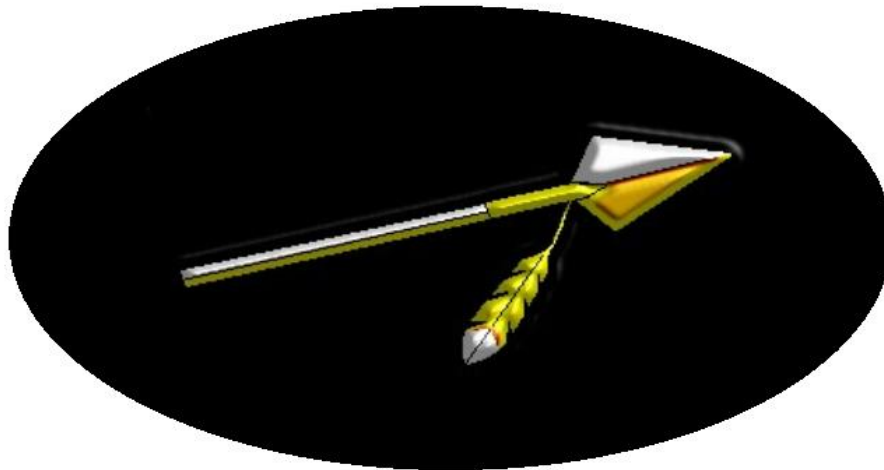


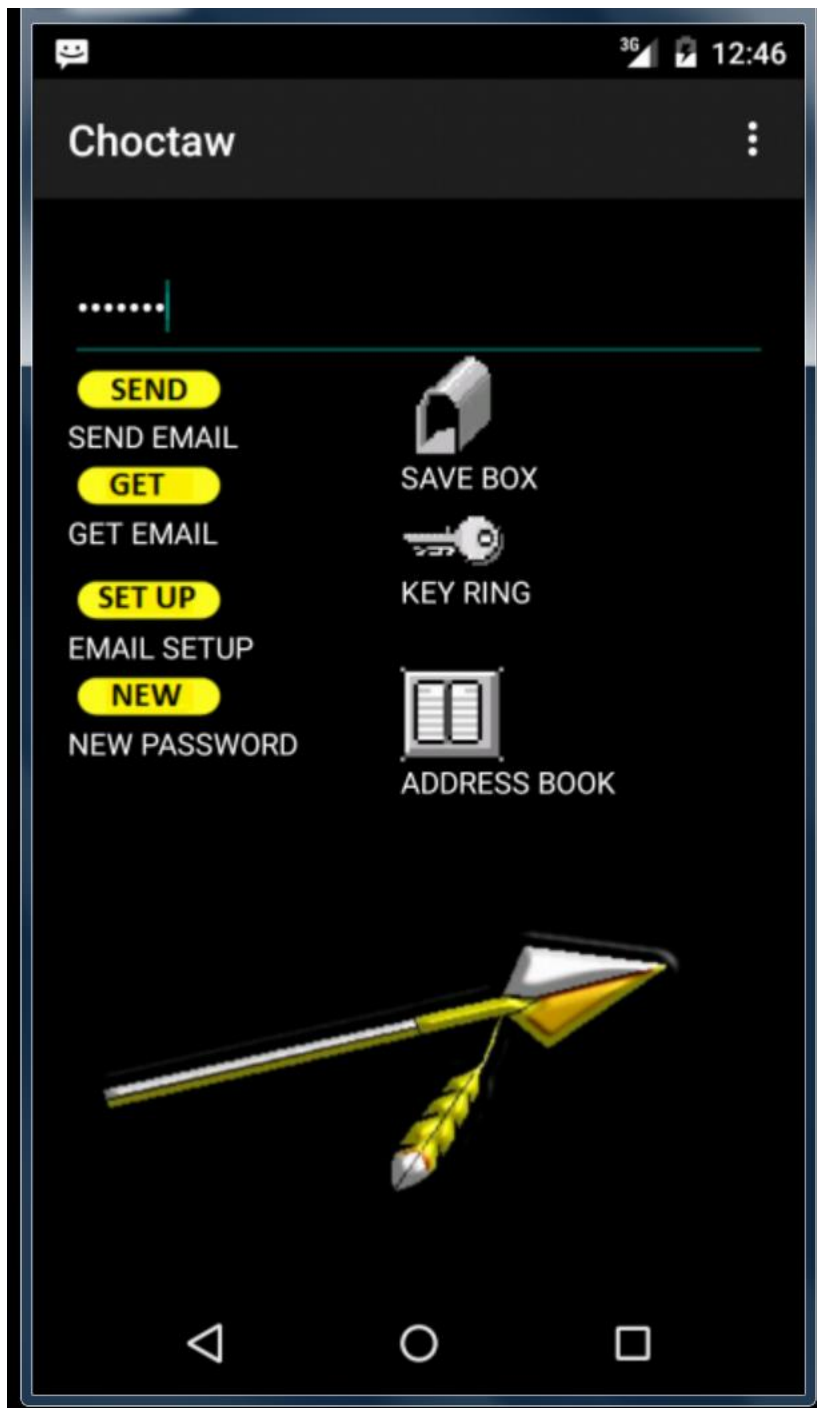
# CHOCTAW



## Secure Email

**SOFTWAR INC.  
PO Box 325  
Manquin, VA 23106  
Information Security**

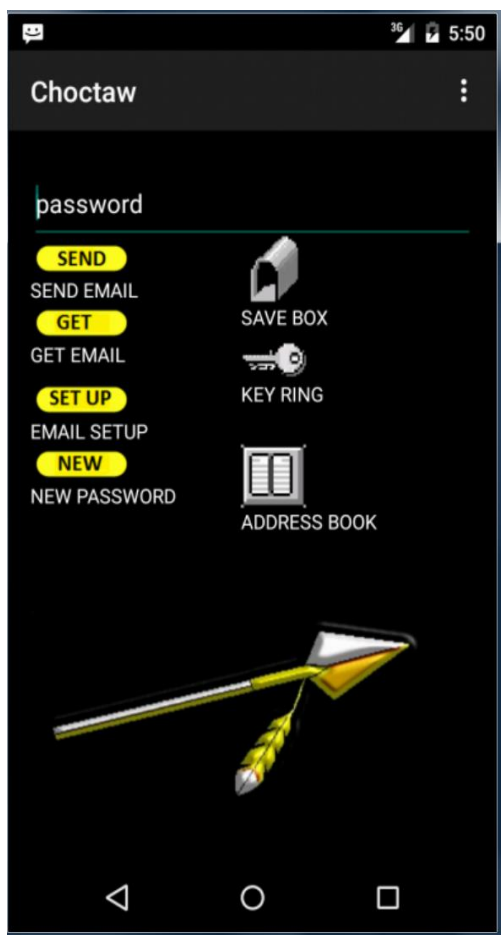
**Softwar Choctaw Secure Email Application © 2017 Softwar Inc. all rights reserved.  
CHOCTAW Secure Email application**



Choctaw provides the ability to manage your email from multiple services and do so in a secure environment. Choctaw cyphers your email data stored on your Android device including inbox, saved messages, email address book and email service provider information. The total security is provided so that any attempt to breach your email stored on your computer is thwarted.

Choctaw is provided with two very powerful cyphering utilities, PDA and CYPHER, which can be used to generate public and private keys. Choctaw provides email to other Choctaw users with the highest levels of cyphering security and provides a nearly seamless method of encoding and decoding messages. Choctaw provides both asymmetric cryptography (public key) and symmetric cryptography (private key) cyphering.

### **GETTING STARTED – Choctaw Main Menu:**



The first item that Choctaw requires is a password to secure the local inbox, address book and email server data. Choctaw requires that you enter your password each time you log in for maximum security. You can enter any password of 8 characters or more.

Keep in mind that all Choctaw email information is cyphered using your log in password. This means that server data, email inbox, and other saved features cannot be accessed from other applications or by unauthorized users.

## EMAIL SET UP



The email setting lists all the email servers and allows you to add or edit any of the server settings.

## ADD/EDIT SERVICE

name

email

pop3 server

smtp server

login ID

password

pop3 port

smtp port

POP SSL

SAVE DELETE EXIT

**Name** – the name of the server for your identification – e.g. “Woopie Email”.

**Email** – the actual email address on this service – e.g. myemail@woopie.com

**POP3 Server** – the POP3 (mail in) service location – e.g. pop.email.woopie.net

**SMTP Server** – the SMTP (mail out) service location – e.g. smtp.email.woopie.net

**Log In ID** – your user log in information – e.g. myemail@woopie.com

**Password** – the password required to log into your email accounts

**POP3 Port** – the POP3 (mail in) port number used by your service – e.g. 995

**SMTP Port** – the SMTP (mail out) port number used by your service – e.g. 465

**SSL** – SSL on if your email service uses Secure Sockets (https)

Items such as POP3 port, SMTP port, POP3 server, SMTP server and SSL settings can be obtained from your email provider. These settings are generally published online by all the major email services. If it is not available online then email your service provider or service administrator for this information. If you have any trouble with these settings feel free to contact us at [softwar@softwar.net](mailto:softwar@softwar.net).



### SAVE

This function saves the service data in the Choctaw database. Always click save after entering any new or updated email service data. All address book entries are cyphered with your startup password/key file. This feature prevents unauthorized access to your address book data.

## **DELETE**

This function will delete the service from the Choctaw database.

## **AUTHENTICATION and TLS/SSL SECURITY**

### **POP SSL**

If your service requires SSL security then turn on the SSL indicator on the service record menu. Choctaw will provide automatic authentication and TLS/SSL security. Choctaw will link up with your service and detect the security requirements so no additional settings are required.

## **SMTP/POP3 SERVICE**

SMTP (mail out) and POP3 (mail in) are often handled by the same email service computer so it is not unusual to enter the same location in both the POP3 and SMTP server fields. Large email service providers often have many computers running separate tasks and may require one location for POP3 (mail in) handling and another location for SMTP (mail out) handling. These email services will require two different settings in the POP3 and SMTP server fields.



## ADDRESS BOOK



This feature allows you to add, change and delete members in the Choctaw cyphered address book. You can use these entries to send and receive email messages, including cyphered messages. Choctaw allows you to enter the name, email and type of cypher used for each secure contact. This allows Choctaw to code and decode messages with others.



**Name** – the name of the member you want to reference in the address book.

**Email** – the email address of the member.

**Phone** – (optional) this is for informational and future use.

**SEND KEY** – select the type of PRIVATE cypher key you want to send messages to this member.

**NONE** – no key

**PASSWORD** – a password of 8 characters or more

**KEY FILE** – any file of your choice (see Cypher Tips section)

**PASTE** – Public key copy/paste from outside source

**RECEIVE KEY** – select the type of PRIVATE cypher key you receive messages from this member. Usually this key is given to you by the member.

**NONE** – no key

**PASSWORD** – a password of 8 characters or more

**KEY FILE** – any file of your choice (see Cypher Tips section)

### **SAVE COMMAND**

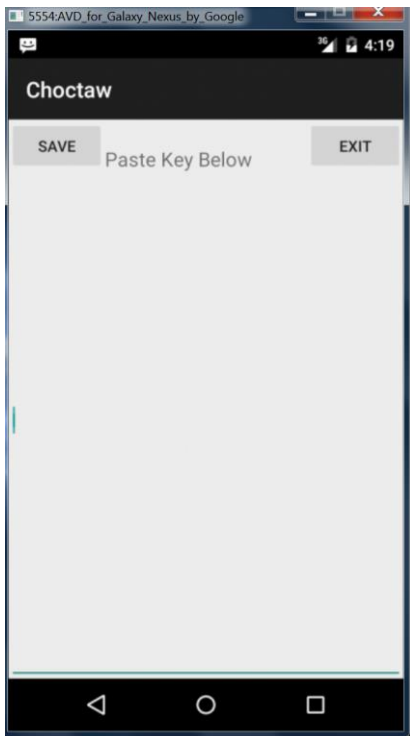
This function saves the entry to the cyphered Choctaw address book. All address book entries are cyphered with your start-up password/key file.

### **DELETE COMMAND**

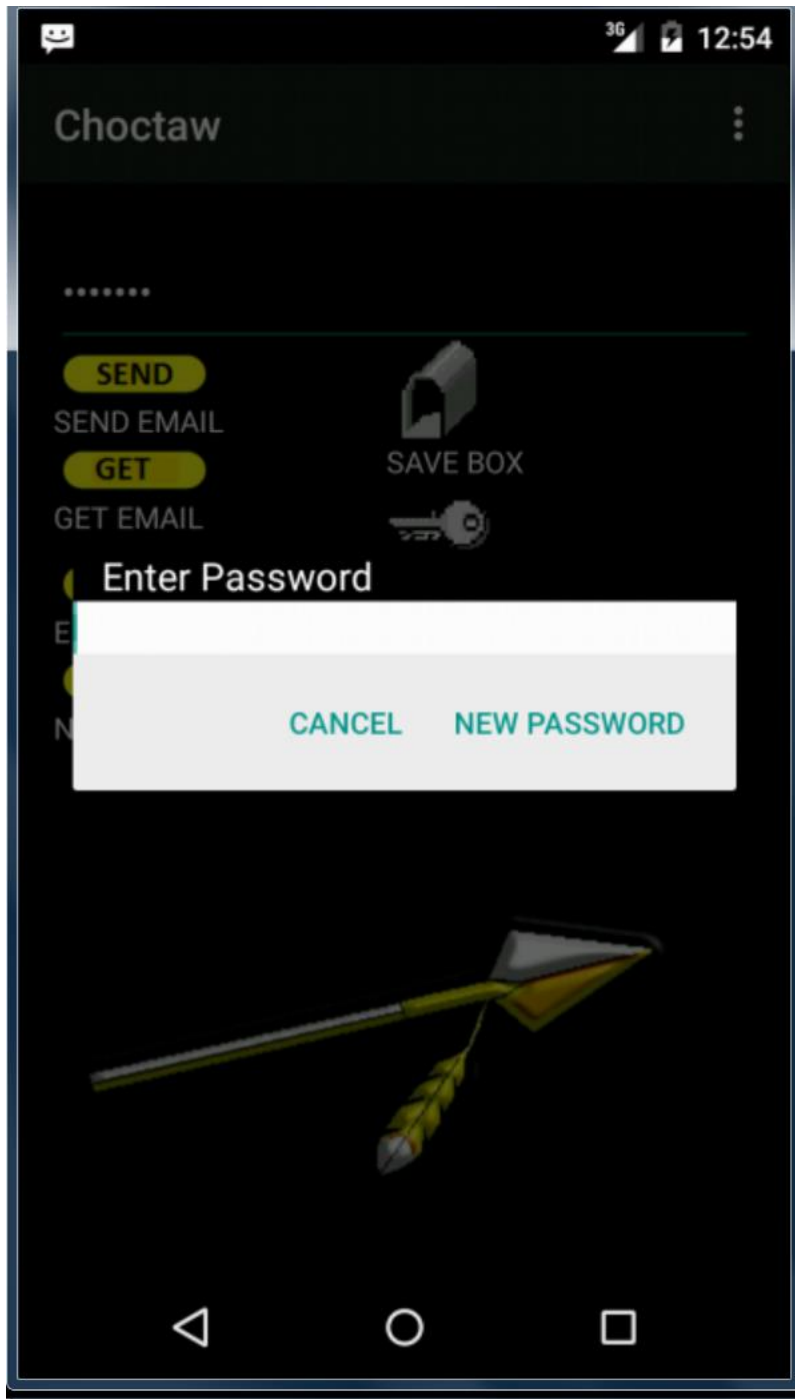
This function deletes the entry from the cyphered Choctaw address book.

### **PASTE COMMAND**

The SEND KEY PASTE command allows you to paste a public key that has been posted on a website or inside a document. SAVE will save the key to the email address in the address book.



## NEW PASSWORD

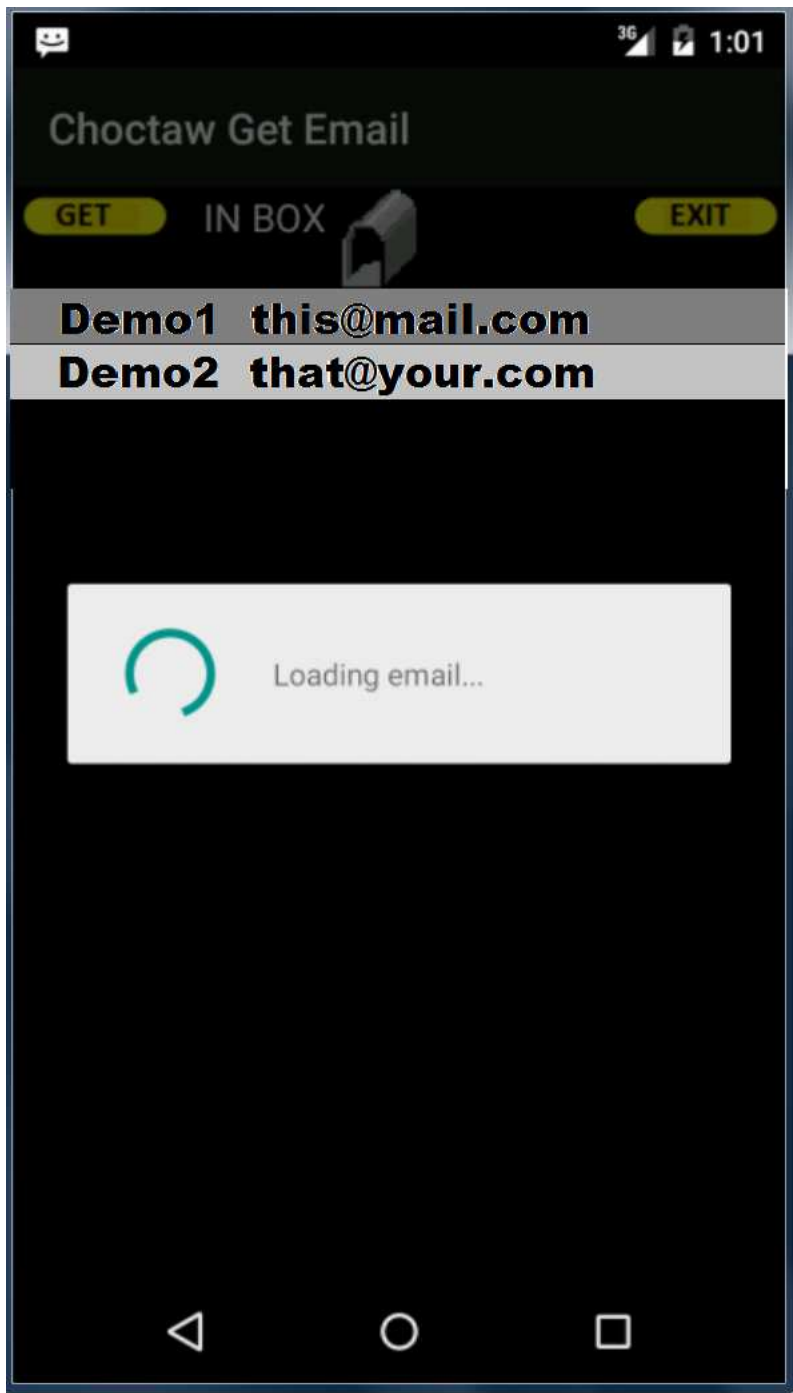


The new password function allows you to change your password to enter Choctaw. The new password must be at least 8 characters. This feature is for your security. It is recommended that you change passwords on a monthly basis.

## GET MAIL



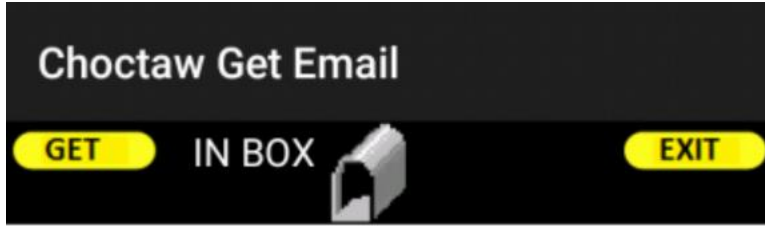
The **GET** function allows you to sign in and retrieve email from selected services. Click on the service you want to get emails from and hit the **GET** command. Choctaw will display a "Loading email..." message while the operation is being executed.



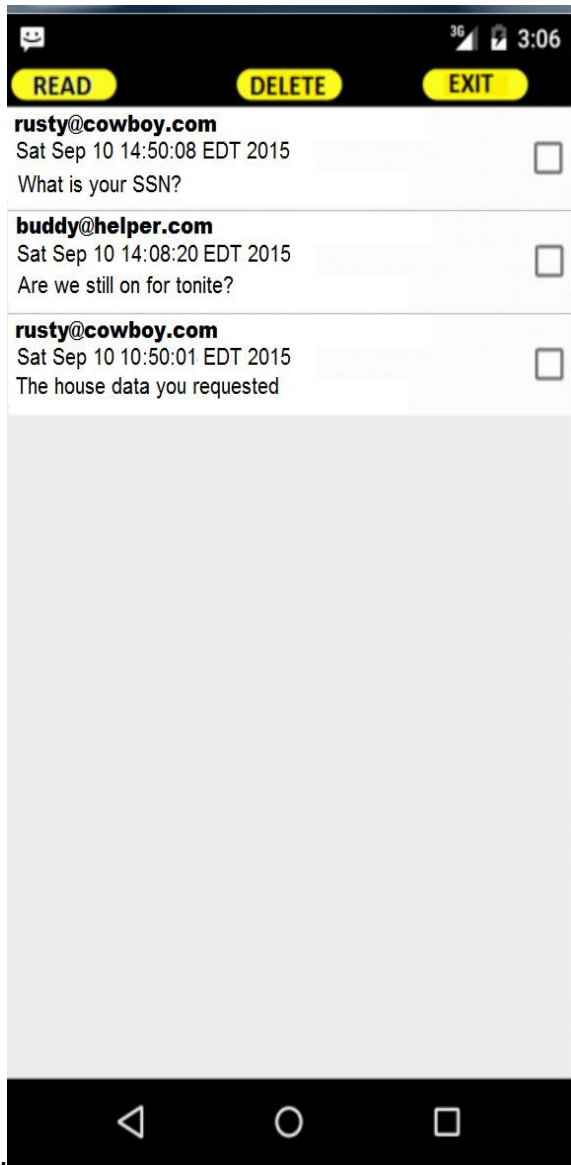
## EXIT

The EXIT function returns you to the Choctaw main menu.

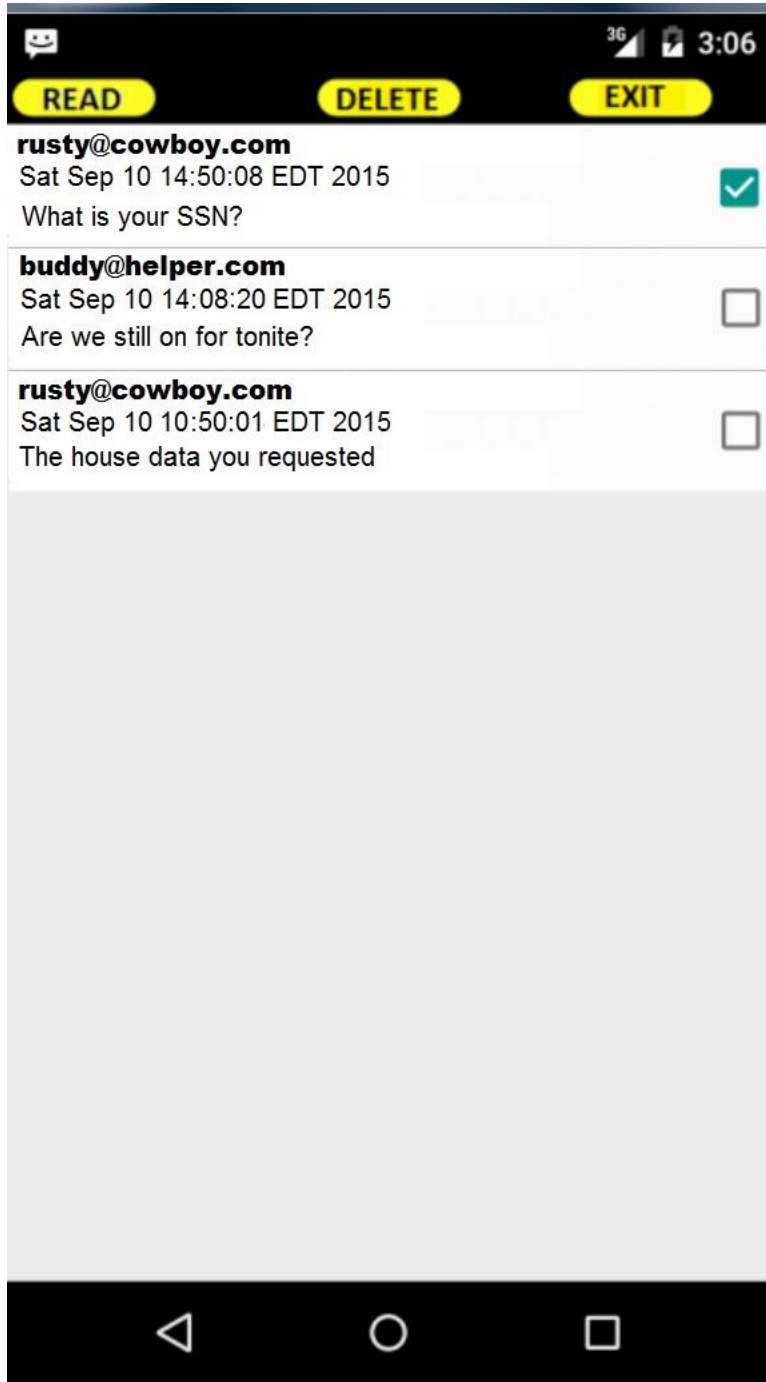
## INBOX



When Choctaw completes the GET email function you can view the downloaded emails by clicking on the INBOX. A list of emails will be displayed with FROM, DATE and SUBJECT columns



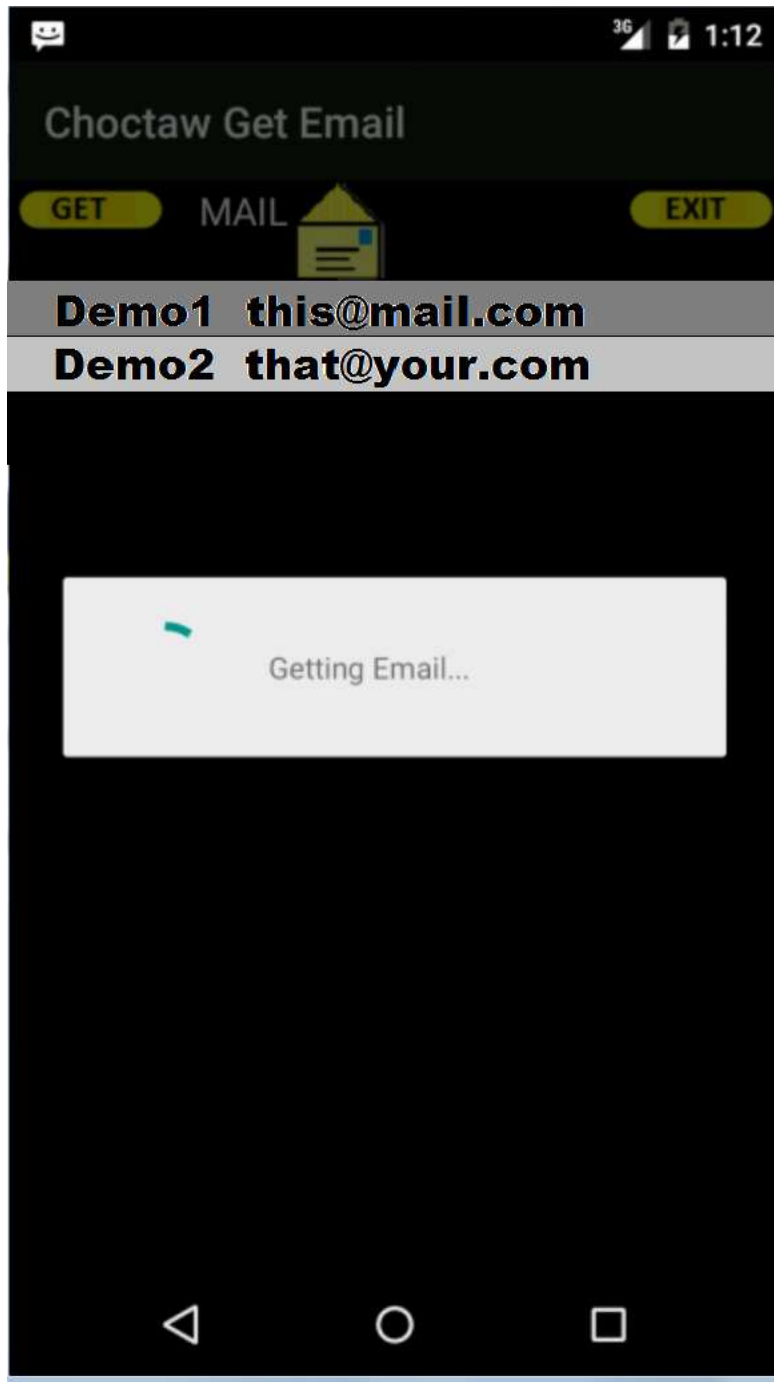
## READ



To get an email simply select the check box next to the email and click **READ**. The **READ** command reads the selected email and places you in the **READ email** menu.

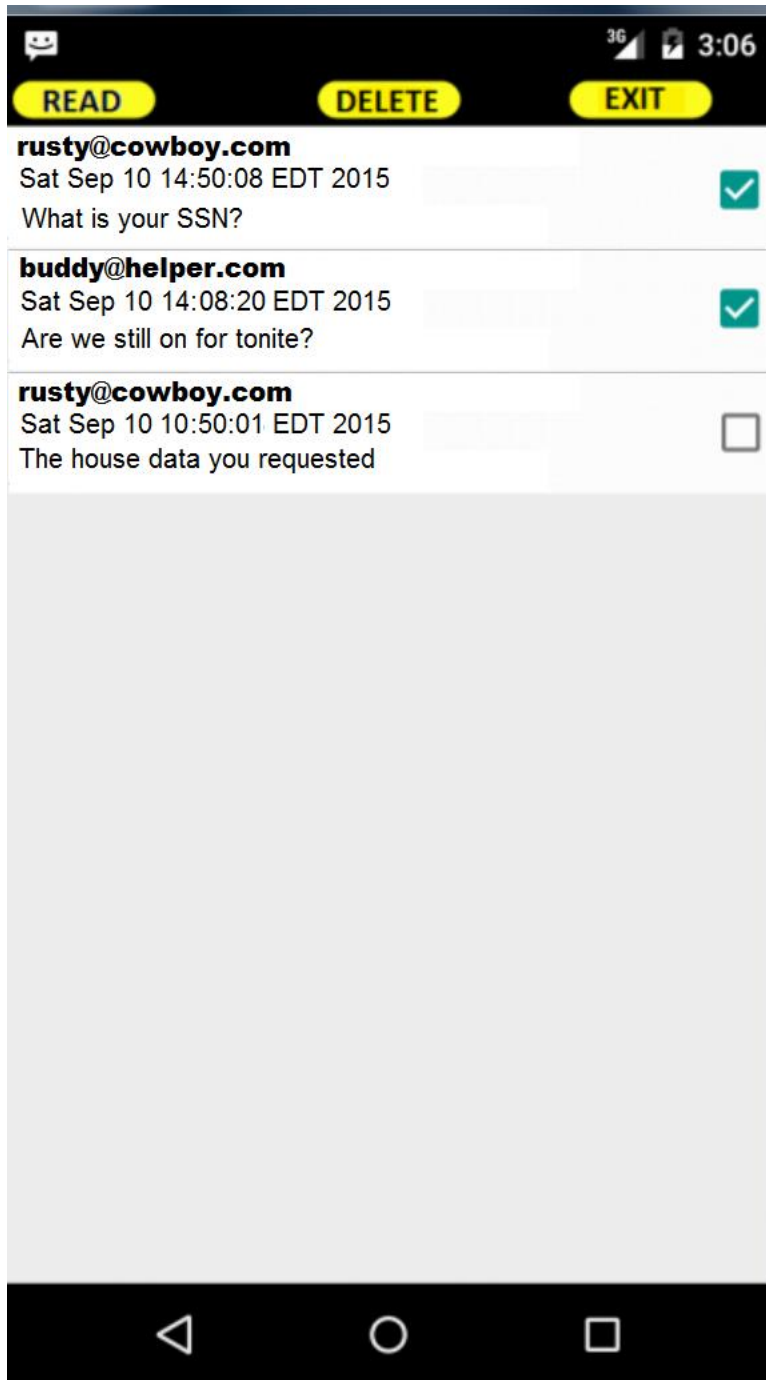


CHOCTAW getting selected email

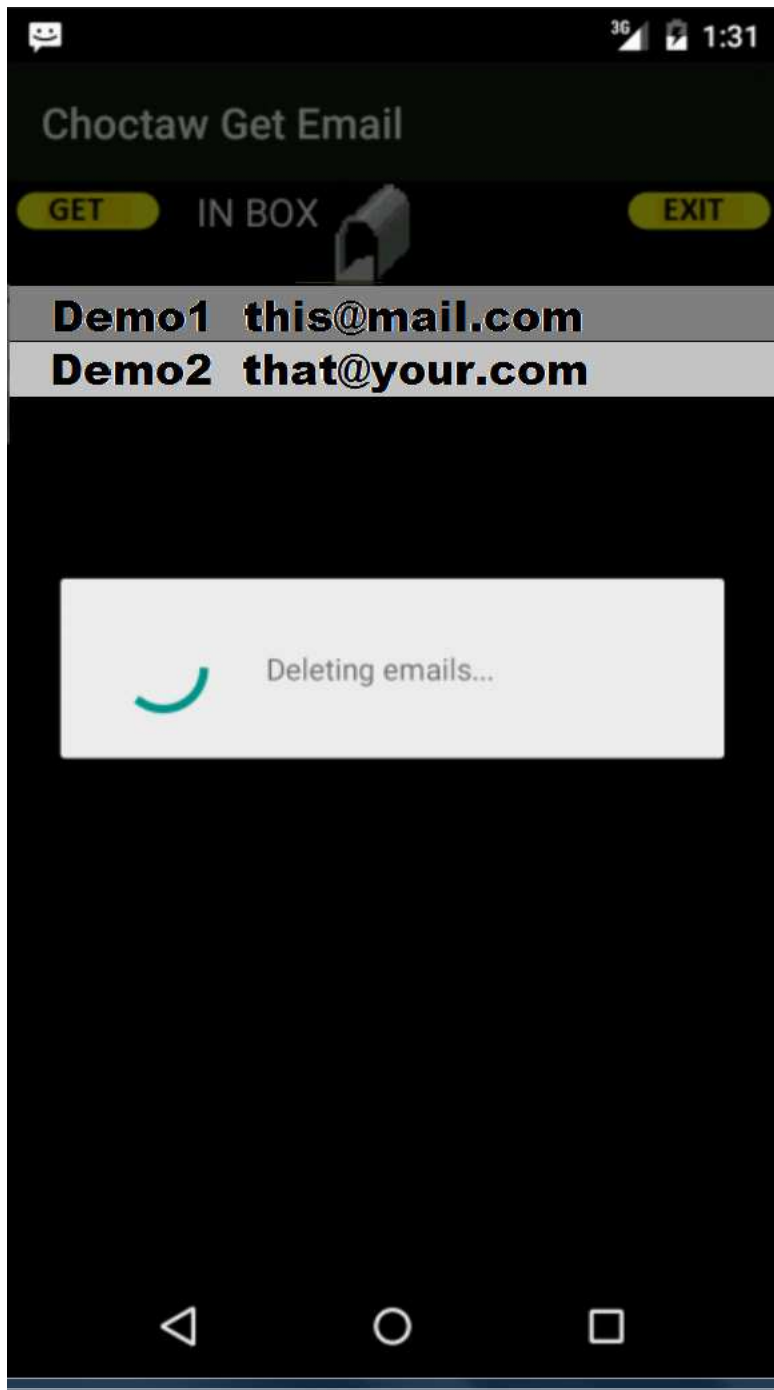


## DELETE

Delete removes the selected emails from your current service. You can select multiple emails by selecting the check box next to each email.

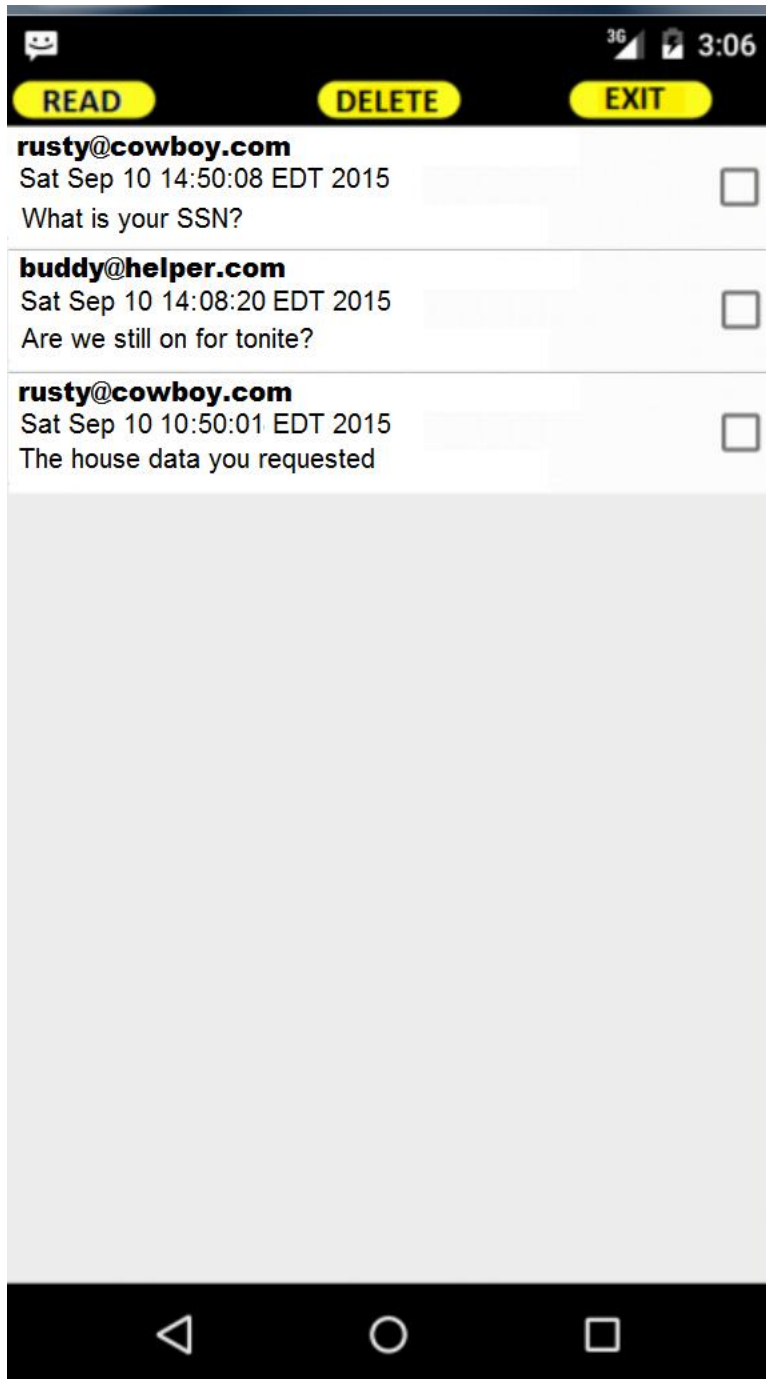


CHOCTAW deleting selected emails

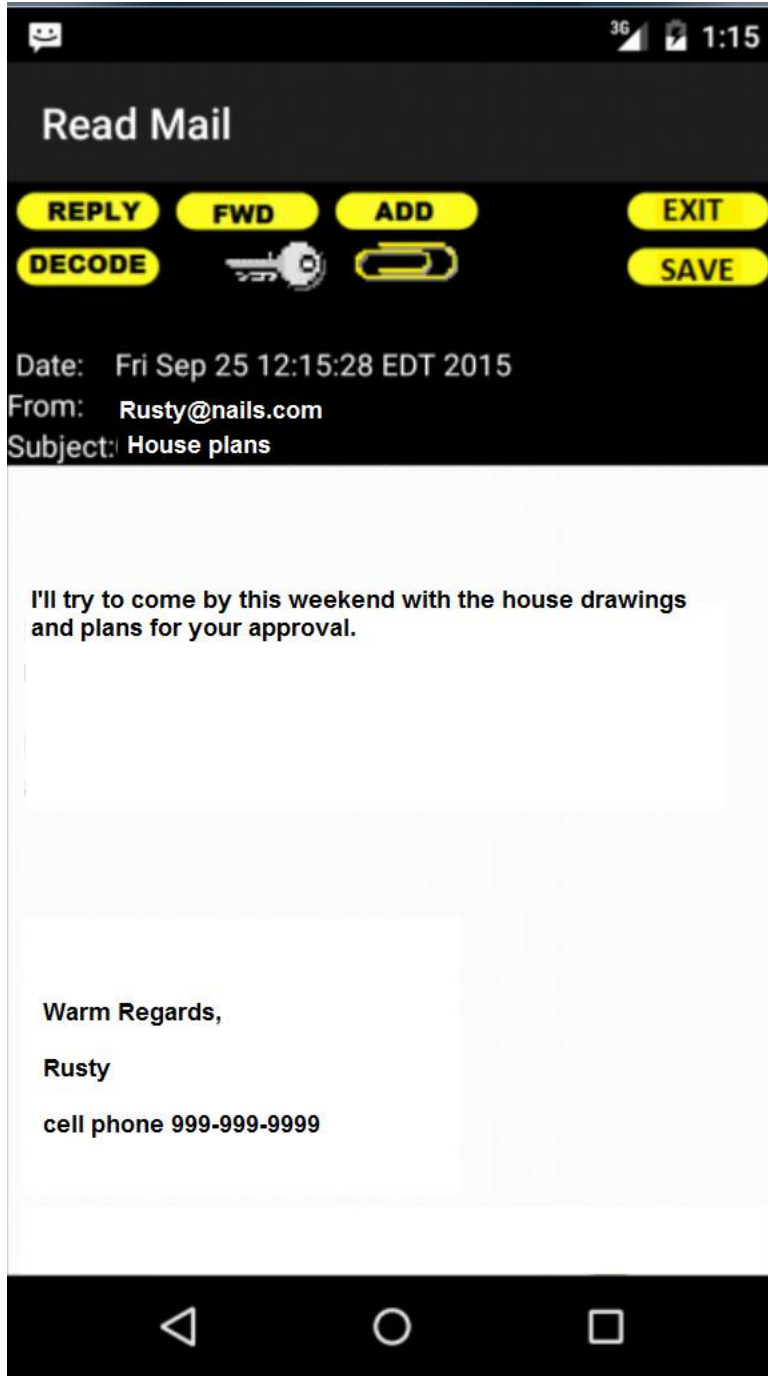


## EXIT

Exits the INBOX menu and returns to the Choctaw GET EMAIL menu.



## READ EMAIL



The READ EMAIL command menu allows you to view and act upon incoming email.

## REPLY

Hit the REPLY button and Choctaw will take the email and sender – place the results in the COMPOSE menu and allow you to send a reply.

## **FWD - FORWARD**

The FORWARD command allows you to forward the email contents to another recipient.

## **DECODE**

The DECODE command decodes incoming emails using the settings provided by the sender entry in the address book and/or the registered public key.

## **ADD – ADD SENDER**

Adds the sender to the Choctaw address book and opens the book at that entry for your update.



## **KEY COMMAND**

The **KEY** command logs or registers any PDA public key attached to the email. This will allow you to reply to the sender using their PDA key.

## **SAVE**

The **SAVE** command will save a cyphered version of your email in the **SAVE BOX** for later viewing.



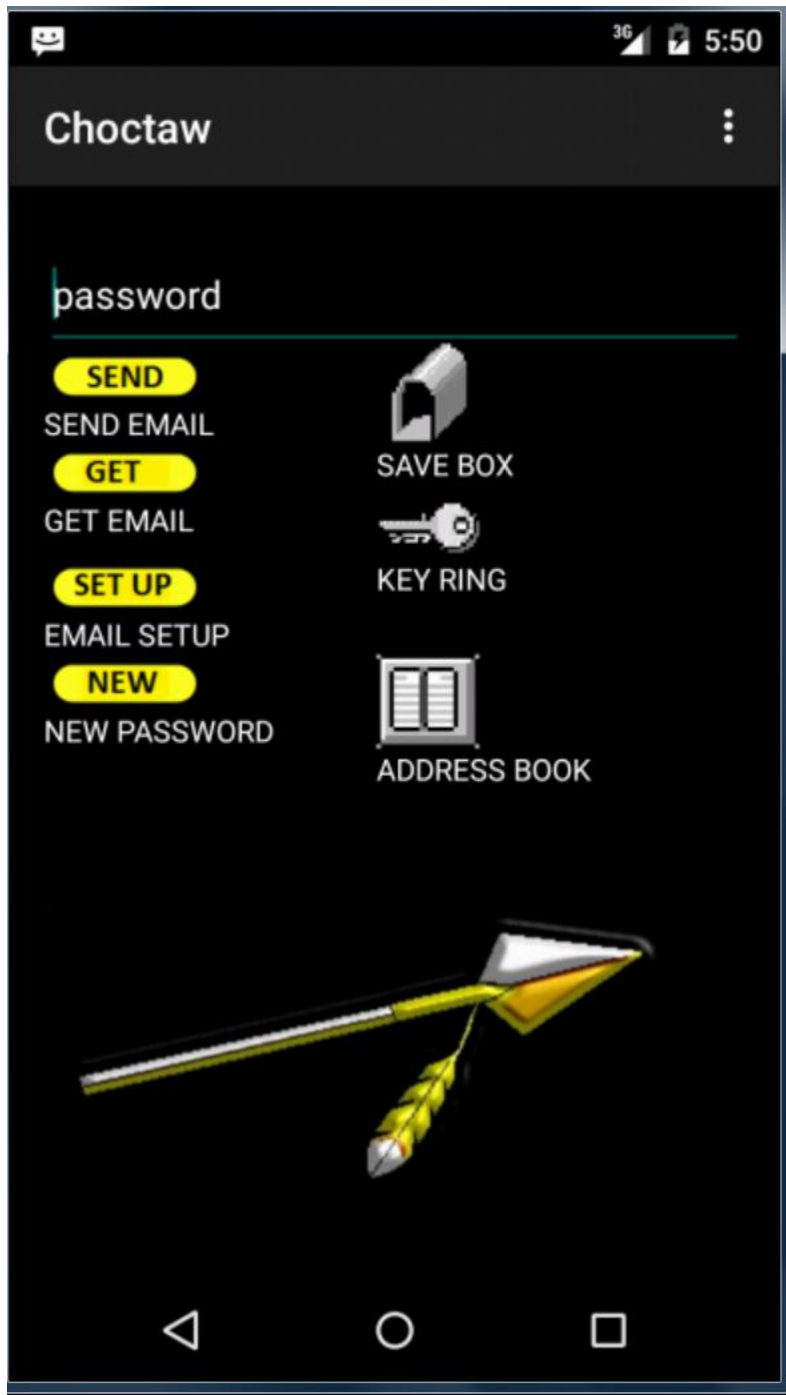
## **ATTACHMENTS**

The Attachment command notes that there are files attached to the email. Click on the paper clip to see the attached files. These files are listed in an attached file menu and can be saved.

## **EXIT**

Exits the **READ EMAIL** menu and returns you to the **INBOX** list of emails.

SEND EMAIL



## SEND MENU



## TO

Click the TO button and Choctaw will take you to your address book. You can select from the address book and bring in an email address. You can also directly enter a TO email address if the contact is not in your address book.



## **From**

Pick a sending email address using the drop down selection list. Simply click on the desired email service by your address. This will bring in your email addresses from each service you have logged into Choctaw.

## **SUBJECT**

Enter your subject for the email here.



## **ATTACH A FILE**

Click the attach clip to add files to your email. The command will allow you to select the files you require to be attached to the email.

## **CODE**

Click the **CODE** command to encrypt your email message when you are done entering the entire message. This will encrypt the message using the **SEND KEY** setting selected for the **TO** recipient in your address book. The **CODE** command will automatically encrypt the message using the public key, private key or password set in the recipients' email setting.

When using a private key file a KEY percent remaining message is displayed in a pop up box showing how much of a PRIVATE KEY is remaining. This is a visual indication provided for the top level of security – the ONE TIME PAD. When you use the ONE TIME PAD system you encrypt messages with the key until it is used up. You should switch to a new key when the KEY percent is low and delete your old key.



## **KEY COMMAND**

Click the KEY command to insert a public key at the end of the email message. This command will allow you to select a public key from your PDA Key Ring to include inside the email message. This is the first step to sending a public key to communicate in a secure fashion with others.

## **SEND**

The SEND command will send your email message to the service selected in the FROM field. Choctaw will display a status of your email as it is being sent.

## **EXIT**

Exit leaves the COMPOSE menu.

## REPLY AND FORWARD HTML



### REPLY

Both the reply and forward features of the Choctaw **READ EMAIL** feature allow you to respond and edit HTML formatted emails. When you hit **REPLY** or **FORWARD** on the **READ EMAIL** menu the email will be formatted into the **SEND** menu. The reply or forward data is displayed at the top of the email and the **REPLY** button will appear on the SEND MAIL menu. To enter any comments or details simply hit the **REPLY** button. A pop up box will allow you to enter your message and place the message above the reply or forward data in the HTML formatted email.

## REPLY POP UP BOX



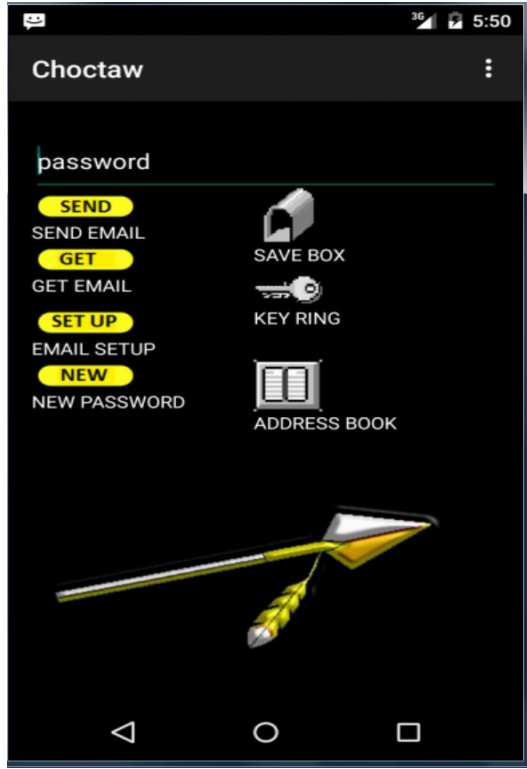
Hit the **REPLY** button.

Enter your reply message in the pop up box and hit the **REPLY MSG** command.




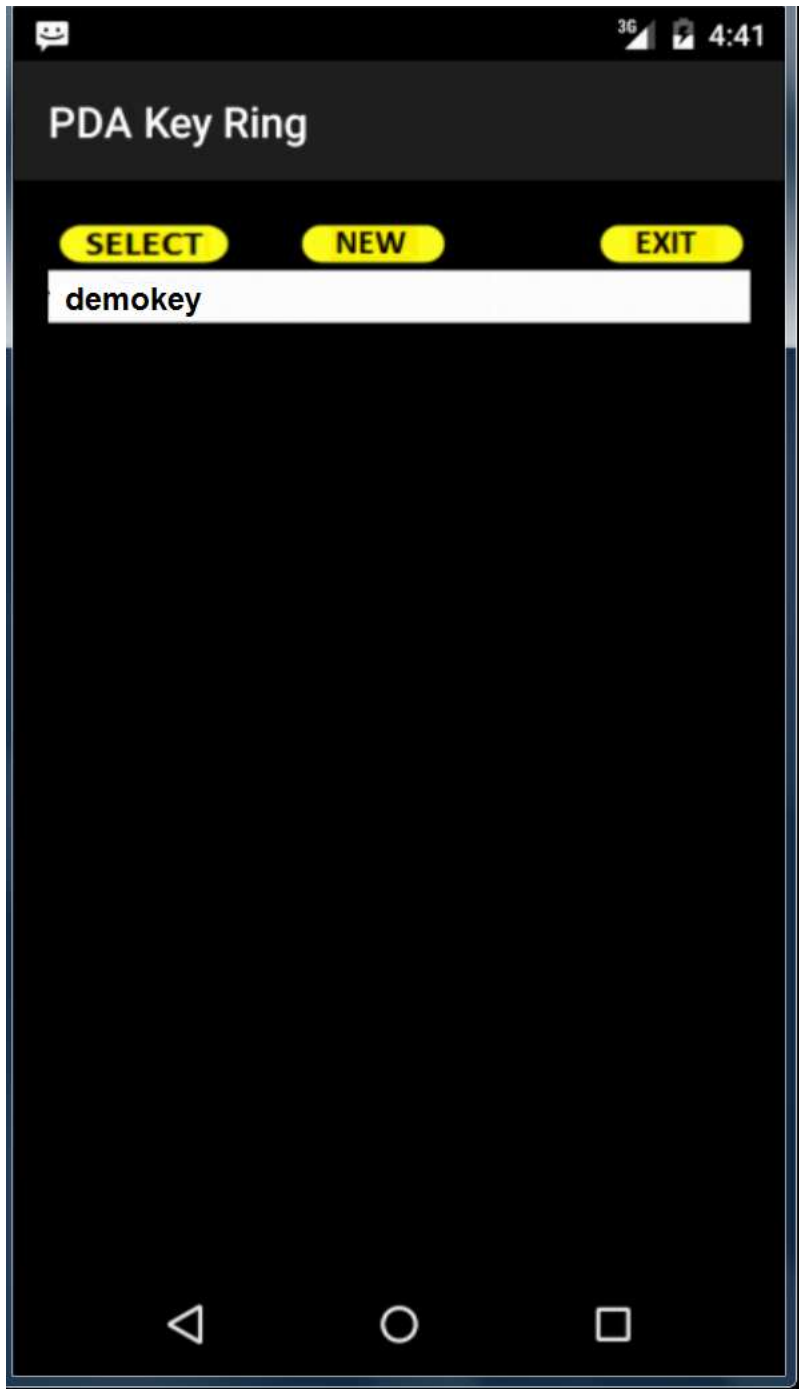
The message will be inserted in the HTML formatted email at the top.

## PDA KEY RING



The PDA KEY ring is the main tracking area for your public key system. In order to use the PDA KEY ring you must first create a key set (private and public) using the PDA Utility. You can create as many PDA keys as you like and you can protect them with different passwords if you require.

HIT the  on the main Choctaw menu to get to the PDA KEY ring.



### NEW

Hit the NEW command to add a new PDA key

## **SELECT**

Hit the **SELECT** command to edit or delete PDA key information.

## **EXIT**

Hit the EXIT command to leave the PDA KEY ring menu.

## PDA KEY RING EDIT MENU



### NAME

Enter the name you will be able to identify the key set with from the main menu.



## **PDA PASSWORD**

Enter the PDA password used to protect the keys in the PDA utility.

## **PRIVATE KEY**

Hit the PRIVATE KEY command to select the private (.PRI) file that contains the PDA private key.

## **PUBLIC KEY**

Hit the PUBLIC KEY command to select the public (.PKY) file that contains the PDA private key.

## **SAVE**

Save the key set in your PDA ring.

## **NEW**

Choctaw can automatically generate a PDA key. Hit the NEW command and the key will be created. Simply save the key for later selection in the compose email menu.

## **DELETE**

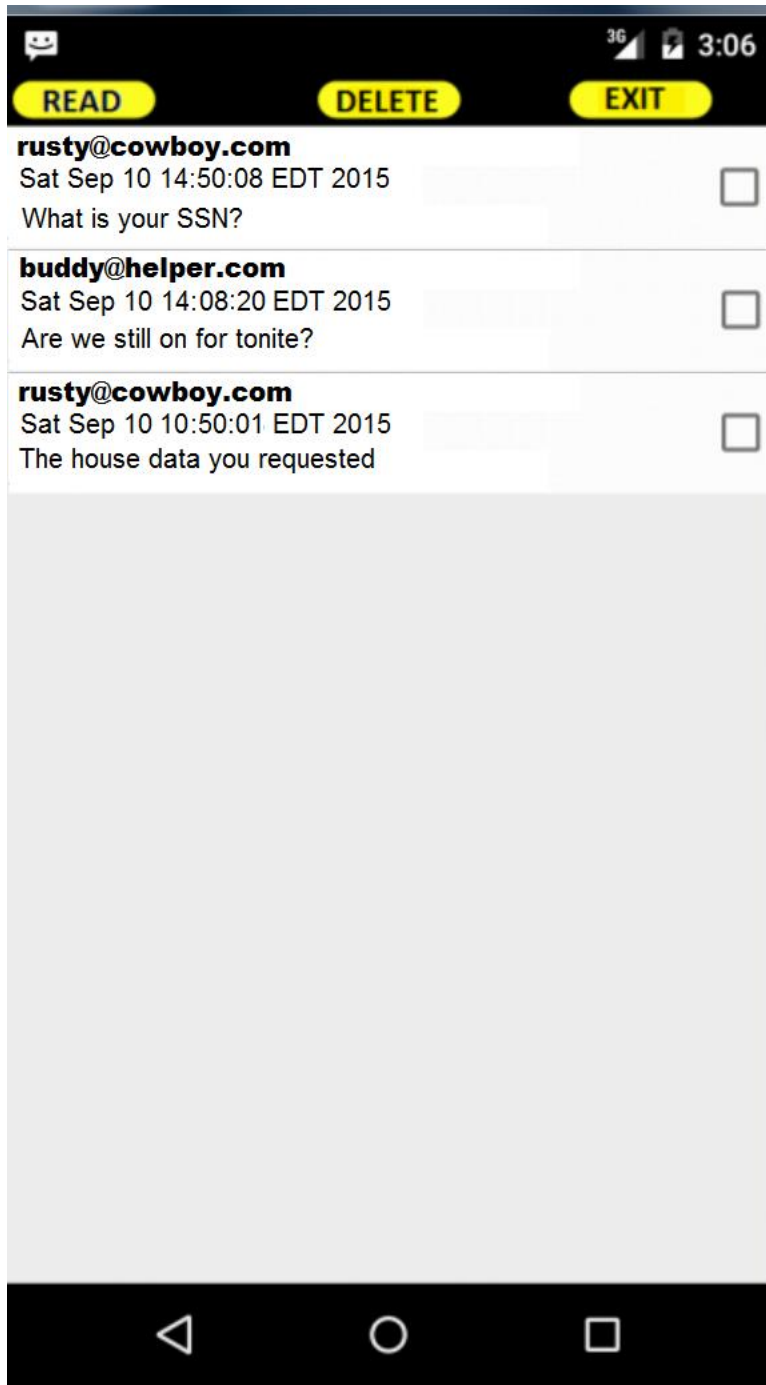
Delete the PDA KEY set.

## **EXIT**

Exit the PDA KEY RING EDIT menu.



## SAVE BOX



The SAVE BOX feature displays all the emails that you selected to SAVE from the view email in menu. All emails in the save box are stored cyphered with your main Choctaw login key/password.

## **READ**

The **READ** command will load and decode the selected email into the VIEW menu.

## **DELETE**

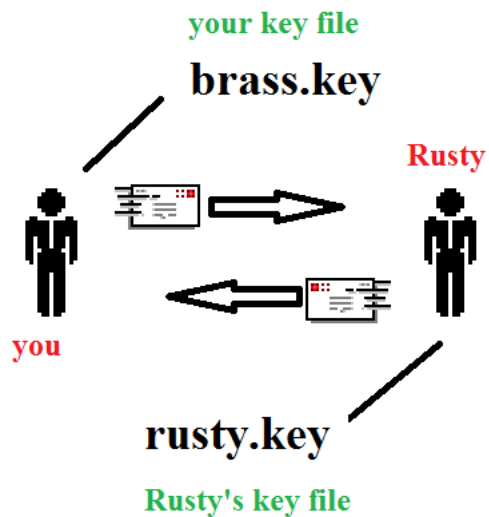
Delete removes the selected email from the SAVE BOX.

## **EXIT**

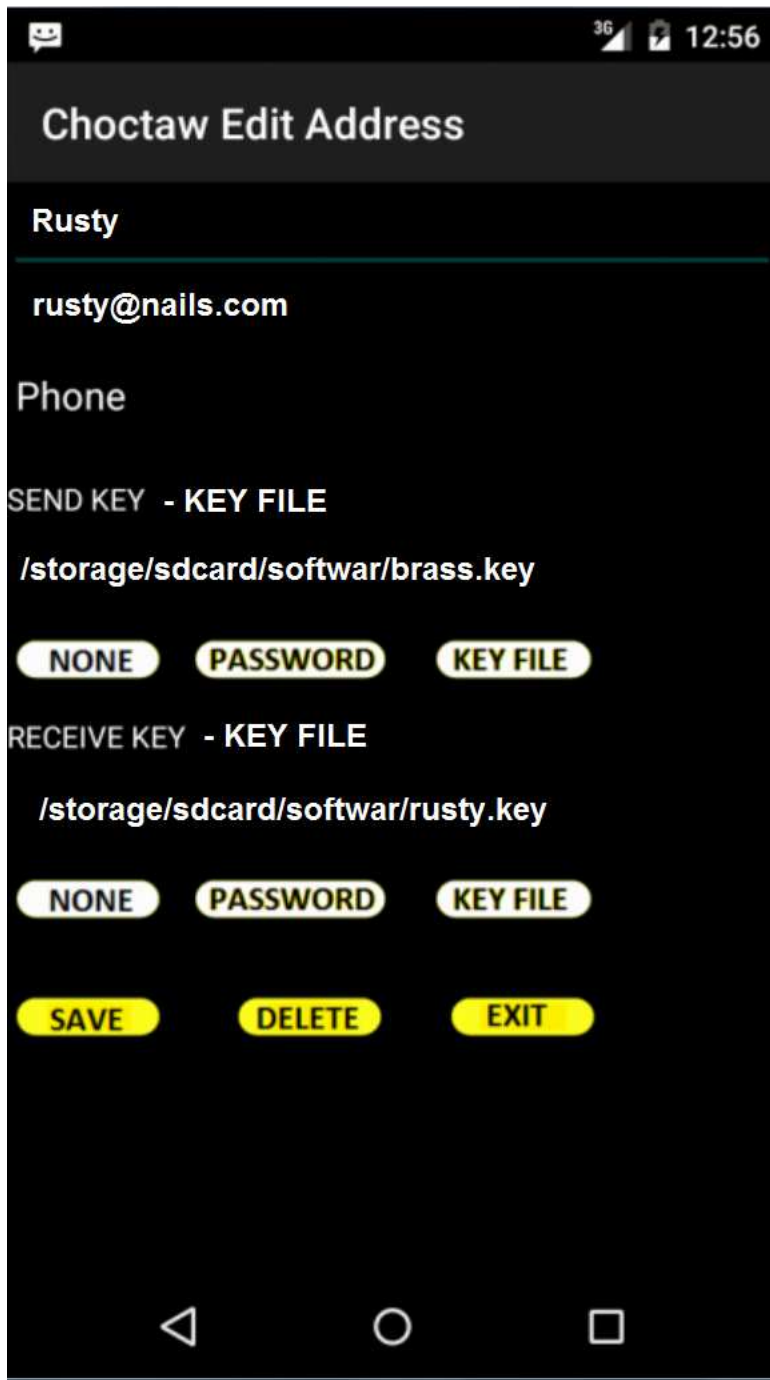
Exits the SAVE BOX menu and returns to the main Choctaw menu.

## PRIVATE KEY CYPHERING

In order to use password or private keys you must enter the data into the address book for each individual. The basic idea for private keys is to exchange the keys in person or by trusted courier - which then allows you to send and receive emails in a secure manner. In this example below you exchange keys with Rusty. You wish to send email to Rusty using the “brass.key” and you will receive email from Rusty using the “rusty.key”.



Your entry to send and receive emails from Rusty would look like this:



## PRIVATE KEY EXCHANGE

Step 1 – Create a key using Cypher

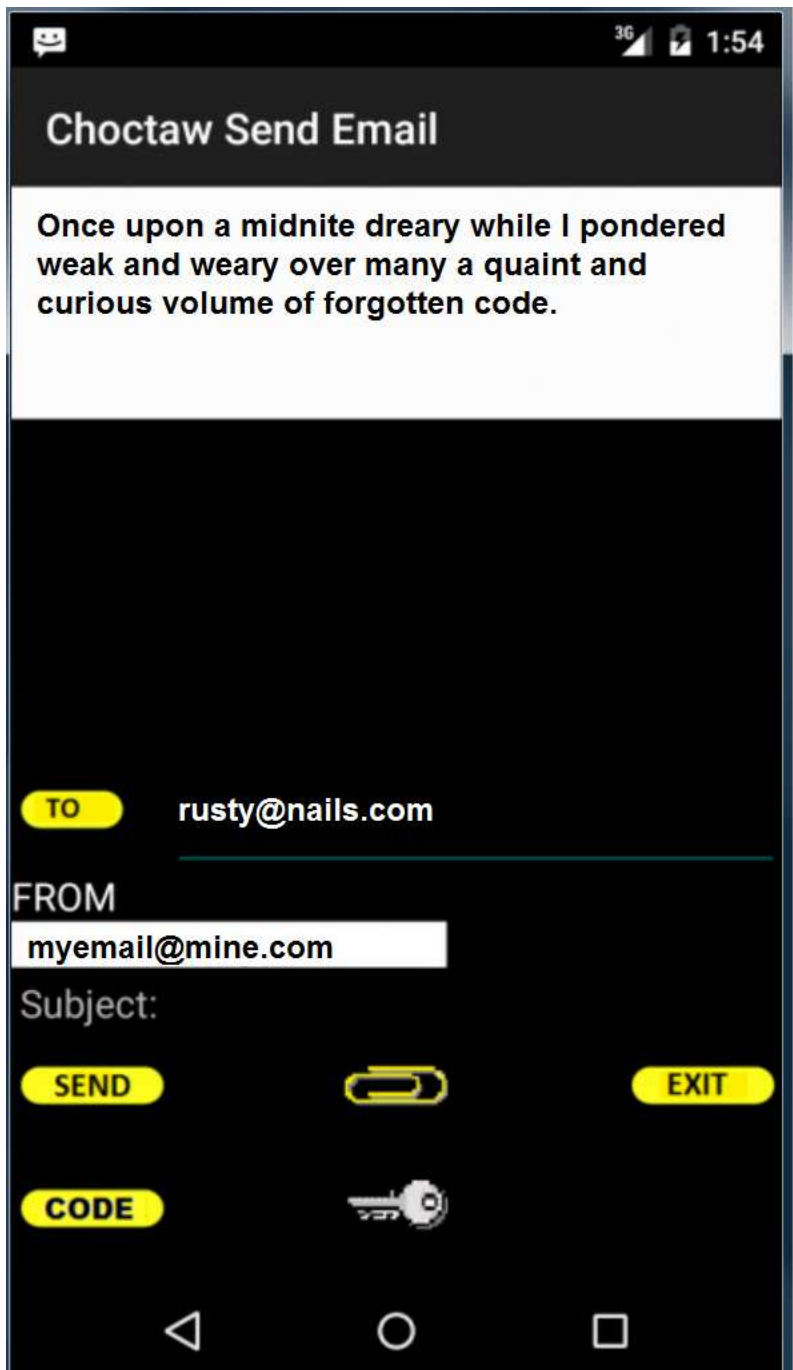
Step 2 – Exchange keys with the intended recipient

Step 3 – Log your key in the SEND field of the recipient address book entry

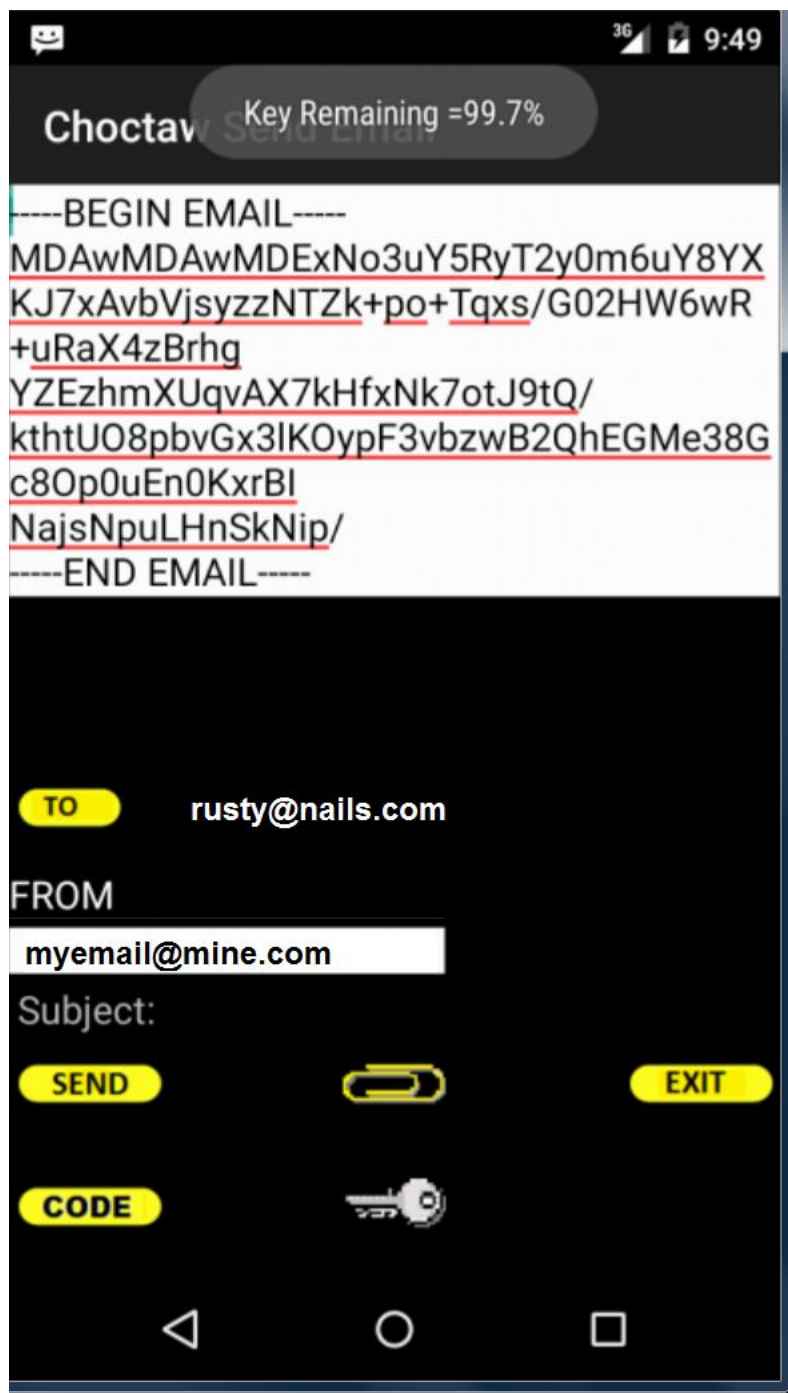
Step 4 – Log their key in the RECEIVE field of the recipient address book entry

To send email –

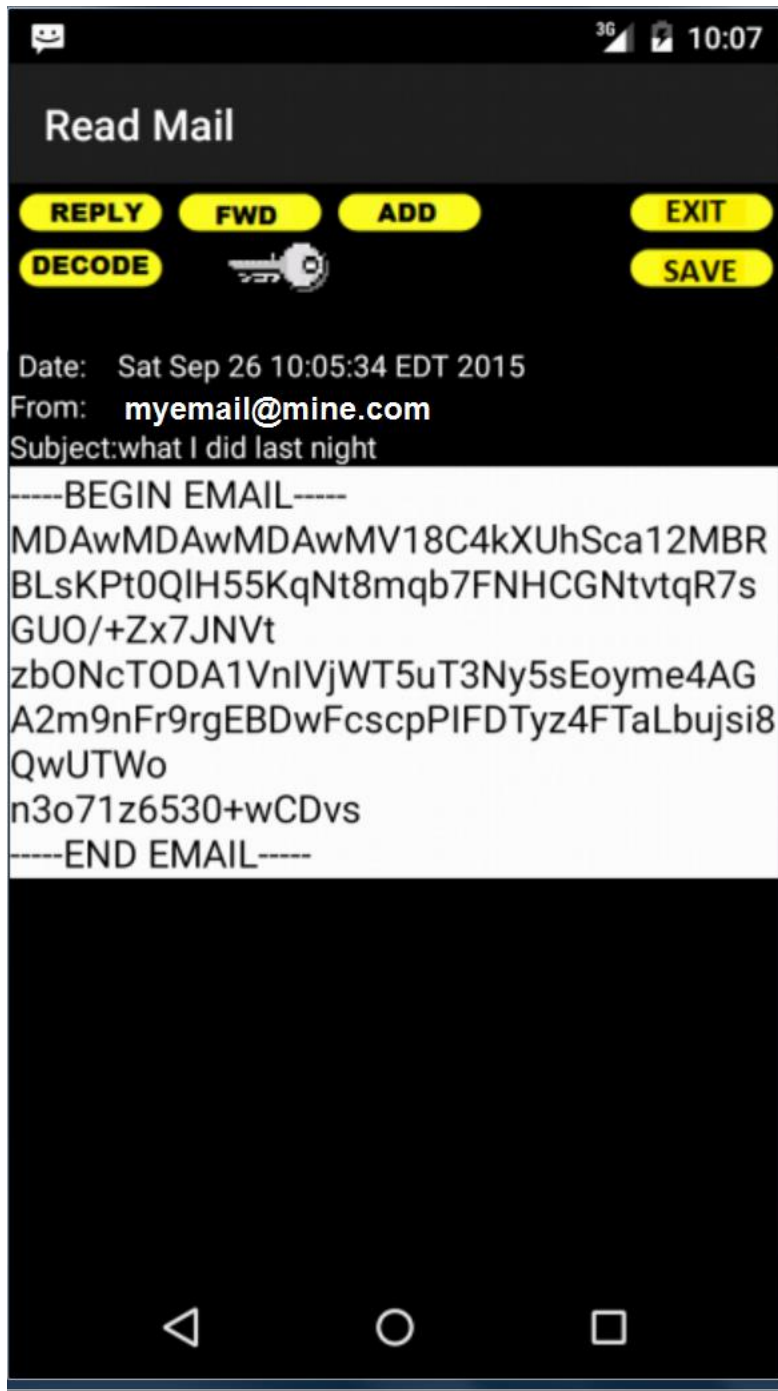
Step 1 - Enter your message in the Send Email menu.



STEP 2 - Hit the CYPHER command and send email.

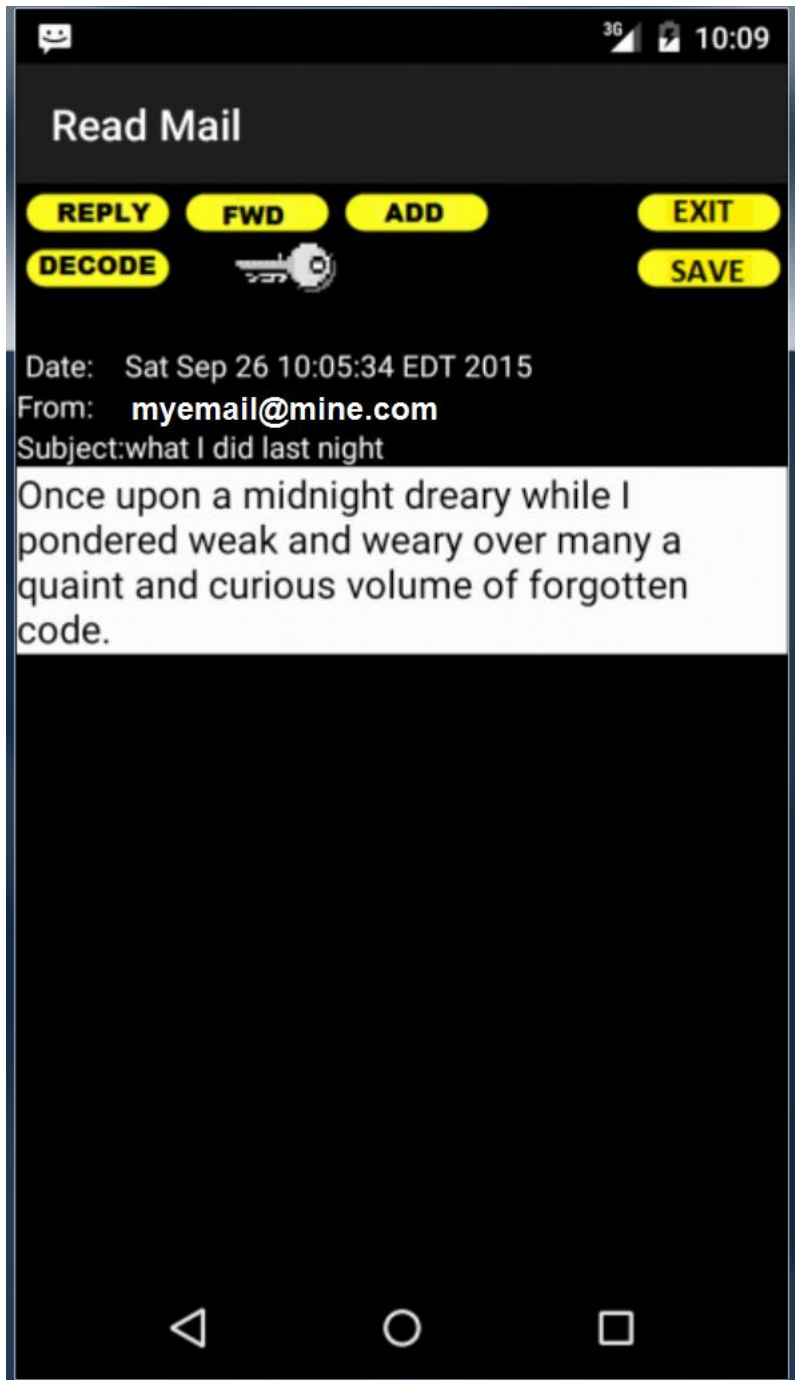


To receive encrypted email –

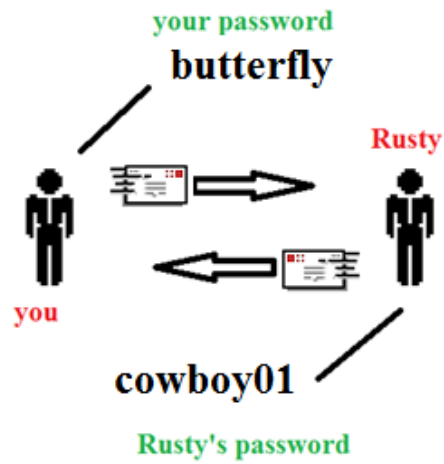




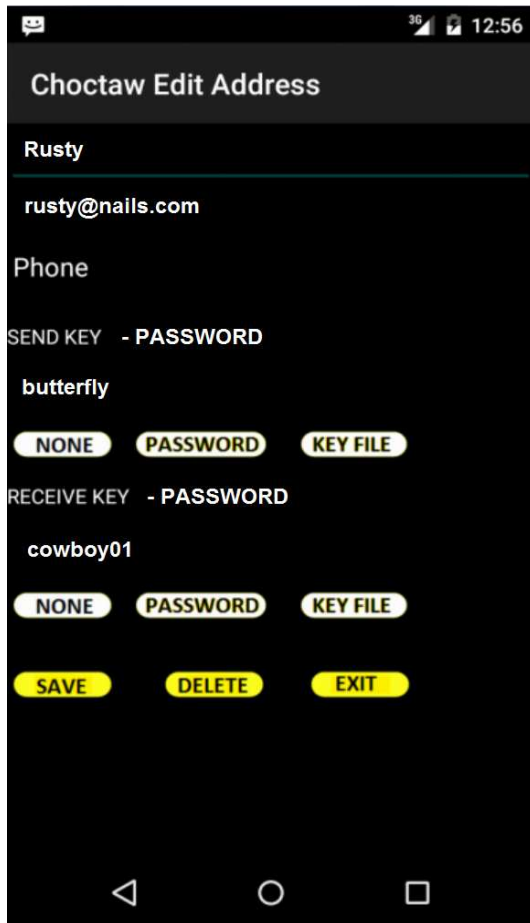
Hit the DECODE command in the READ email menu.



In this example below you exchange passwords with Rusty. You wish to send email to Rusty using the “butterfly” and you will receive email from Rusty using “cowboy01”.



Your entry to send and receive emails from Rusty would look like this:



## PUBLIC KEY CYPHERING

Public key cyphering, also known as asymmetric cryptography, is a two key system. Think of the system as a one way lock. The public key can only lock data and the private key can only unlock data. No entry in the address book is necessary to use the public key system built into Choctaw. Choctaw will automatically update the address book with public keys.

Use the PDA utility to create a matching pair of keys: a private key and a public key. Email cyphered with the public key can only be de-cyphered with the matching private key. Your PDA private key is password locked so unauthorized individuals cannot access or decode information.

All you have to do is add the PDA keys to your key ring on the main menu and then send the public key in your email messages. The public key may be published without compromising security, whereas the private key must not be revealed to any unauthorized individual. When you send your public key in your email messages to other users they can cypher email and send it back to you.

**PDA makes 2 keys - you keep  
private key and send public  
key to others**



**mykey.pri** **keep**  
unlocks emails encrypted  
with public key



**you**



**others**

use key to  
send you  
email

**mykey.pky** **send**  
locks emails using  
public key  
put key on email to others



## PUBLIC KEY EXCHANGE

### SEND A PUBLIC KEY –

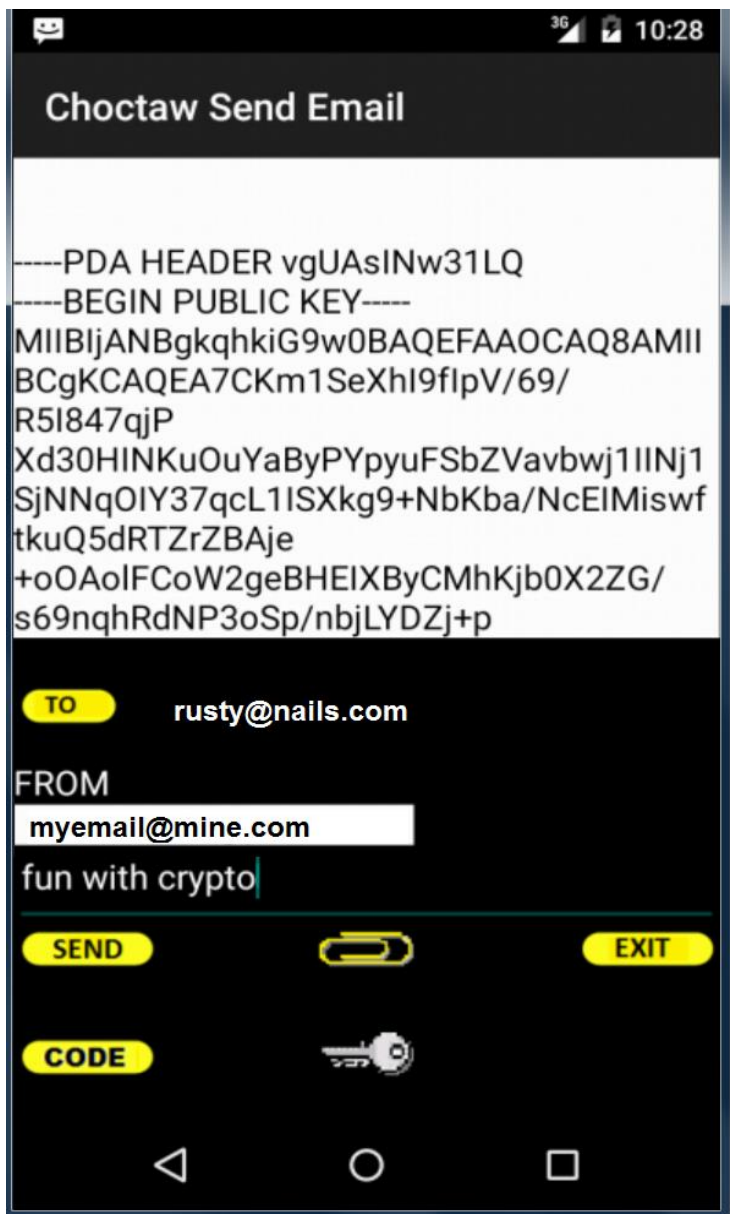
STEP 1 – make key using PDA or

You can create the PDA key using the  and select NEW in the Ring selection

STEP 2 – add key to Choctaw  KEY RING on main menu

STEP 3 – put the KEY in an email  KEY command in SEND email

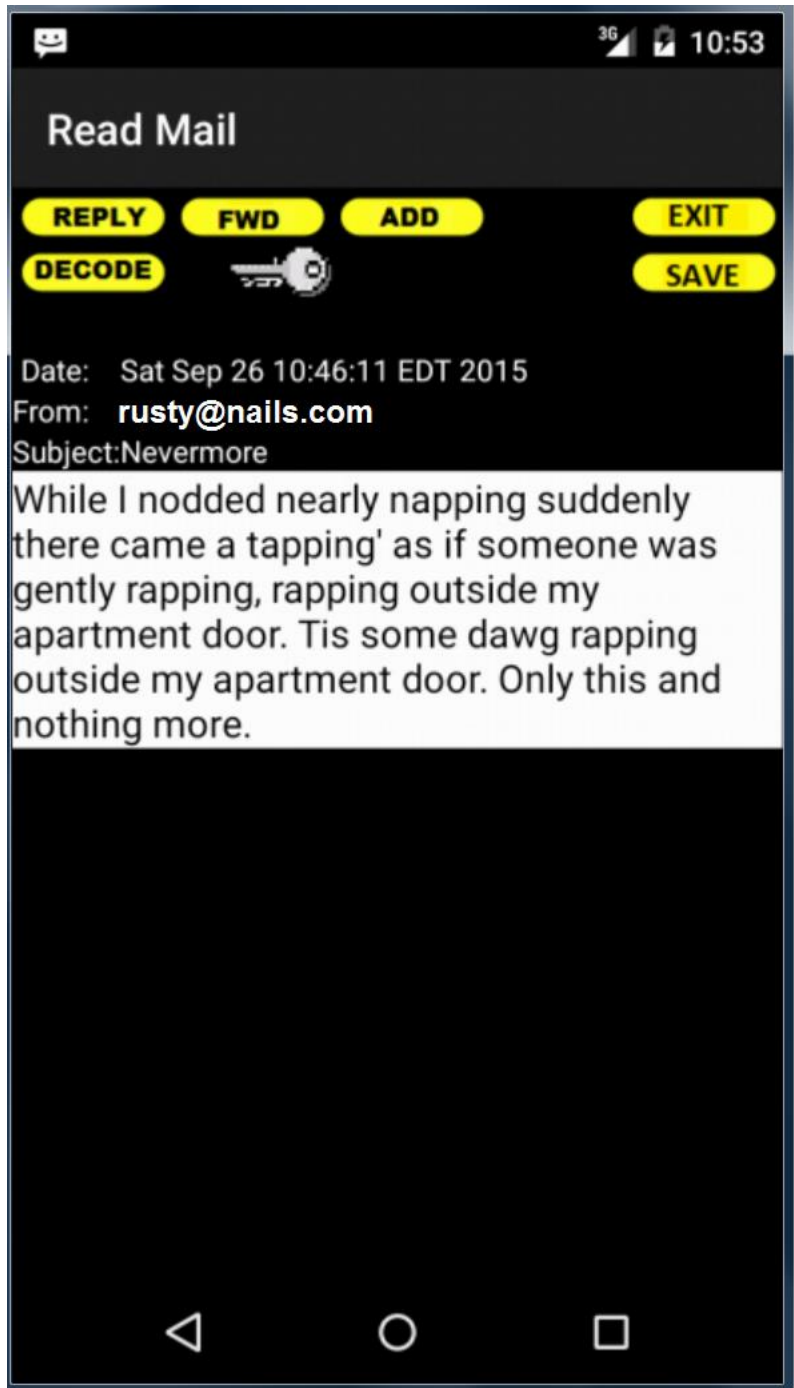
STEP 4 – send email with KEY to recipient



STEP 5- Other person will send you an email cyphered with your public key.



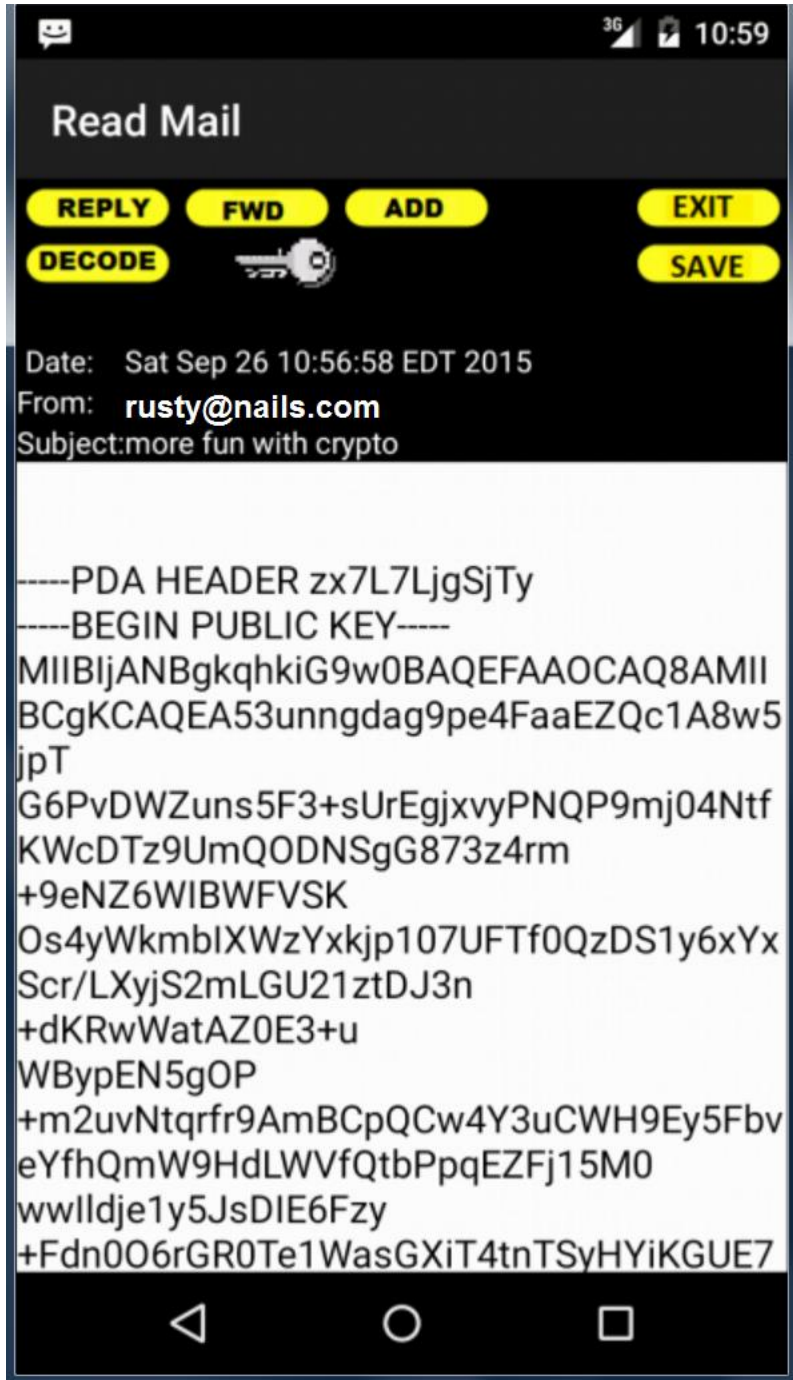
STEP 6 - Hit the DECODE command and email will be decoded.



Get a PUBLIC KEY –

STEP 1 – have other person send you a PDA key in email.

STEP 2 – log KEY using  command in READ mail menu.



**STEP 3 –**

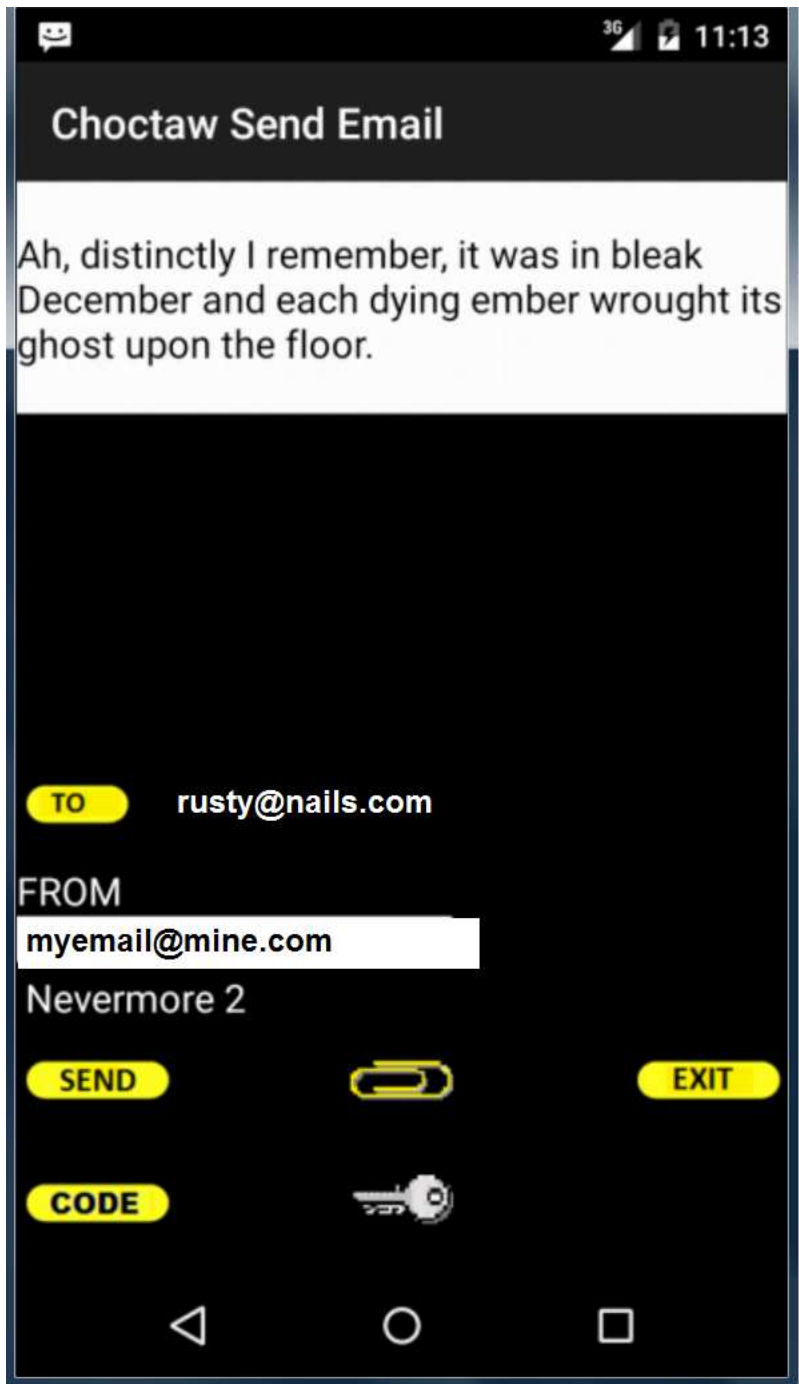
Choctaw will create or edit the sender ADDRESS book entry with the new key.

Save the entry by clicking on the **SAVE** command. The Address Record saved message will confirm the log in process.

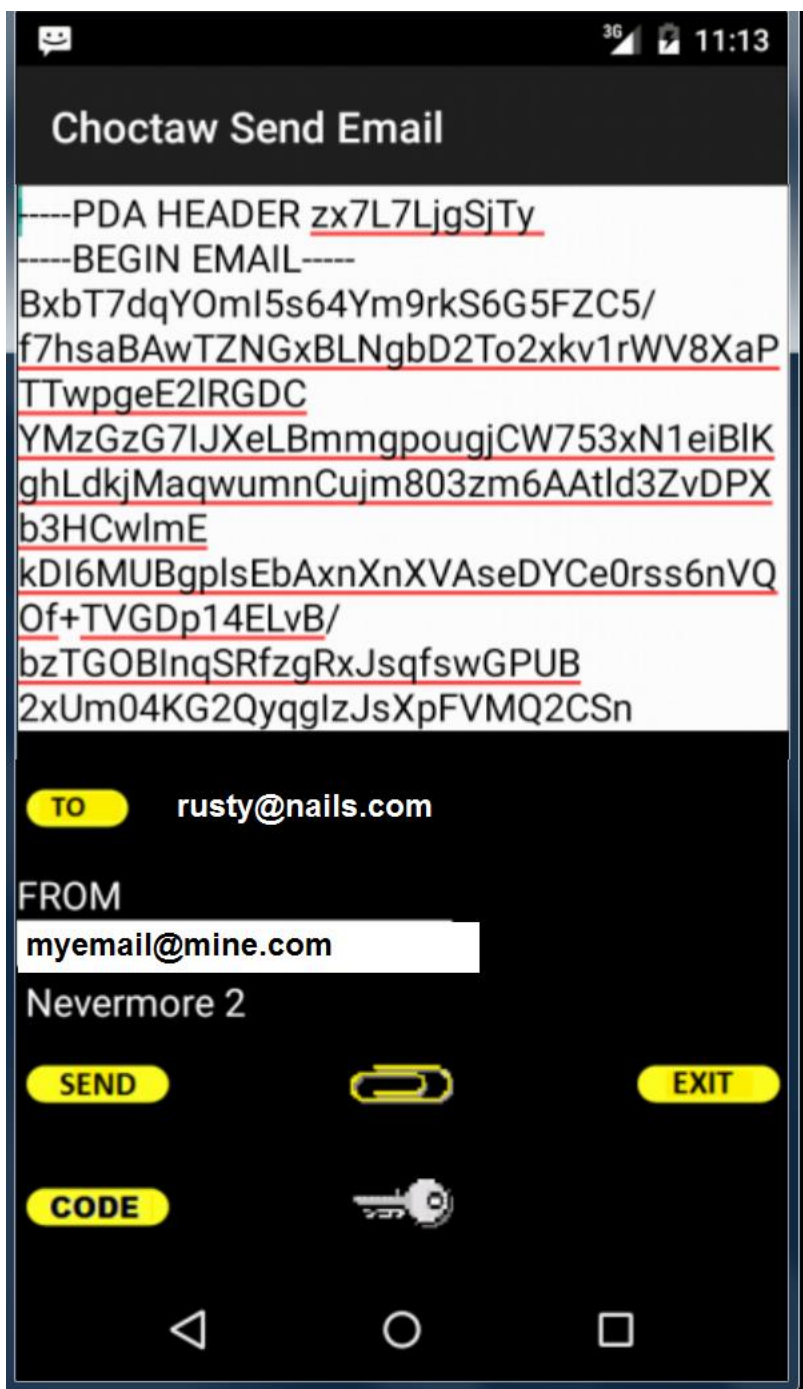




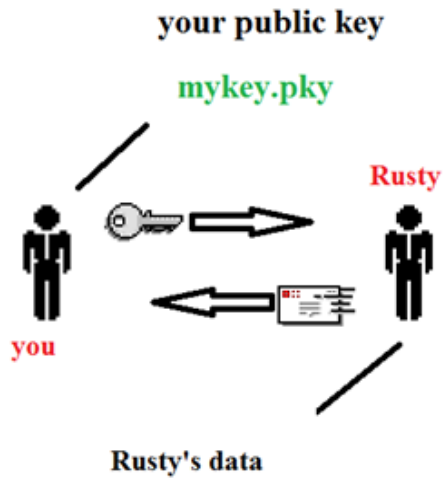
STEP 4 – Write an email to the key sender using the SEND Email menu.



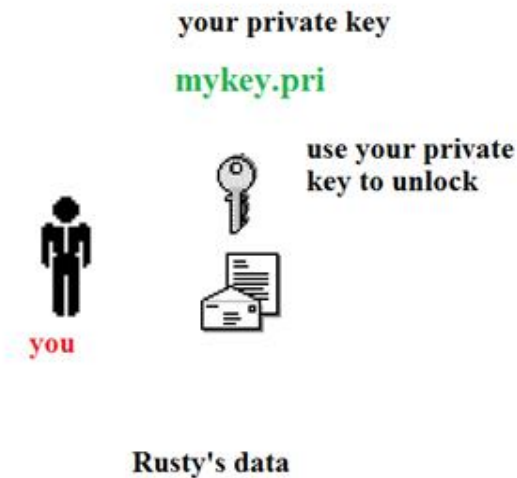
STEP 5 – hit the **CODE** command in the SEND Email menu.



In the example below – you send a public key in your email to Rusty who then codes his email message and sends it back to you.



View the message and click on the **DECODE** command. Choctaw will automatically select the correct private key to unlock the email and allow you to access Rusty's message.



## **CYPHER DETAILS**

There are several levels of security provided by Choctaw when combined with the Cypher and PDA utilities. Select a cypher level during entry in the Choctaw address book for each member you wish to communicate with.

### **Password – First level security:**

Cypher and de-cypher using a personal password of no less than 8 characters.

### **User Key File – Second level security:**

Any file to be used as a key to cypher and de-cypher. The user selected key file can be any document, picture, music, text or work file. It is recommended that you do not use files that contain large amounts of repeating characters such as bitmap files. However, files that are compressed such as zip, jpeg, MP3 or other media files that have been compressed are acceptable. DO NOT pick a file that will change. Just as with a physical lock on a door, a key file must be the same used to cypher (lock) a file in order to successfully de-cypher (unlock) the same data.

### **PDA Public keys –Third level security:**

The PDA asymmetrical public key system uses a 4096 bit RSA key and a built in unique session key for each email message. Choctaw allows you to add the public keys directly to your outgoing emails and automatically decodes any emails using a key ring. The public key system is different from the private key systems in that it does not require direct key exchange to be secure.

### **Crypto Key File - Fourth level security:**

This is a key file created by the **Cypher** utility key maker that utilizes the computer Pseudo-Random Number Generator (PRNG) to create a very large set of random numbers. The Crypto Key maker utilizes several system features such as time, key strokes, position of the hard drive and many other variables to randomly seed and create large keys using a mathematical algorithm. The crypto key file is considered to be superior to the User key in that it is much more random than regular user data files.

### **IMAGE Key File – Highest level security:**

The image key is created by using your android camera equipped phone to sample light in three basic colors – red, green and blue. This system is known as a True Random Number Generator (TRNG) because the key is generated by the light recorded by your camera. The image key is the most secure because it is created using quantum physics by recording the values of photons electronically. The image key is similar in performance to keys generated by sensors inside Atomic clocks that detect radioactivity.

## **KEY EXCHANGE – STORAGE & USAGE**

Private Key systems rely on a direct key exchange. You issue keys directly to others either face to face or by a trusted courier. For private key cyphering you can use a simple password or any file of your choice to protect your information. The advantage of this is that no one else can intercept the keys. Private Key files can be cyphered with a pre-arranged password and sent as an attachment.

While Choctaw can use any file to secure data and emails, it is recommended that you use CYPHER light generated keys for the highest level of security. If used correctly, the light keys provide ONE TIME PAD email security which cannot be compromised.

However, it is not always possible to directly exchange keys. The PDA utility is designed to cypher and de-cypher any data file using PUBLIC Keys. You can send private keys in a secure fashion by using PDA.

Simply send a public key file made with PDA as an email attachment to the other user of Choctaw. The recipient can then send you their CYPHER key files or other data using 4096 bit RSA security. PDA creates an output file containing the selected data file cyphered with the public key. This allows you to exchange keys and data with others in a secure manner.

You can also use the PDA Key Ring provided in Choctaw to register your public keys. When you send a message you can add the public key directly to the message text and others can use your public key to send you cyphered messages. Choctaw will automatically find the correct keys and decode incoming email messages.

For public key cyphering, simply create a PDA key set, add it to the Choctaw key ring and add the public key to any email to be sent. Users who want to reply using the public key can cypher their emails with your public key and send them back to you. You can decode their messages with the touch of one button.

## **TECHNICAL SPECIFICATIONS**

Choctaw is a POP3 and SMTP email application with TLS and SSL automatic security.

Choctaw has two cyphering systems:

A symmetrical stream cipher private key system that can be used in a ONE TIME PAD mode. This means that you must exchange keys with the individuals you wish to communicate to and use the key only ONE TIME. The ONE TIME system has been used by US presidents to communicate with Moscow and by the US military to lock down nuclear weapons.

An asymmetrical public key system using a 4096 bit RSA key and a built in unique session key for each email message. Choctaw allows you to add the public keys directly to your outgoing emails and decodes any incoming emails using your personal key ring.

### **CONTACT INFORMATION:**

<http://www.softwar.net>

Email: [softwar@softwar.net](mailto:softwar@softwar.net)

Copyright notice:

Softwar Choctaw © 2015 Softwar Inc. all rights reserved.

Trademarks:

Windows is a registered trademark of Microsoft Inc.

## SOFTWARE End-User License Agreement

BY INSTALLING OR USING THE LICENSED SOFTWARE AND HARDWARE FROM SOFTWARE INC. THE INDIVIDUAL IF ACTING ON BEHALF OF HIMSELF OR HERSELF ("INDIVIDUAL CUSTOMER") OR THE INDIVIDUAL WHO IS ACTING ON BEHALF OF AN EDUCATIONAL OR NONPROFIT INSTITUTION, GOVERNMENTAL AGENCY, OR OTHER ("ENTITY CUSTOMER", THE INDIVIDUAL CUSTOMER AND ENTITY CUSTOMER TOGETHER ARE "CUSTOMER") IS AGREEING TO BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT").

IF CUSTOMER DOES NOT AGREE TO THIS AGREEMENT, CUSTOMER MAY NOT INSTALL, COPY, OR USE THE LICENSED SOFTWARE.

THE "EFFECTIVE DATE" FOR THIS AGREEMENT IS THE DAY CUSTOMER INSTALLS THE SOFTWARE.

The export and re-export of Software Inc. products are controlled by the United States Export Administration Regulations and such software may not be exported or re-exported. This product is classified as information security cyphering technology under Category 5, Part 2 in the U.S. Commerce Control List and IS NOT eligible for export outside the United States.

In addition, Software Inc. software may not be distributed to persons on the Table of Denial Orders, the Entity List, or the List of Specially Designated Nationals. By using an Software Inc. software product you are certifying that you are not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, or any country to which the United States embargoes goods and that you are not a person on the Table of Denial Orders, the Entity List, or the List of Specially Designated Nationals.

Customer shall not, nor permit any person (including any Authorized User) to: (i) reverse engineer, reverse compile, decypher, disassemble, or otherwise attempt to derive the source code of the Licensed Software (except to the extent that this restriction is expressly prohibited by law); (ii) modify, translate, or create derivative works of the Licensed Software; (iii) sublicense, resell, rent, lease, distribute, market, commercialize, or otherwise transfer rights or usage to the Licensed Software (except as expressly permitted under this Agreement); (iv) remove, modify, or obscure any copyright notices or other proprietary notices or legends appearing on or in the Licensed Software, or any portion thereof; (v) transfer, use, or export the Licensed Software in violation of any applicable laws, rules, or regulations of any government or governmental agency; (vi) use the Licensed Software or any system services accessed through the Licensed Software to disrupt, disable, or otherwise harm the operations, software, hardware, equipment, and/or systems of a business, institution, or other entity, including, without limitation, exposing the business, institution, or other entity to any computer virus, trojan horse, or other harmful, disruptive, or unauthorized component; or (vii) embed the Licensed Software in any third-party applications, unless otherwise authorized in writing in advance by an officer of SOFTWARE INC.

IN NO EVENT SHALL SOFTWARE INC. HAVE ANY LIABILITY FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE FORM OF THE ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT

PRODUCT LIABILITY, OR OTHERWISE, EVEN IF ANY REPRESENTATIVE OF SOFTWARE INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR ANY LIMITED REMEDY HEREUNDER.

DISCLAIMER OF WARRANTIES: YOU AGREE THAT SOFTWARE INC. HAS MADE NO EXPRESS WARRANTIES TO YOU REGARDING THE SOFTWARE AND THAT THE SOFTWARE IS BEING PROVIDED TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND. SOFTWARE INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO THE SOFTWARE, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, MERCHANTABLE QUALITY, OR NONINFRINGEMENT OF THIRD-PARTY RIGHTS.