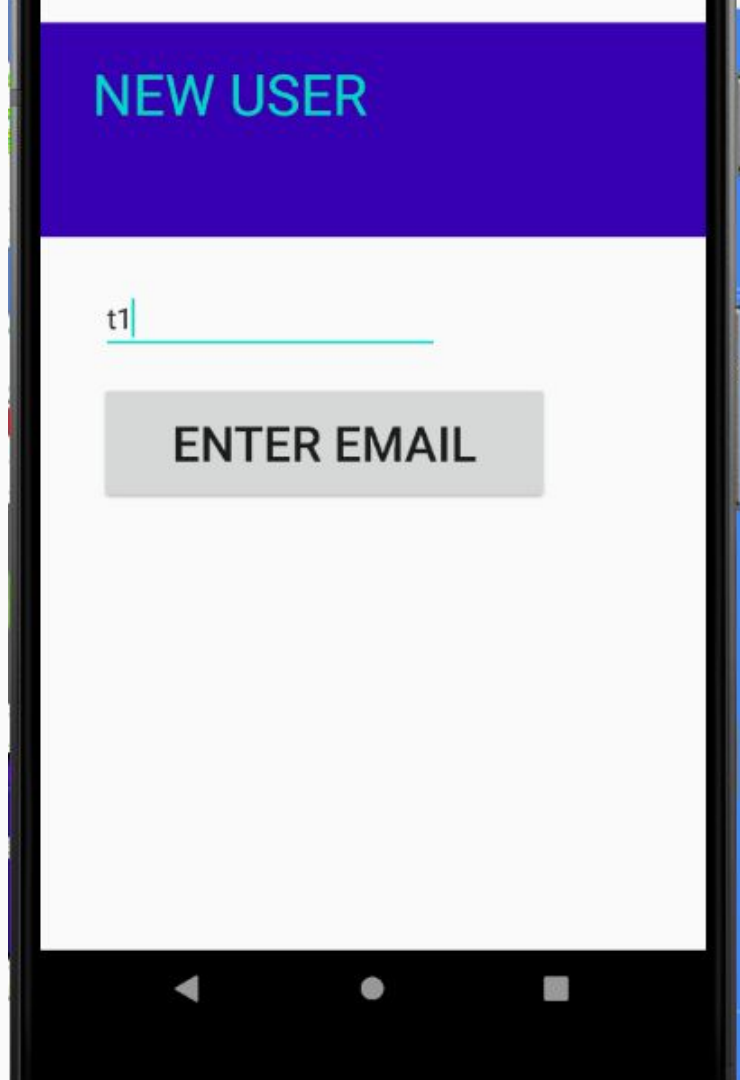
new user -: if the user is not registered with us

#Registered user: if the user is already registered with us

New user

#user has enter a user id to registered with us

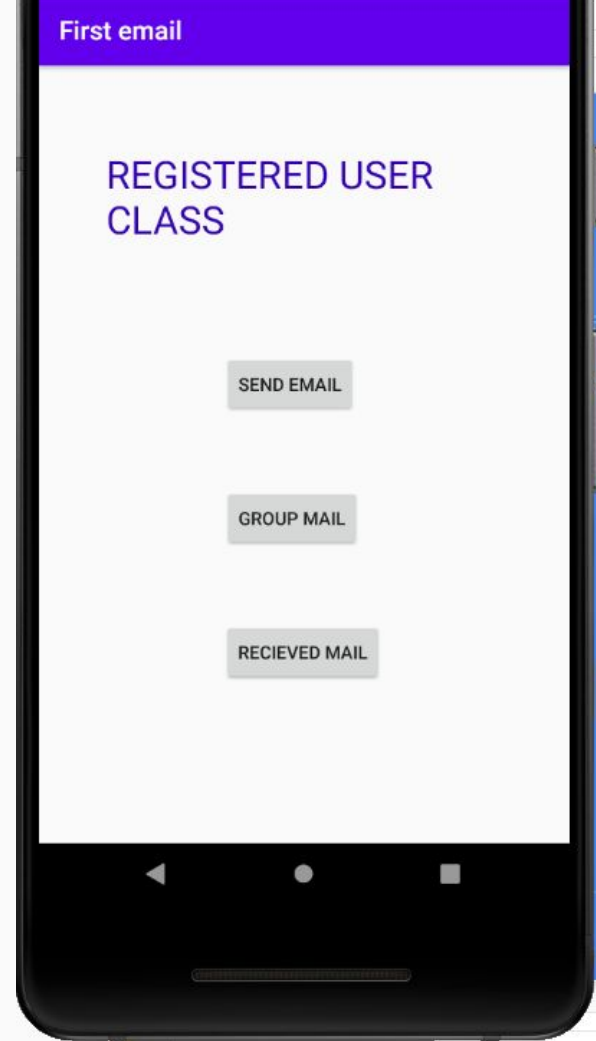# here we are registered t1 and similarly we have t2,t3

Registered user class
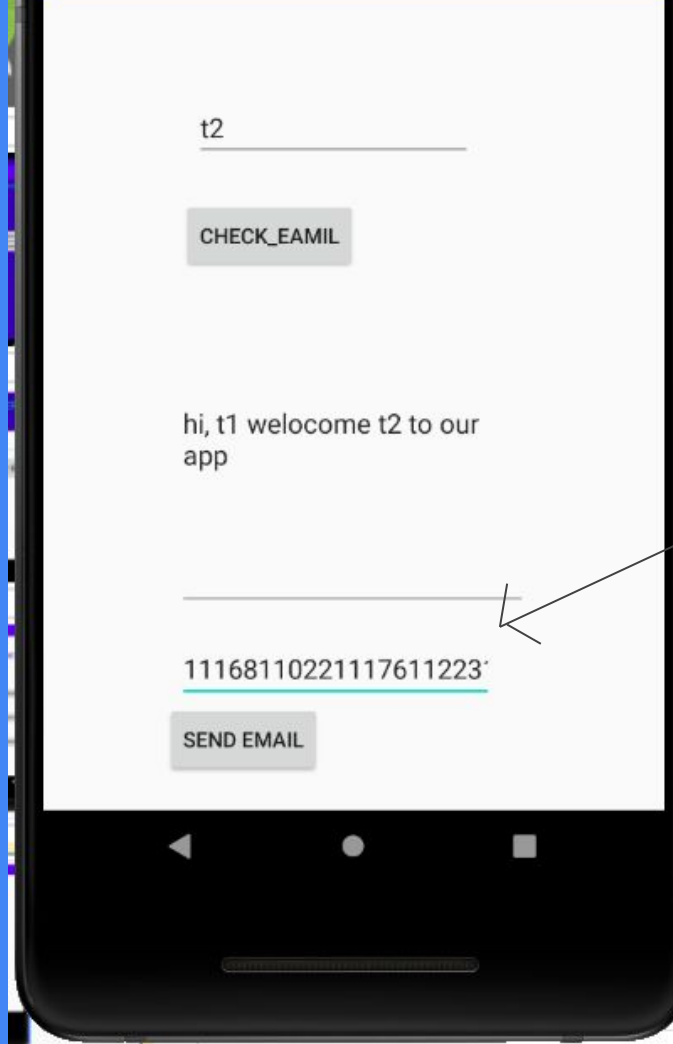
It has three section

#Send email

#Group mail

#Received mail

Send mail

here check mail button check that the receiver mail is registered with us or not

#then , t1 send a mail to t2 that "hi t1 welcome t2 to our app"

t2

CHECK_EAMIL

hi, t1 welocome t2 to our app

11168110221117611223

SEND EMAIL

the email is encrypted with the t2 public key and
And encrypted text is shown here
And this is send to the server
server also cannot decrypt it
only receiver can decrypt it with his public key

First email

Encrpted text{t1=1116811

DECRYPT MAIL

1223112411100611006 -

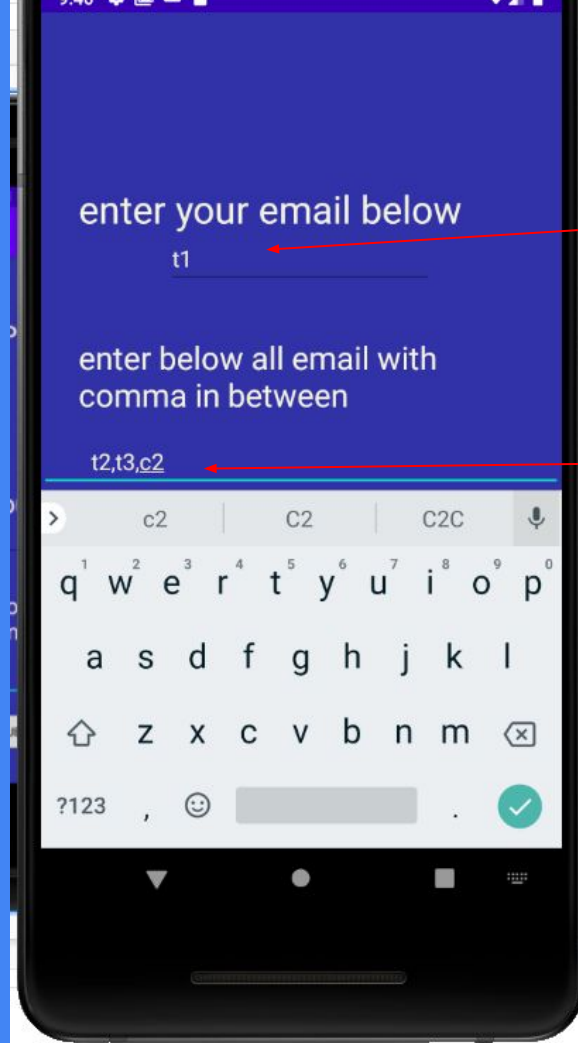**Encryptrd no**

RECEIVED MAIL

t1:hi, t1 welocome t2 to our app

It is encrypted text receive from server In email:encrypted text format

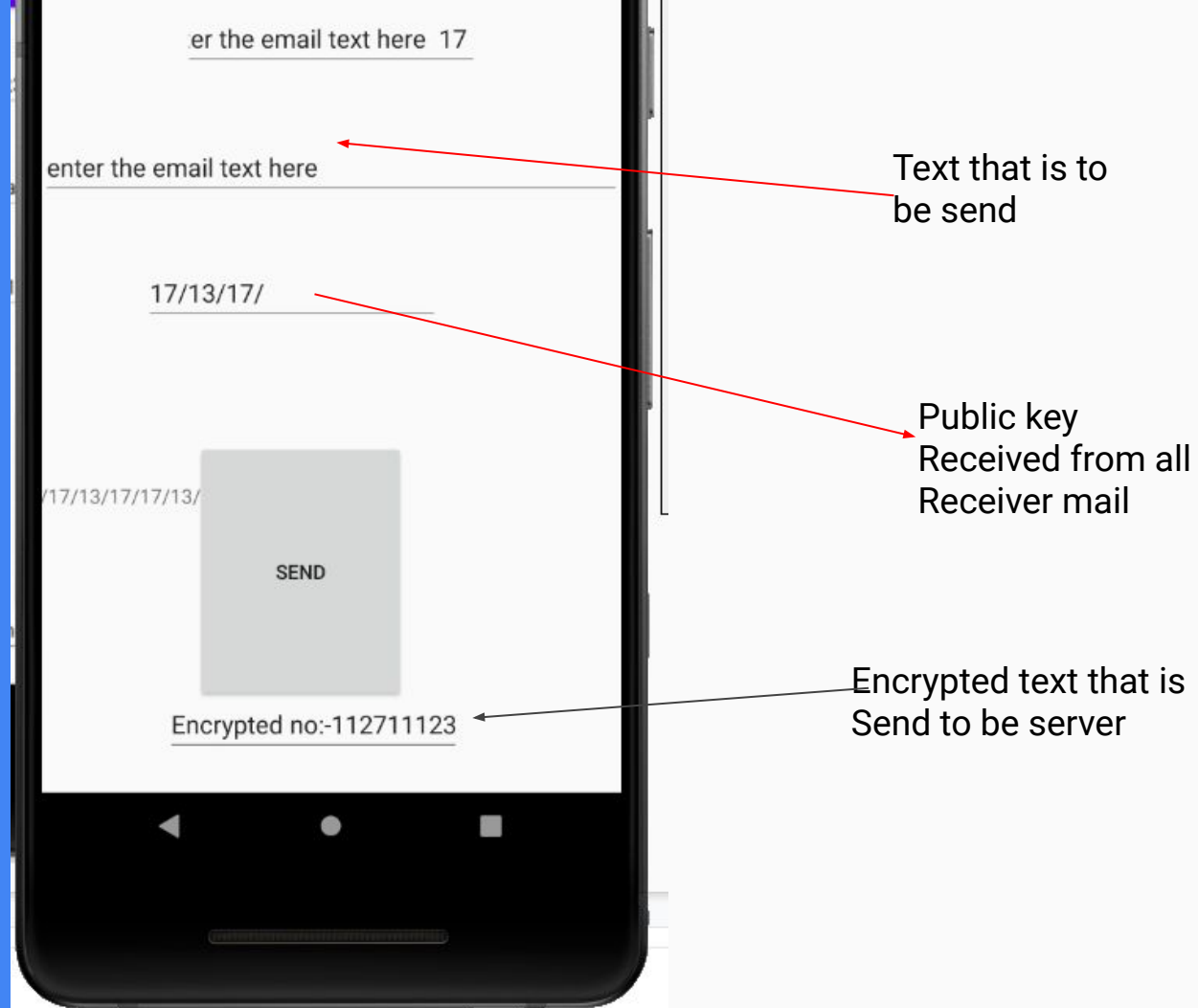Encrypted no that need to be decrypted

Decrypted text

Group mail class

enter your email below

t1

Enter the mail of sender

enter below all email with comma in between

t2,t3,c2

Enter the mail address of all receiver with a comma in between

Group mail class

er the email text here 17

enter the email text here

17/13/17/

/17/13/17/17/13/

SEND

Encrypted no:-112711123

Text that is to
be send

Public key
Received from all
Receiver mail

Encrypted text that is
Send to be server

THANK YOU