Getting the most from Apple Mail

Larry Kerschberg, Roy Wagner, Jonathan Bernstein and Friends

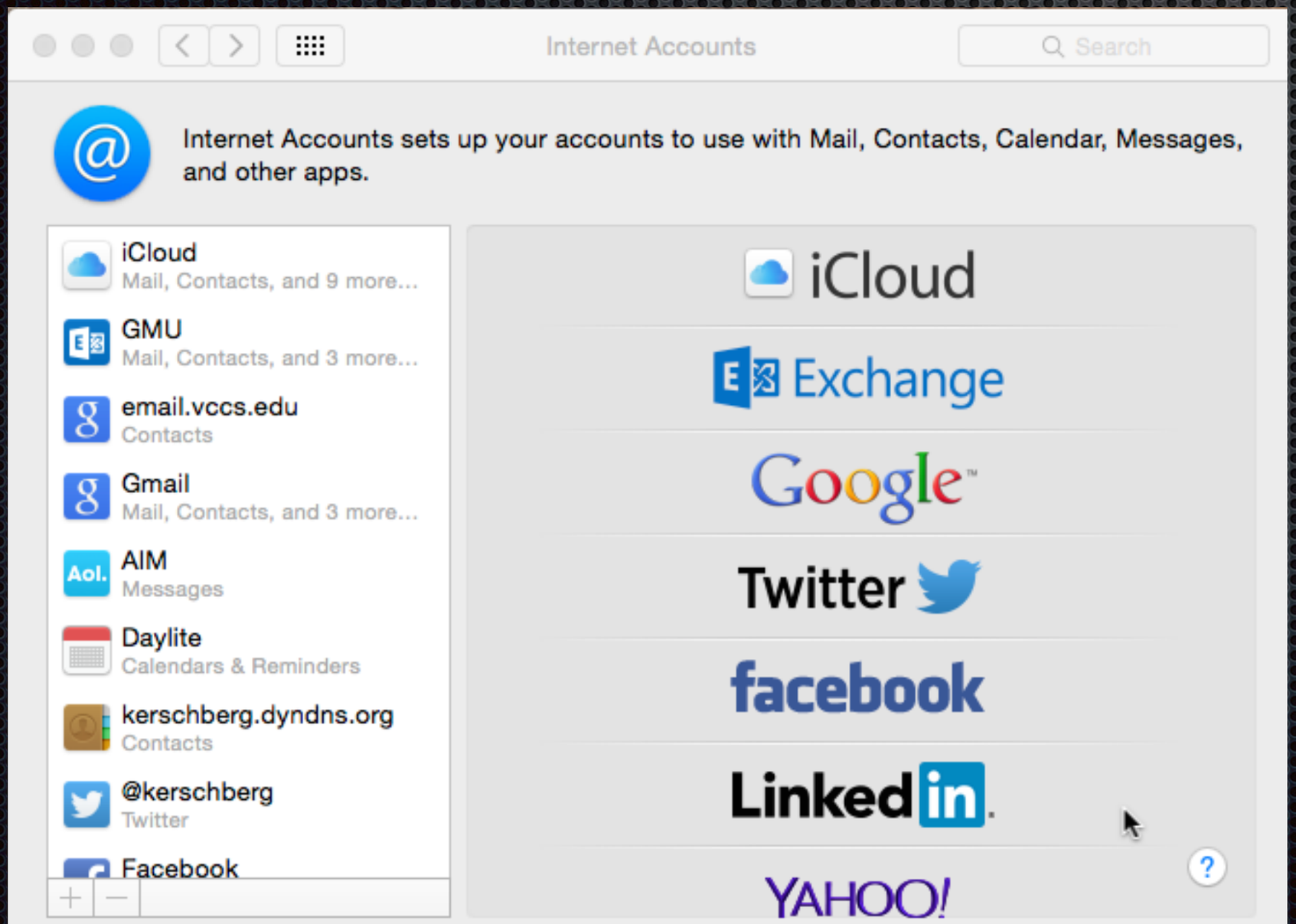
February 28, 2015

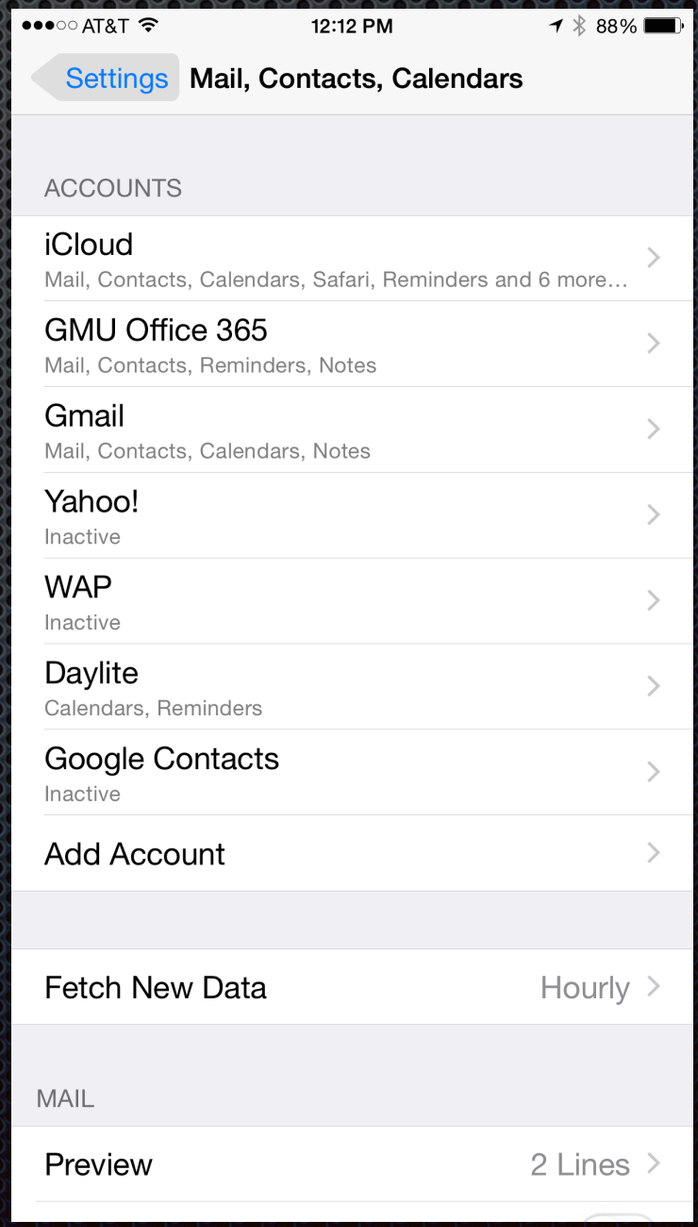
Topics

- Mail on Macs and iOS devices
- Configuring your accounts
- IMAP Folders
- VIP Contacts, Conversations and Notifications
- Smart Mailboxes and Search
- How email flows through the Internet
- Secure email concepts with demonstration.

Mail on Mac and iOS Devices

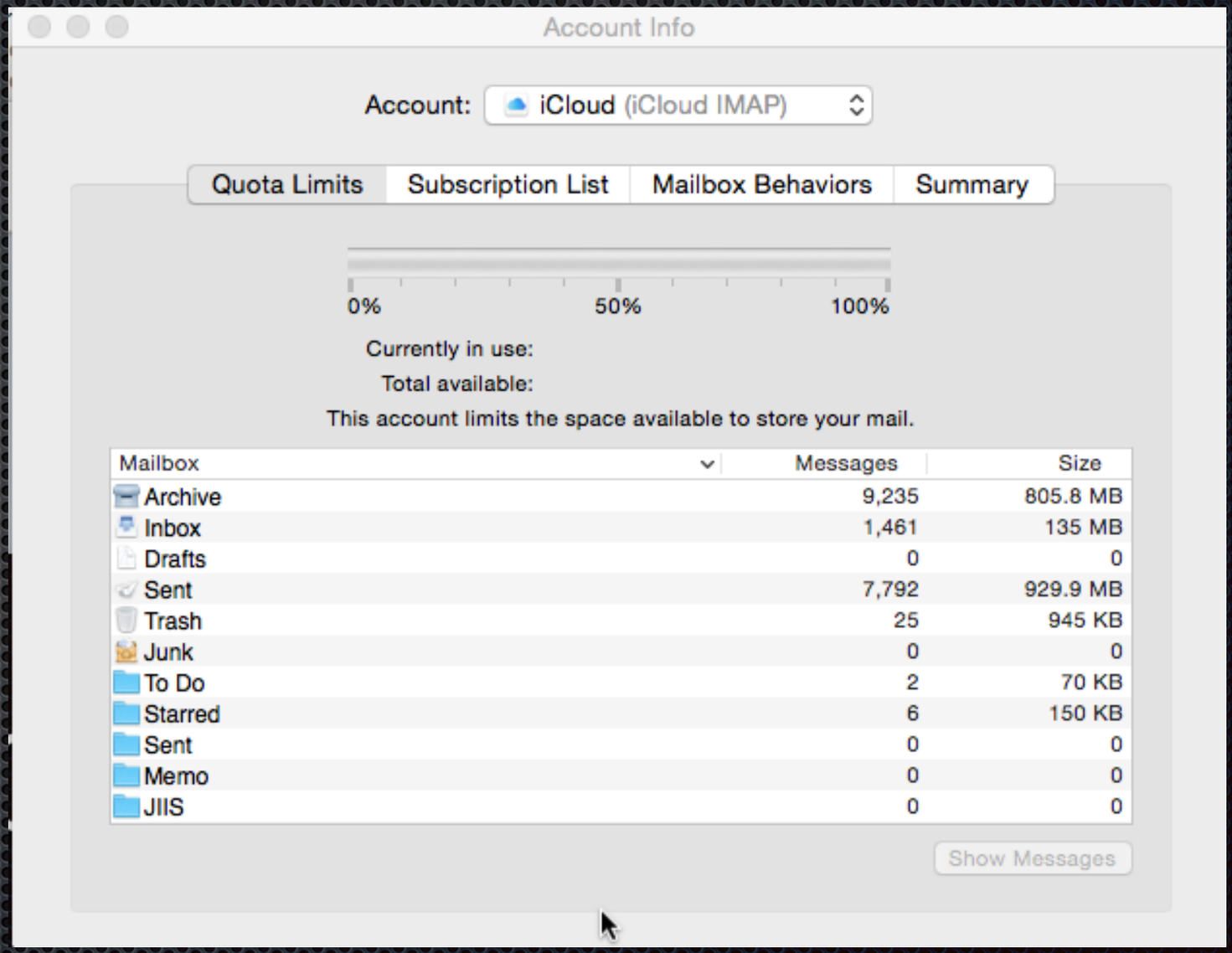
- Set up your email accounts using the Internet Accounts in the System Preferences (Mac) and in "Mail, Contacts, Calendars" in Settings (iPhone/iPad).





Configure your accounts

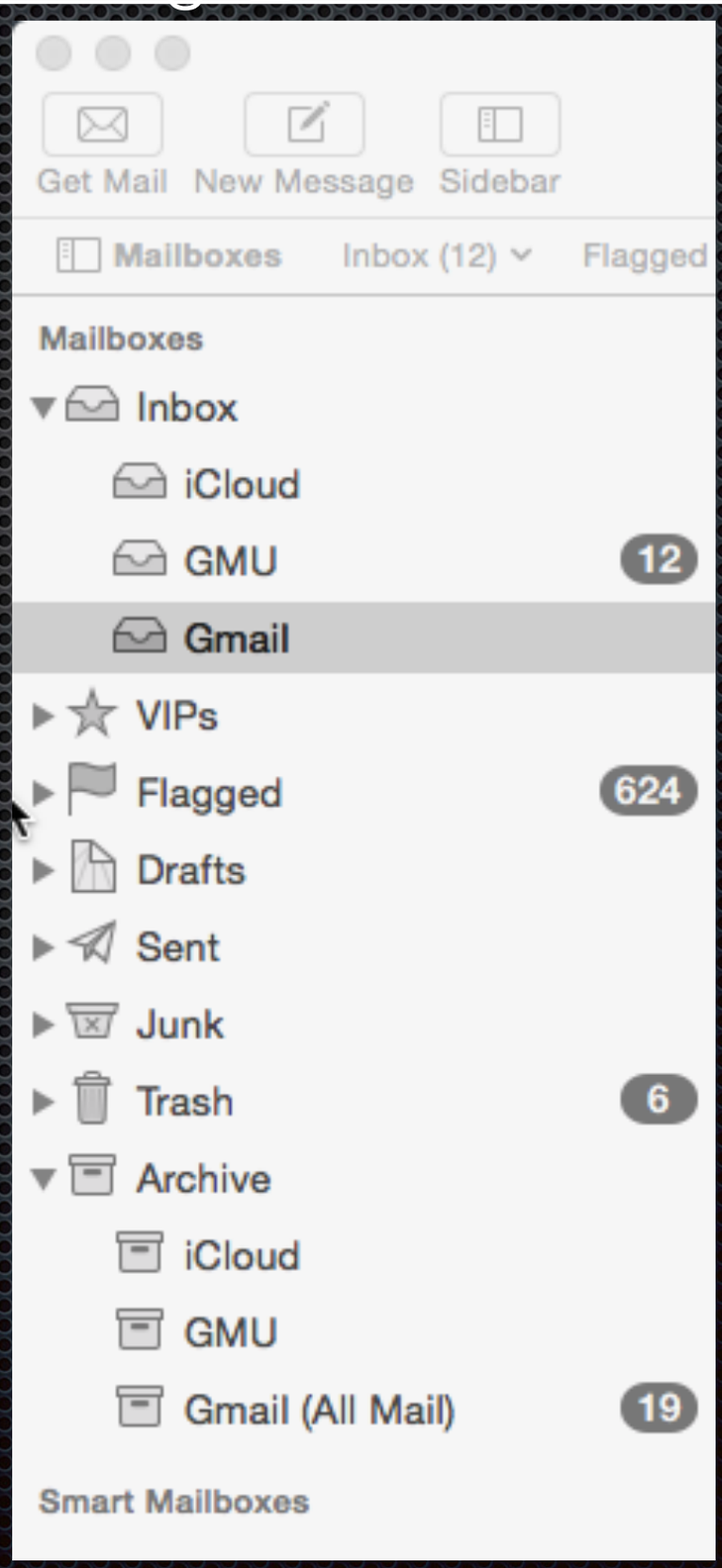
- First you have to have set up your email accounts with each email provider; iCloud mail, Google mail, Yahoo Mail, etc.
- You can view your account settings by accessing account info by right-clicking on the mailbox in the upper-left-hand corner of the main window.



IMAP (Internet Message Access Protocol)

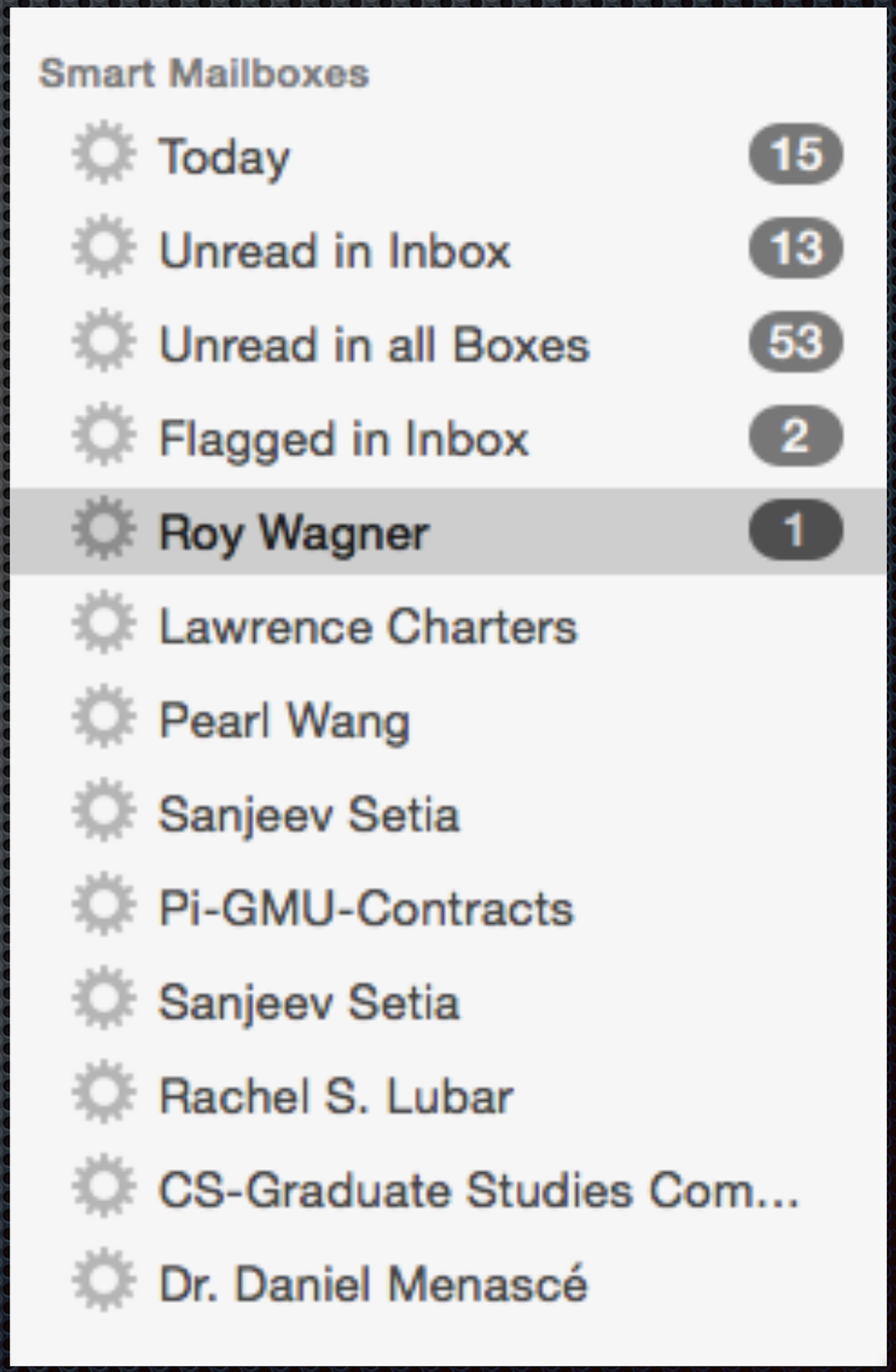
http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

- Most modern email services use IMAP;
- Multiple email "clients" – Mac Mail, Web, iOS – can access messages stored on the server;
- IMAP allows you to define folders and to drag-and-drop messages into these folders;
- If you flag a message in a client, that flag will appear in another client.



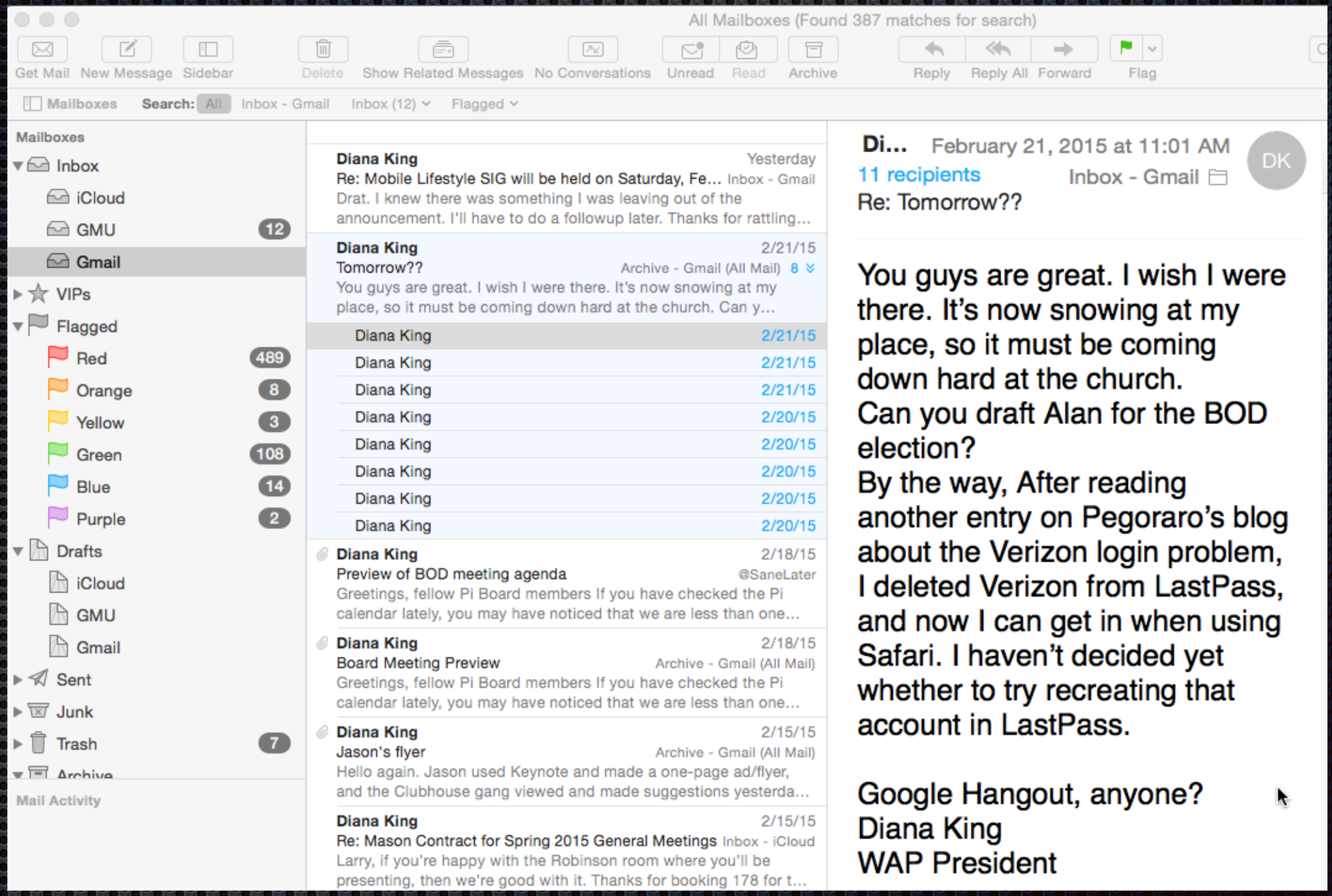
Folders, Smart Mailboxes and Search

- You can create a folder in the sidebar and drag and drop messages into the folder.
- You can also define a Smart Mailbox by means of a rule and then all messages that satisfy the rule conditions will be placed in that smart mailbox.
- You can search the entire collection of mailboxes using the search box on the right-hand-side of the main mail window.



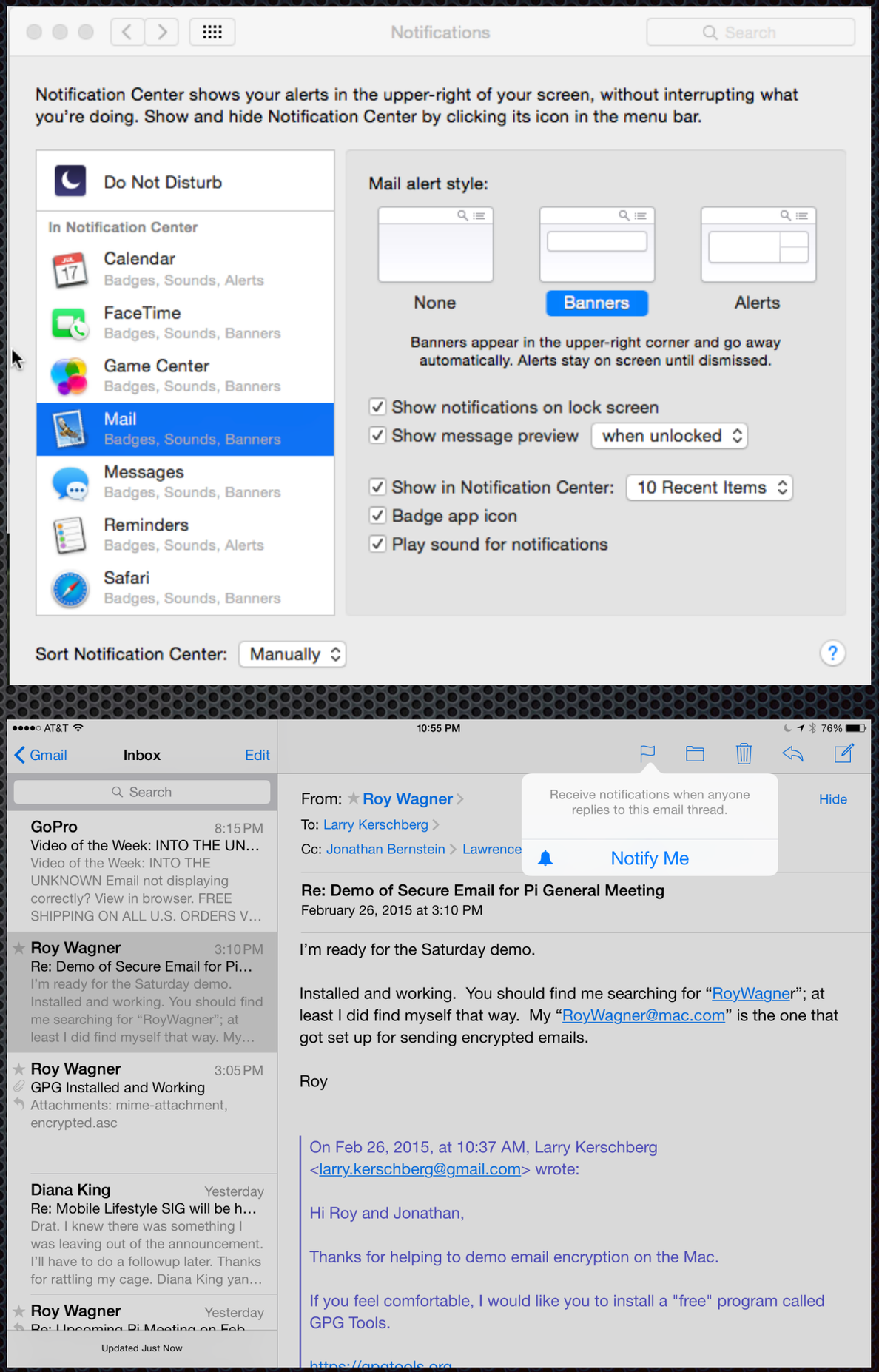
VIP Contacts & Conversations

- You can assign a contact to be a VIP, and all messages from your VIP contact will appear in the VIP folder;
- You have the option of grouping all messages on the same subject as a conversation.



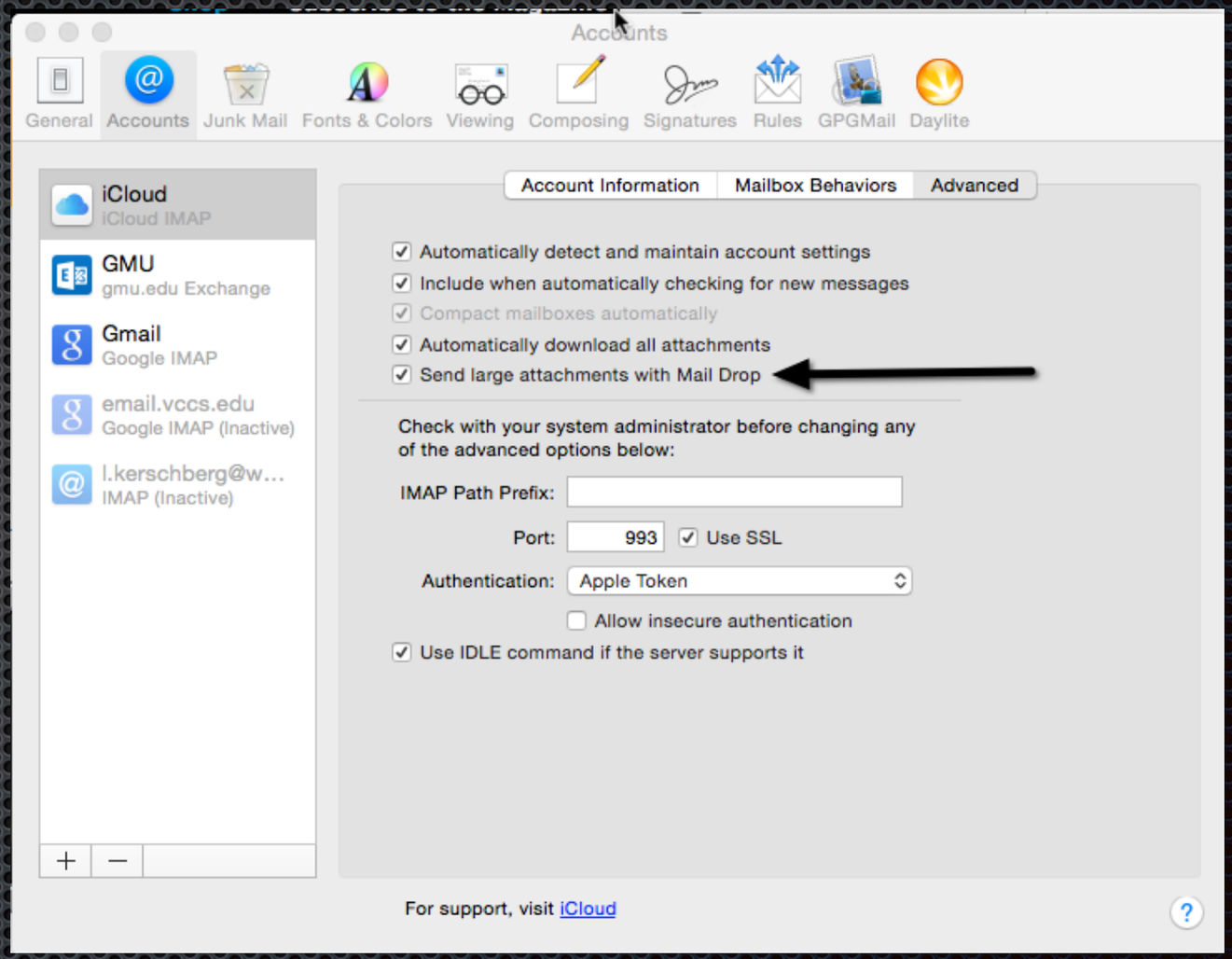
Notifications

- Both OS X Yosemite and iOS 8 have notifications;
- In iOS 8 you can turn on notifications on a particular thread to be notified when someone replies to an email message.



MailDrop for large file attachments

- In Yosemite, go to Mail preferences and for each account for which you want to use MailDrop, check off the: Send large attachments with Mail Drop.

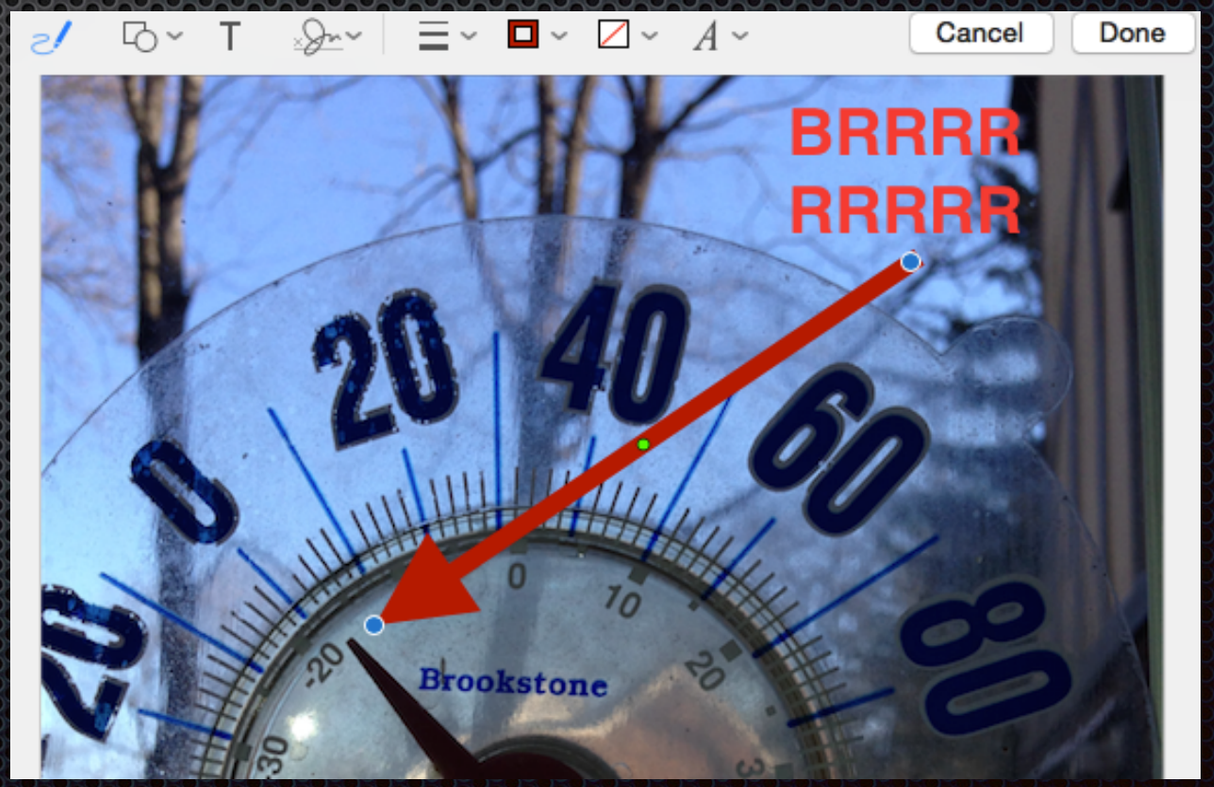


- If an attachment exceeds the limit on the size of the email attachment, the file is stored in iCloud Drive for 30 days for pickup.

Markup in Mail (Yosemite)

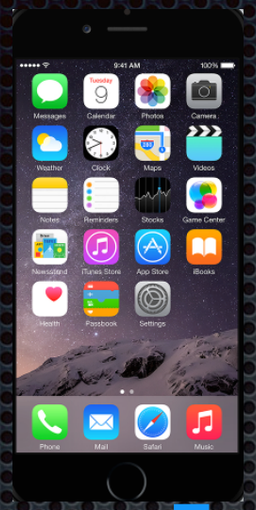
- Most of us know how to use Preview or other tools to annotate pictures or pdfs
- Mail in Yosemite allows such annotation on the fly after attaching a file to a new email message.
- This new feature is called “Markup”

After you attach a picture or pdf file to an email, either by drag and drop or using the “Attach” paper clip, it will appear as an icon in the message. But hover over the attachment and a pulldown lets you choose “Markup”. This opens the attachment with Preview’s annotation tools, allowing on the fly annotations.



How does email travel over the Internet?

Alice



Alice's iPhone

IMAP
HTTP
Protocols

Bob's Laptop

Bob

IMAP
HTTP
Protocols

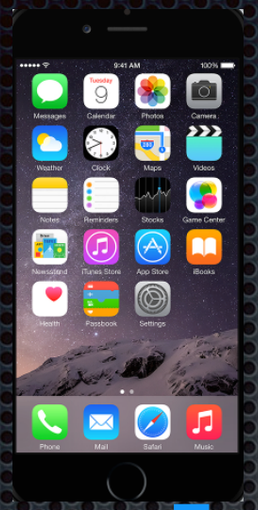
iCloud.com Servers

SMTP
Protocol
Between
Mail Servers

google.com Servers

Security of email transmission over the Internet?

Alice



Alice's iPhone

SECURE

IMAP
HTTP
Protocols

Bob's Laptop

SECURE

IMAP
HTTP
Protocols

Bob

iCloud.com
Servers

SMTP
Protocol
Between
Mail Servers

SECURE

google.com
Servers

Security of the messages themselves

- Our messages may be stored in the Internet Service Provider's servers (iCloud, Google, Yahoo) as "clear text";

- We have to encrypt the messages in our email clients BEFORE we send them to the recipient.
- Then we will have end-to-end secure transmission of our messages.

Simple Encryption Scheme

- Substitution cipher: substituting one thing for another
  - monoalphabetic cipher: substitute one letter for another
    - plaintext: abcdefghijklmnopqrstuvwxyz
    - ciphertext: mnbvcxzasdfghjklpoiuytrewq

Example:

Plaintext: bob. i love you. alice

Ciphertext: nkn. s gktc wky. mgsbc

Key:

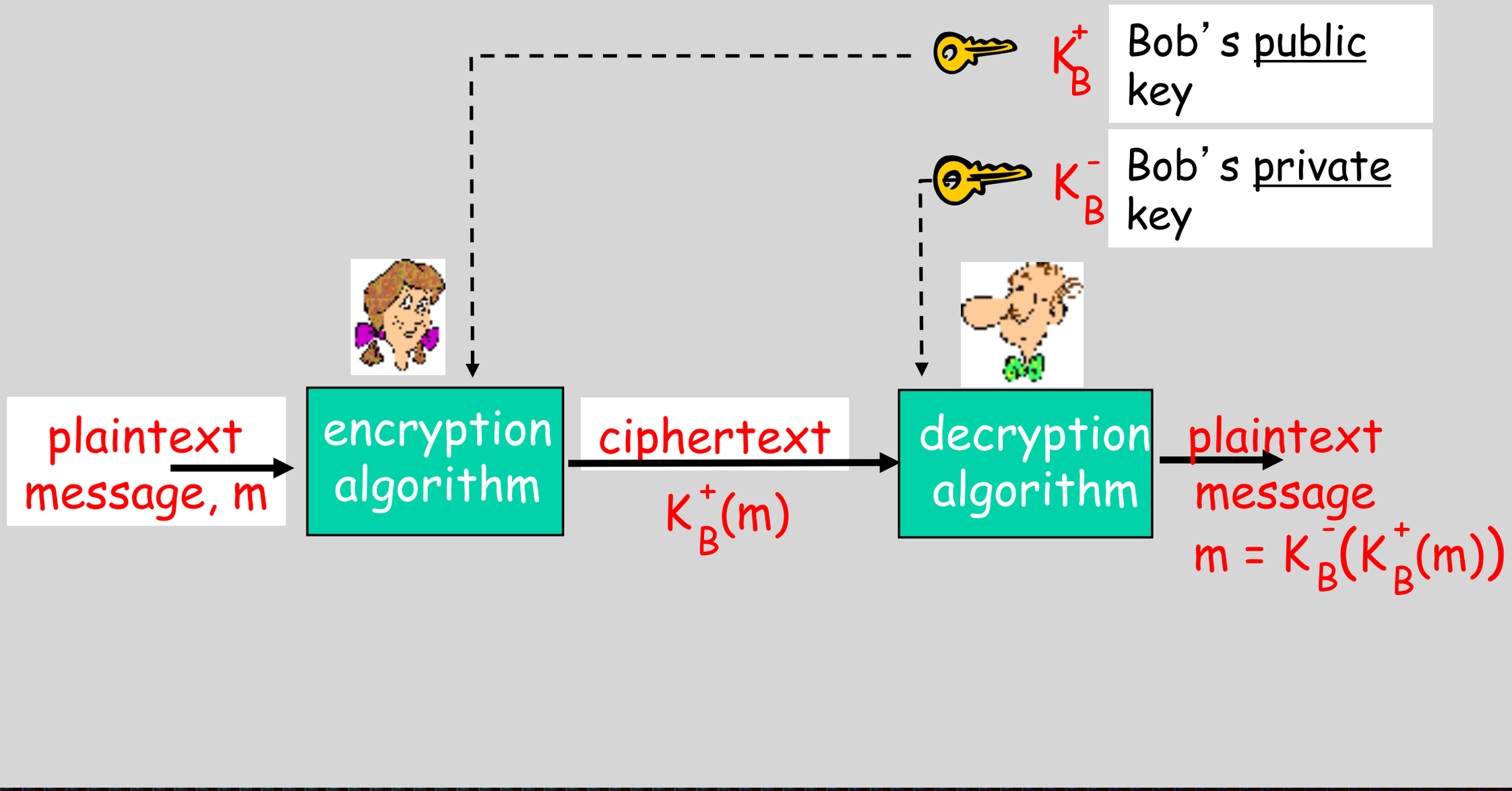
The mapping from the set of 26 letters to the set of 26 letters.

How Modern Encryption Works

- Based on the work of Rivest, Shamir and Adleman (RSA) and Diffie and Helman;
- Use prime numbers to generate two keys:
  - **Public Key** – available to anyone to use to encrypt a message
  - **Private Key** – for you only to use to encrypt messages.
- Private Key is ***impossible*** to break!
- Public keys are stored in a public repository to access and use to encrypt.

Public Key Infrastructure

Public Key Cryptography



From: Kurose/Ross, Computer Networks: A Top-Down Approach

Interesting Property of PKI

- The public and private keys are ***transposable***
  - You can encrypt with the public key and decrypt with the private key; or
  - You can encrypt with the private key and decrypt with the public key.

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

Use public key first, followed by private key

Use private key first, followed by public key

PKI in use for email

- **Digital Signatures**
  - You can use your ***private key*** to sign your message; you have *digitally signed* your message.
  - The recipient of the digitally signed message can access your ***public key*** to verify that you are the sender, with the added assurance that *only you could have sent the message*.
  - Why: Because only you have your private key which is literally impossible to crack.
  - The message will still be sent as *clear text*, unless you encrypt it (see next slide.)

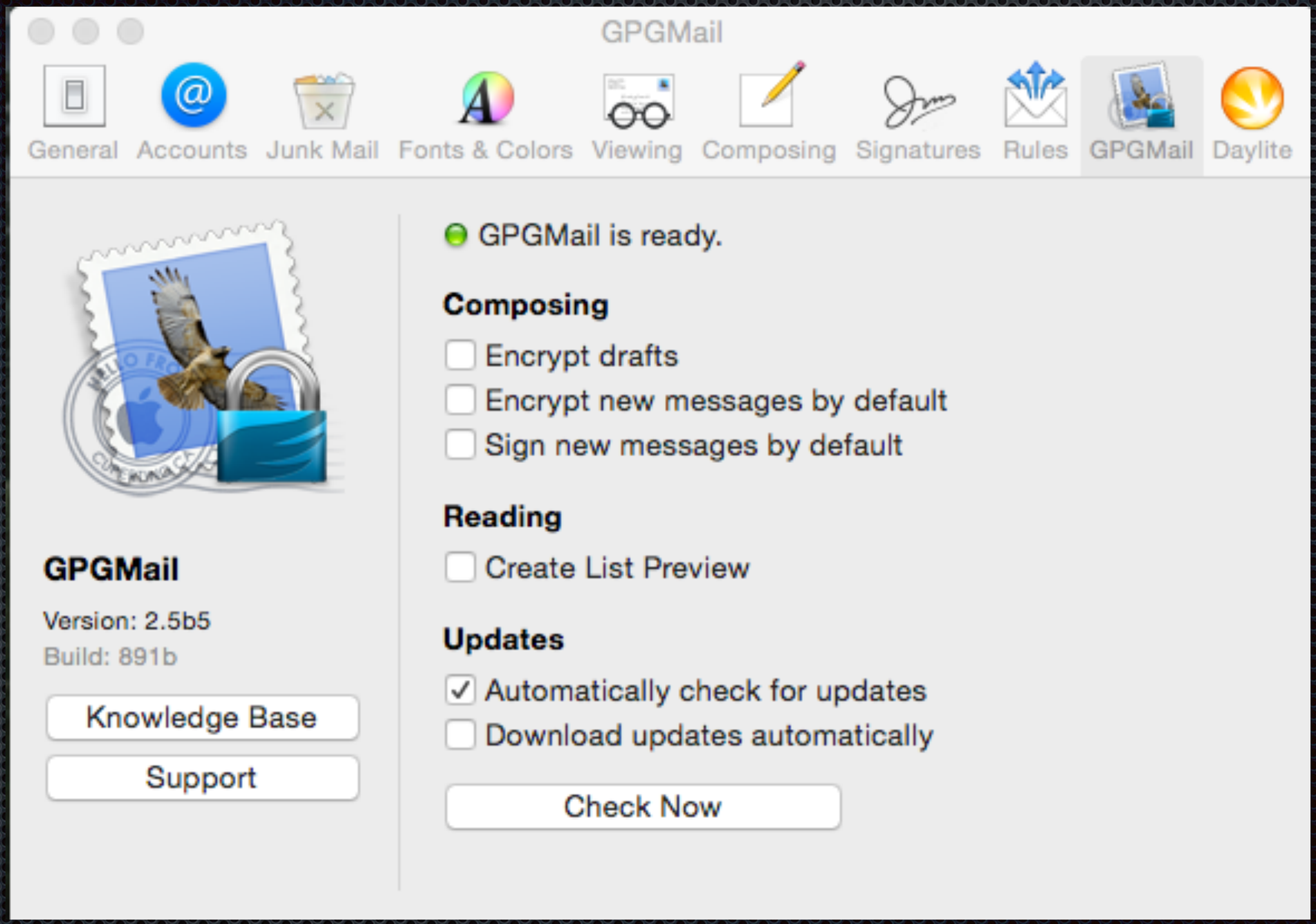
PKI in use for email

- **Encrypting Messages**
  - You can use the recipient's ***public key*** to encrypt your message, with the added assurance that only the recipient will be able to decrypt the message.
    - Why: Because he holds the ***private key*** of the key pair, so only he can read the original message.
    - Furthermore, if the sender has digitally signed the message, the recipient will know that only the sender could have sent the message.
    - So the transposable property of the key pair is very important.

Demonstration of Secure Email

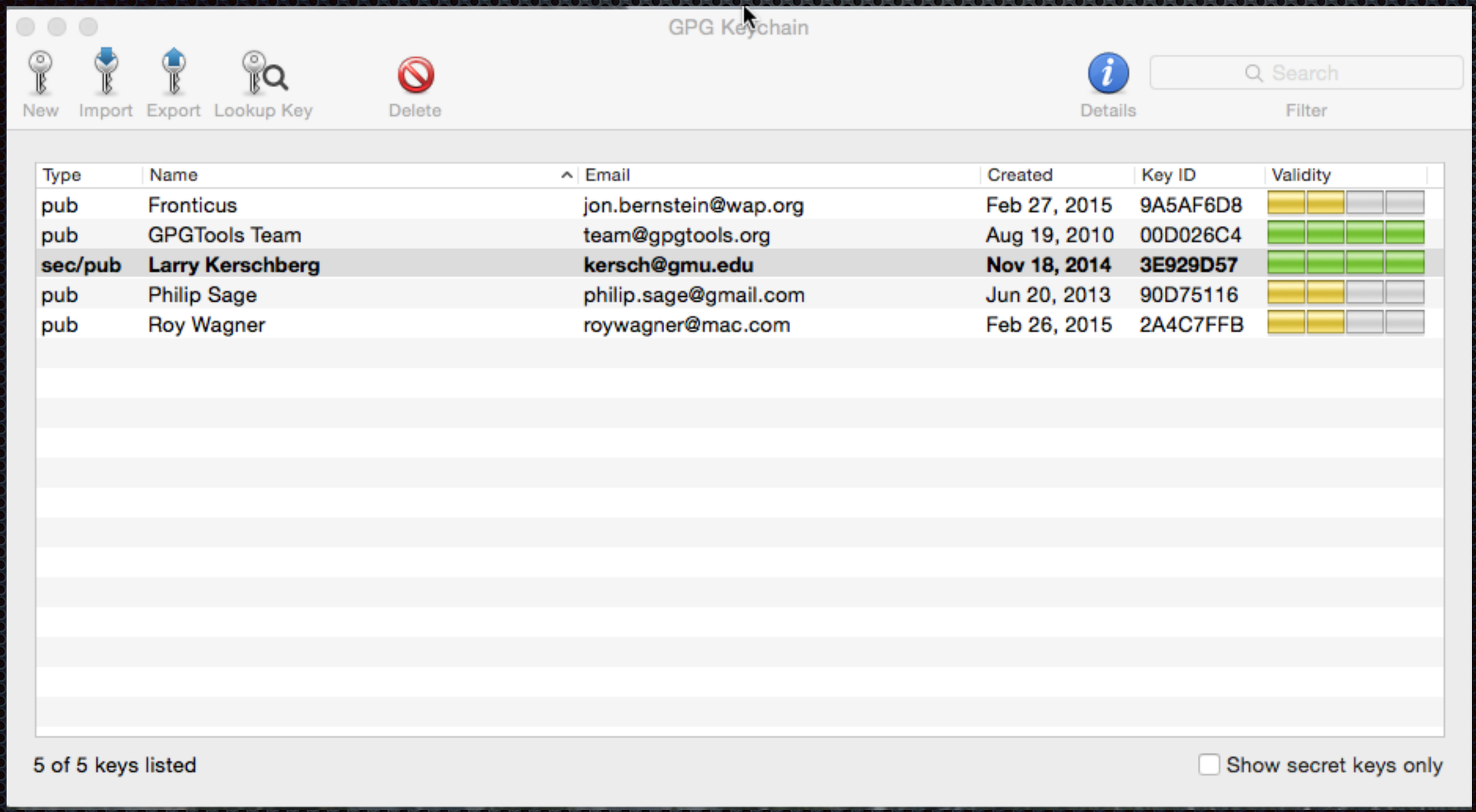
- Use GPGTools: https://gpgtools.org
- Install the application, generate your key pairs using a strong password (store it in 1Password).
- Submit it to the Repository
- Configure your Mail.app preferences
- Begin signing email messages and sending encrypted email messages.

Mail.app GPG Plugin Preferences

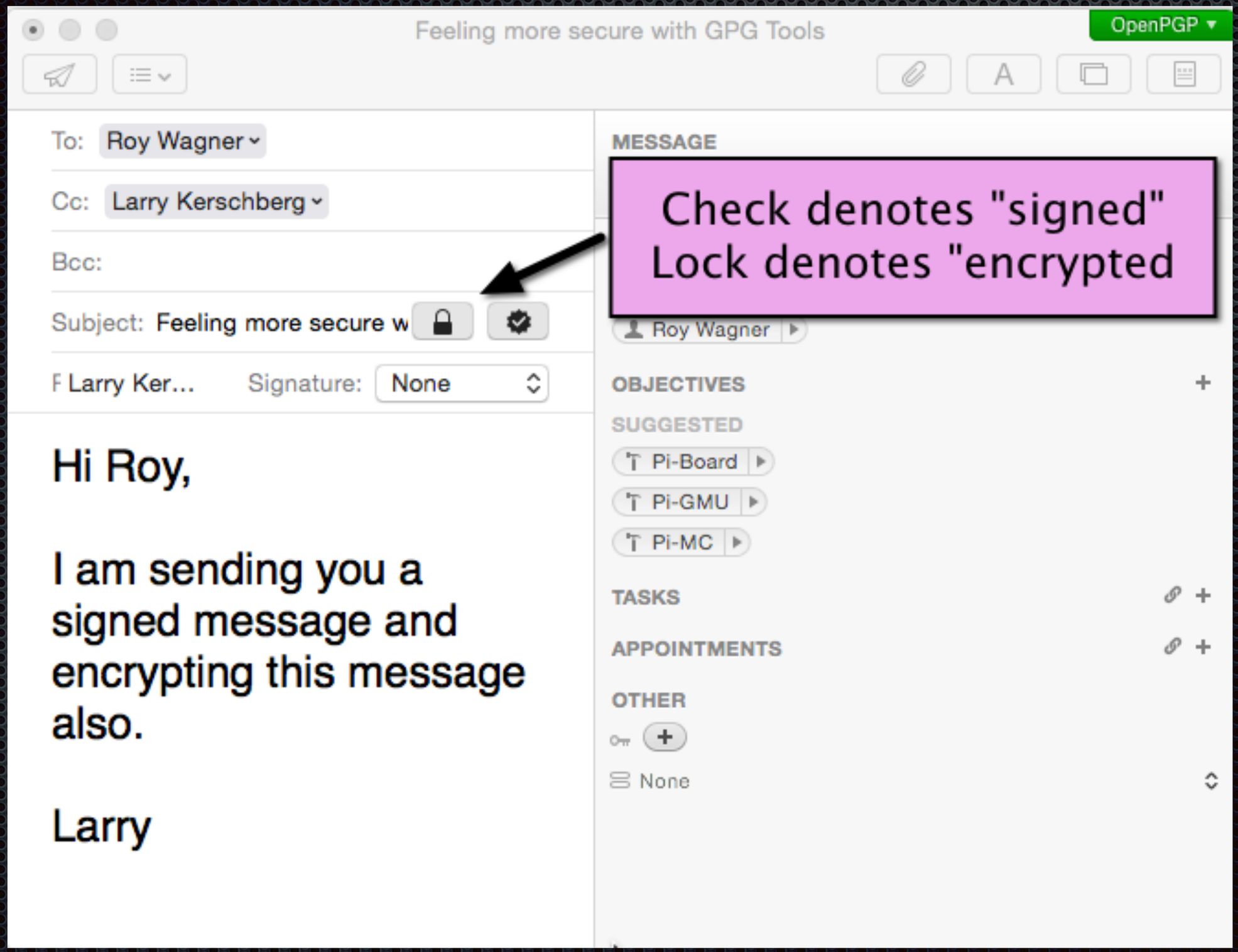


Quick Start Tutorial

GPG Keychain

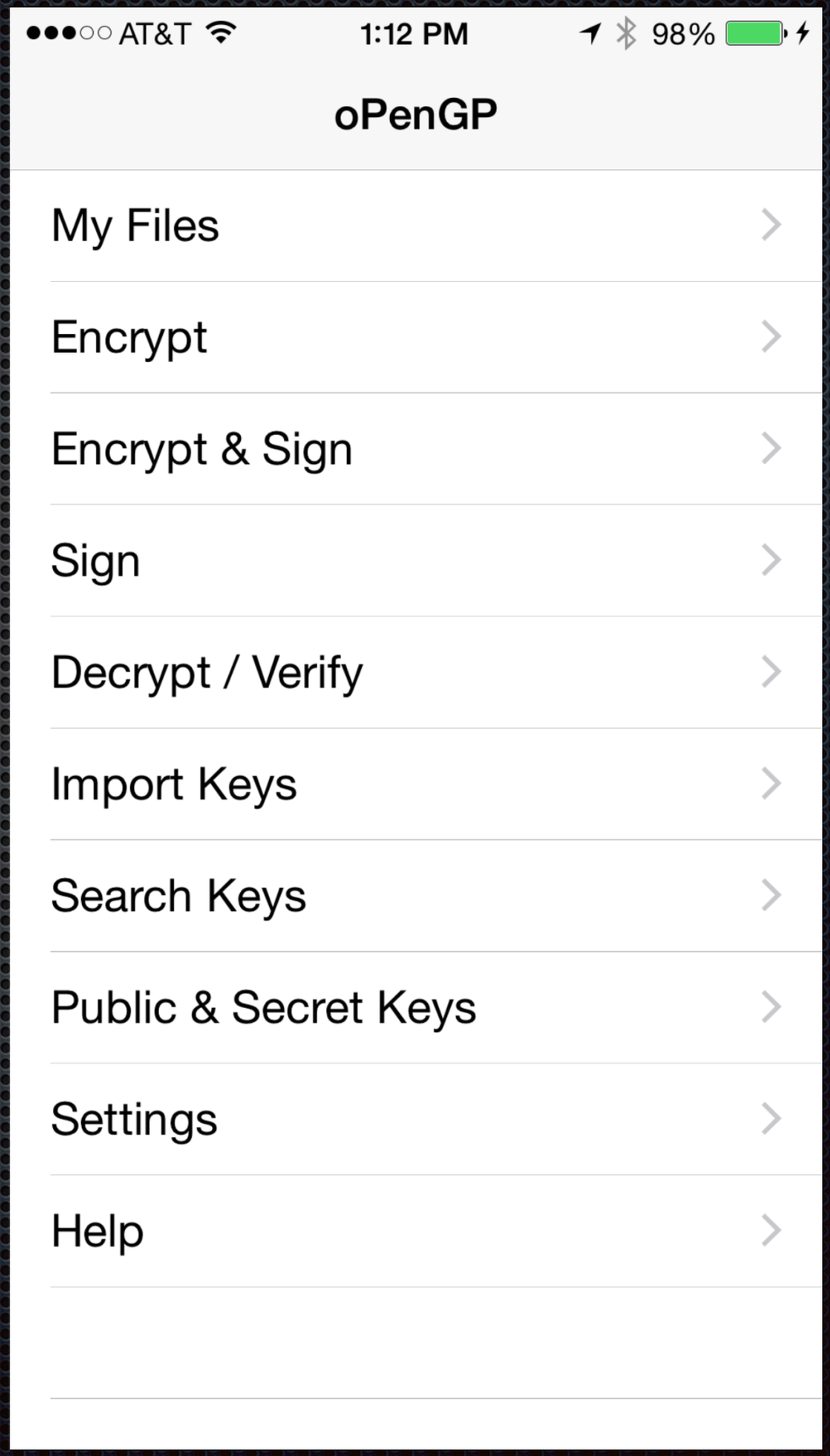


Signed and Encrypted Mail Message

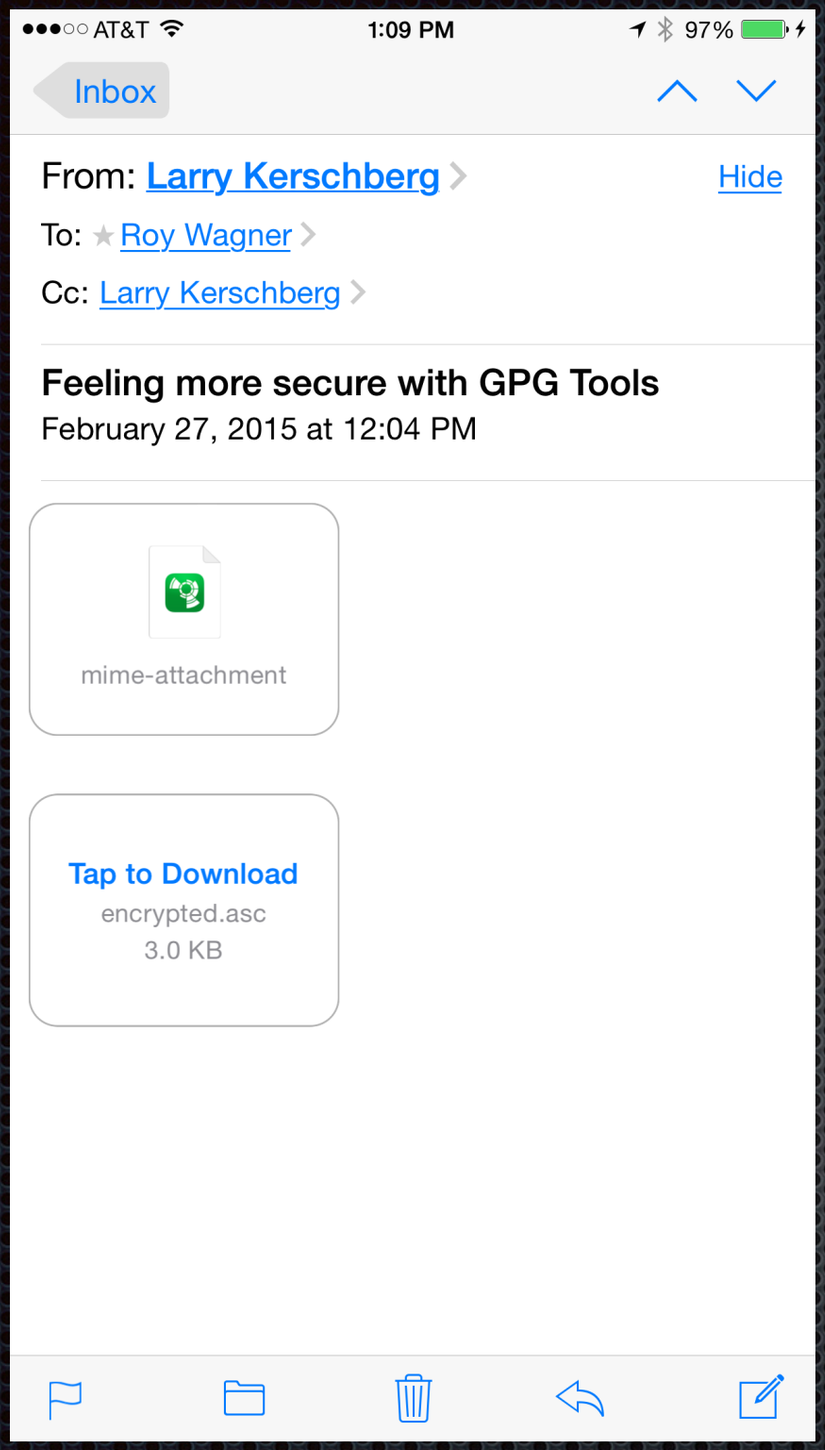


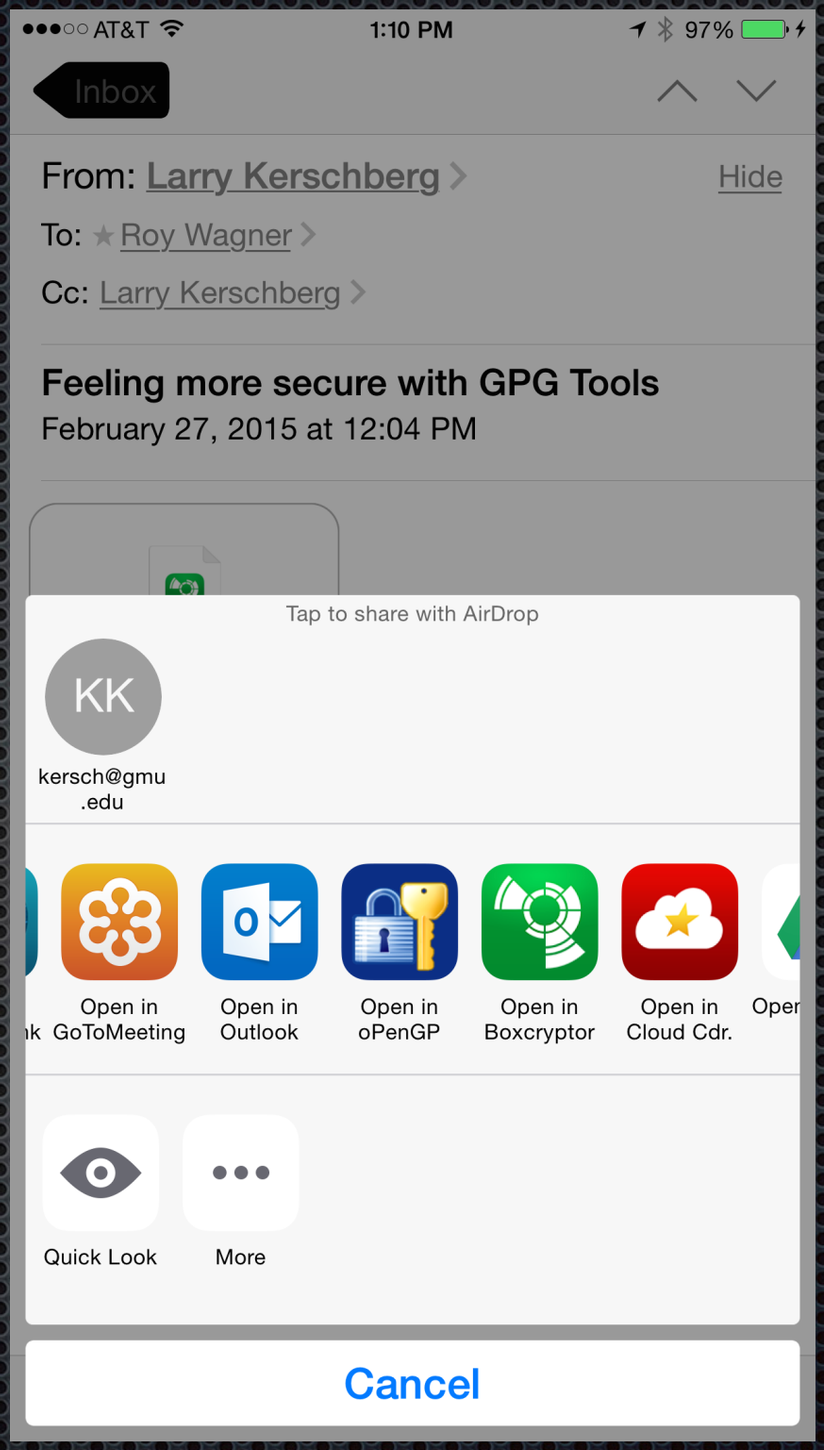
oPenGP for iOS

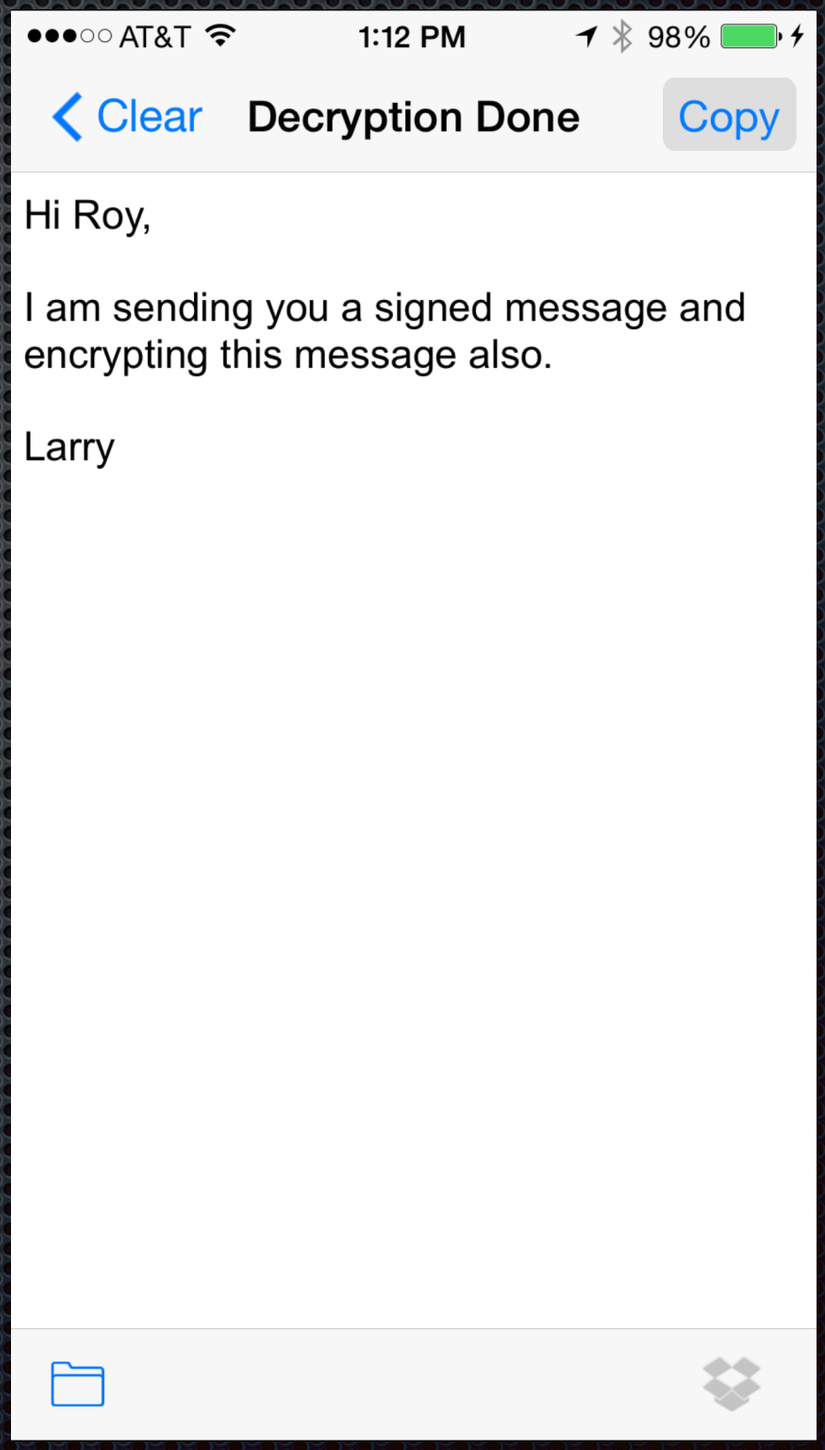
- Read and send signed and encrypted email on your iOS;
- Export your GPG Keychain (including secret key) to a file (.asc)
- Sync the file via app file sharing on iTunes;



Screenshots of oPenGP







Conclusions

- We use email every day as part of our communication with family, friends and family;
- We have shown how to take advantage of the tools provided by Mail on OS X Yosemite and iOS 8;
  - iCloud syncing of accounts,
  - IMAP folders, VIP Contacts, Conversations,
  - MailDrop, Smart Mailboxes, and Search.
- Learned how email messages flow over the Internet;
- PKI encryption can be used in Mail program to both sign messages and to encrypt messages.