Crypto-Book: Secure Facebook messaging

John Maheswaran

The Problem

- Facebook store everything indefinitely
  - Messages, photos, wall posts etc.
  - Facebook software reads messages to display ads
- If someone hacks your account, they can access all your private chats
- Facebook may hand over message transcripts to the government
- If you forget to log out of Facebook on public or shared computer, other people can read everything

Existing solutions

- Symmetrically encrypt using another tool eg encipher.it then send encrypted message over Facebook
  - Requires user to decide on a different password for every friend in advance
- Encrypt-Facebook Chrome plugin
  - Allows you to encrypt messages before you post them to a group
  - Symmetric key for encryption/decryption must be shared in advance
  - Only for Chrome – no other browser support

Existing solutions

- Abine Encrypt
  - Allows you to encrypt messages using transient keypair
  - Messages are lost when you close the browser
  - Other user has to be online at the same time to send them encrypted messages

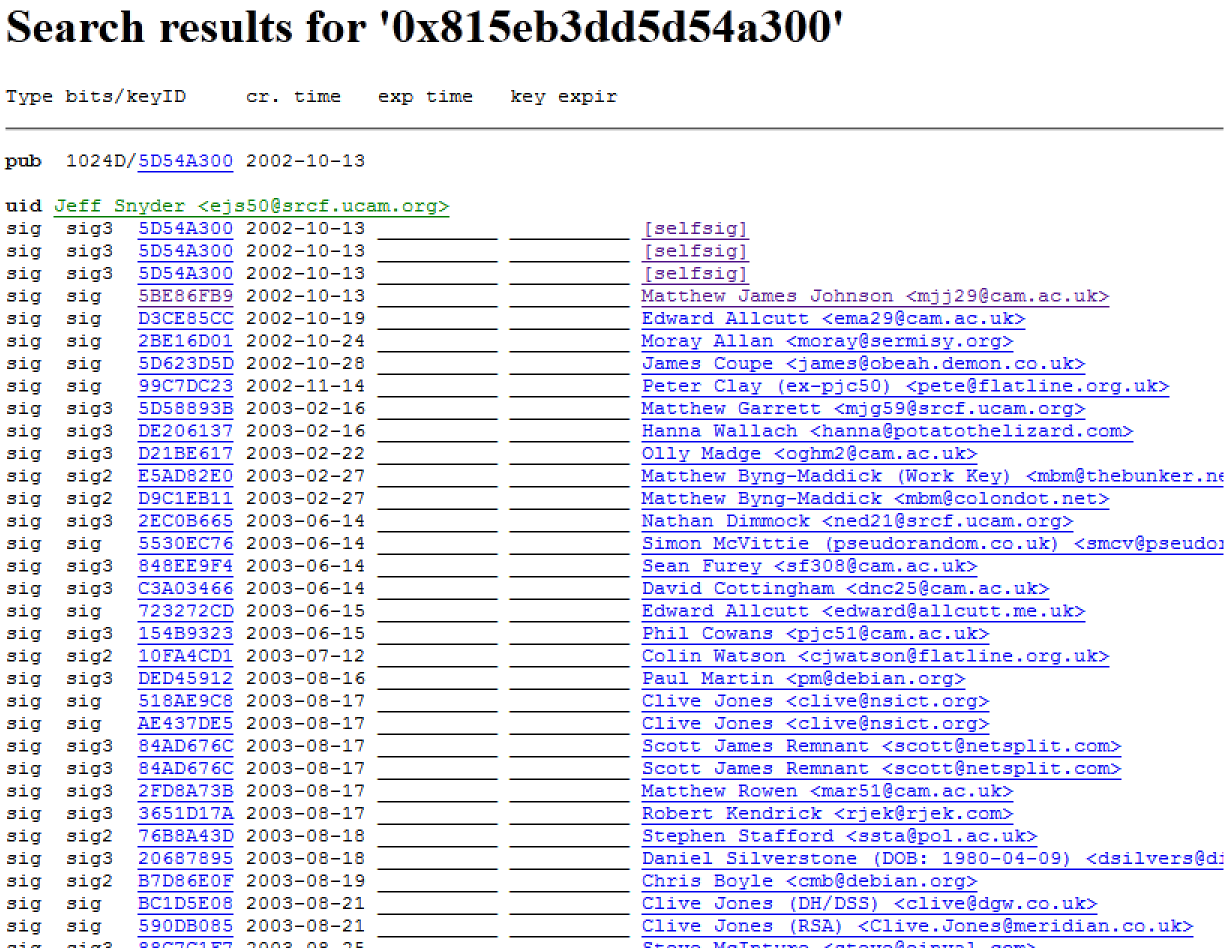
Public/private key encryption

- Asymmetric encryption
- I can send you an encrypted message even if I haven’t set up my own keypair yet
- Secure
- But used be few users due to complexities

Public/private key encryption

- Difficult to use
- Not easy to generate key
  - Have to use command line tools
  - No easy way to generate on Windows
- Difficult to distribute
  - Have to submit to keyserver
- Difficult to look up others’ public keys
- Difficult to use keys to do encryption and decryption

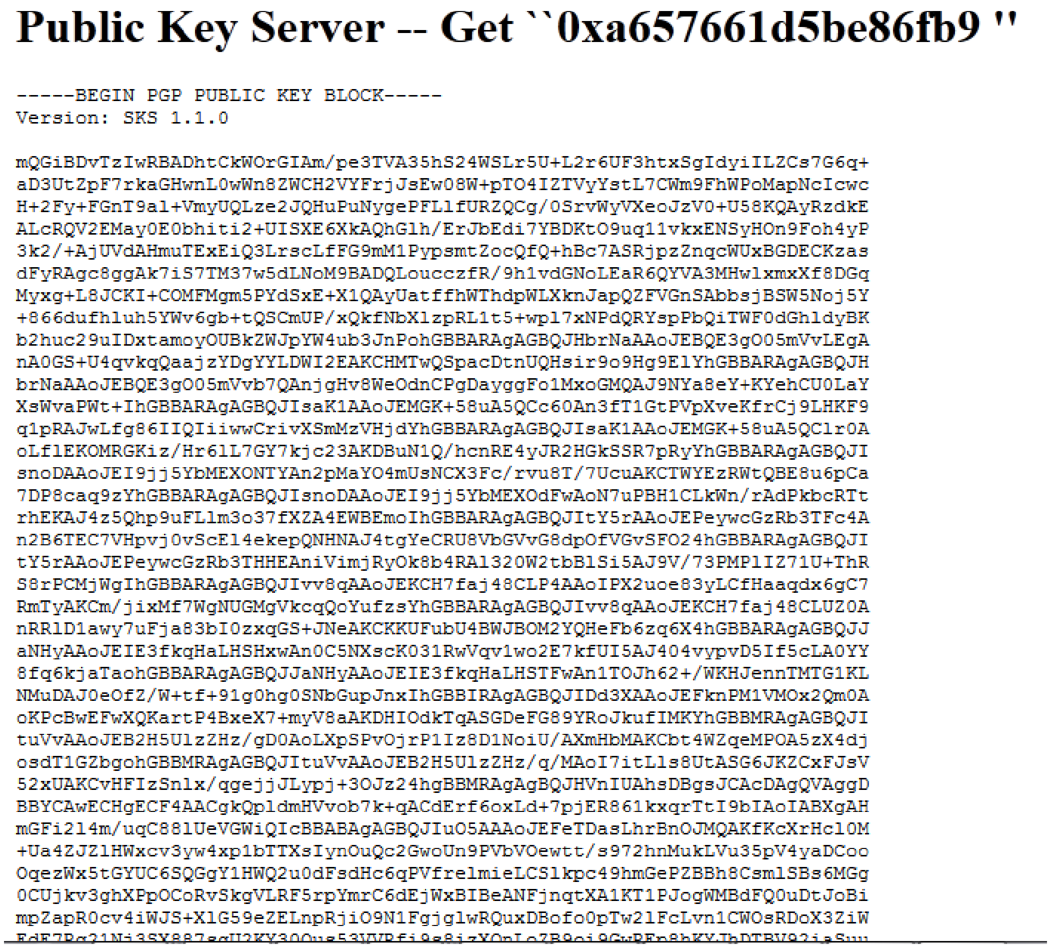
Key lookup not user friendly



Search results for '0x815eb3dd5d54a300'

```
Type bits/keyID     cr. time   exp time   key expir
___________________________________________________________________________________

pub  1024D/5D54A300 2002-10-13

uid Jeff Snyder <ejs50@srcf.ucam.org>
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig   5BE86FB9 2002-10-13 __________ __________ Matthew James Johnson <mjj29@cam.ac.uk>
sig  sig   D3CE85CC 2002-10-19 __________ __________ Edward Allcutt <ema29@cam.ac.uk>
sig  sig   2BE16D01 2002-10-24 __________ __________ Moray Allan <moray@sermisy.org>
sig  sig   5D623D5D 2002-10-28 __________ __________ James Coupe <james@obeah.demon.co.uk>
sig  sig   99C7DC23 2002-11-14 __________ __________ Peter Clay (ex-pjc50) <pete@flatline.org.uk>
sig  sig3  5D58893B 2003-02-16 __________ __________ Matthew Garrett <mjg59@srcf.ucam.org>
sig  sig3  DE206137 2003-02-16 __________ __________ Hanna Wallach <hanna@potatothelizard.com>
sig  sig3  D21BE617 2003-02-22 __________ __________ Olly Madge <oghm2@cam.ac.uk>
sig  sig2  E5AD82E0 2003-02-27 __________ __________ Matthew Byng-Maddick (Work Key) <mbm@thebunker.ne
sig  sig2  D9C1EB11 2003-02-27 __________ __________ Matthew Byng-Maddick <mbm@colondot.net>
sig  sig3  2EC0B665 2003-06-14 __________ __________ Nathan Dimmock <ned21@srcf.ucam.org>
sig  sig   5530EC76 2003-06-14 __________ __________ Simon McVittie (pseudorandom.co.uk) <smcv@pseudo
sig  sig3  848EE9F4 2003-06-14 __________ __________ Sean Furey <sf308@cam.ac.uk>
sig  sig3  C3A03466 2003-06-14 __________ __________ David Cottingham <dnc25@cam.ac.uk>
sig  sig   723272CD 2003-06-15 __________ __________ Edward Allcutt <edward@allcutt.me.uk>
sig  sig3  154B9323 2003-06-15 __________ __________ Phil Cowans <pjc51@cam.ac.uk>
sig  sig2  10FA4CD1 2003-07-12 __________ __________ Colin Watson <cjwatson@flatline.org.uk>
sig  sig3  DED45912 2003-08-16 __________ __________ Paul Martin <pm@debian.org>
sig  sig   518AE9C8 2003-08-17 __________ __________ Clive Jones <clive@nsict.org>
sig  sig   AE437DE5 2003-08-17 __________ __________ Clive Jones <clive@nsict.org>
sig  sig3  84AD676C 2003-08-17 __________ __________ Scott James Remnant <scott@netsplit.com>
sig  sig3  84AD676C 2003-08-17 __________ __________ Scott James Remnant <scott@netsplit.com>
sig  sig3  2FD8A73B 2003-08-17 __________ __________ Matthew Rowen <mar51@cam.ac.uk>
sig  sig3  3651D17A 2003-08-17 __________ __________ Robert Kendrick <rjek@rjek.com>
sig  sig2  76B8A43D 2003-08-18 __________ __________ Stephen Stafford <ssta@pol.ac.uk>
sig  sig3  20687895 2003-08-18 __________ __________ Daniel Silverstone (DOB: 1980-04-09) <dsilvers@di
sig  sig2  B7D86E0F 2003-08-19 __________ __________ Chris Boyle <cmb@debian.org>
sig  sig   BC1D5E08 2003-08-21 __________ __________ Clive Jones (DH/DSS) <clive@dgw.co.uk>
sig  sig   590DB085 2003-08-21 __________ __________ Clive Jones (RSA) <Clive.Jones@meridian.co.uk>
sig  sig3  88C7C1F7 2003-08-25                       Steve McIntyre <steve@einval.com>
```

Keys are confusing to most users

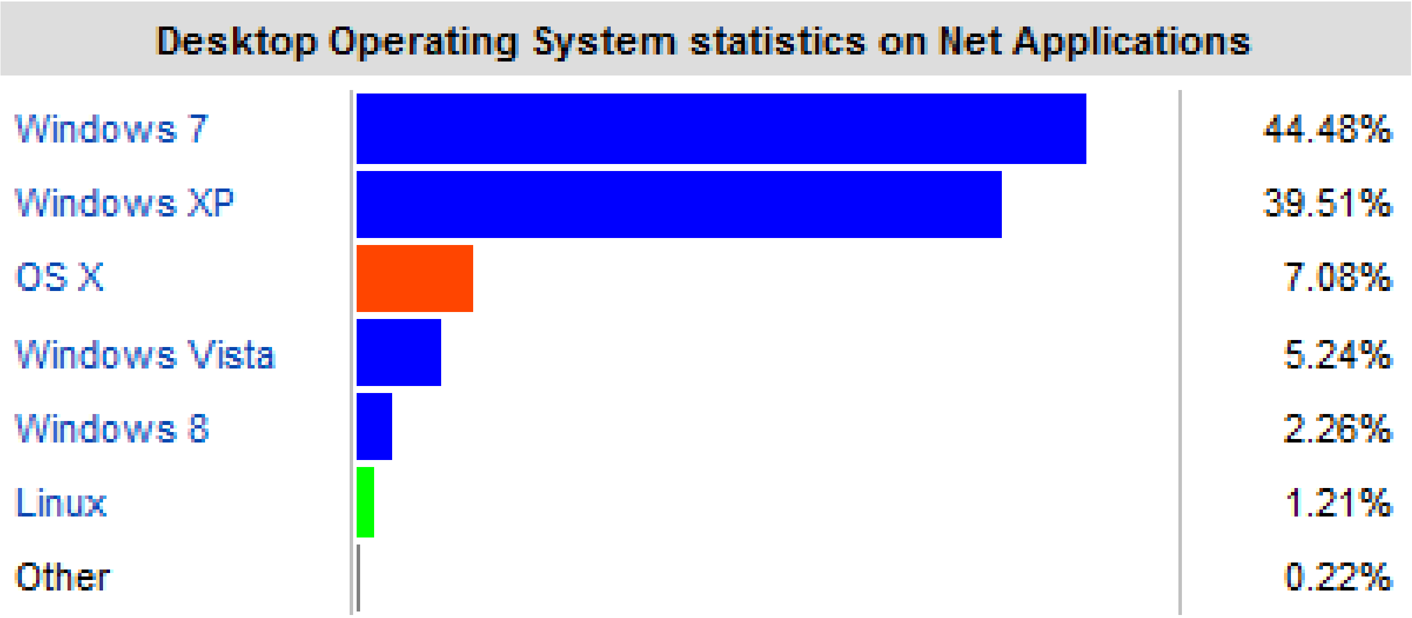


Public Key Server -- Get ``0xa657661d5be86fb9 ''

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQGiBDvTzIwRBADhtCkWOrGIAm/pe3TVA35hS24WSLr5U+L2r6UF3htxSgIdyiILZCs7G6q+
aD3UtZpF7rkaGHwnL0wWn8ZWCH2VYFrjJsEw08W+pTO4IZTVyYstL7CWm9FhWPoMapNcIcwc
H+2Fy+FGnT9al+VmyUQLze2JQHuPuNygePFL1fURZQCg/0SrvWyVXeoJzV0+U58KQAyRzdkE
ALcRQV2EMay0E0bhiti2+UISXE6XkAQhGlh/ErJbEdi7YBDKtO9uq11vkxENSyHOn9Foh4yP
3k2/+AjUVdAHmuTExEiQ3LrscLfFG9mM1PypsmtZocQfQ+hBc7ASRjpzZnqcWUxBGDECKzas
dFyRAgc8ggAk7iS7TM37w5dLNoM9BADQLoucczfR/9h1vdGNoLEaR6QYVA3MHwlxmxXf8DGq
Myxg+L8JCKI+COMFMgm5PYdSxE+X1QAyUatffhWThdpWLXknJapQZFVGnSAbbsjBSW5Noj5Y
+866dufhluh5YWv6gb+tQSCmUP/xQkfNbXlzpRL1t5+wpl7xNPdQRYspPbQiTWF0dGhldyBK
b2huc29uIDxtamoyOUBkZWJpYW4ub3JnPohGBBARAgAGBQJHbrNaAAoJEBQE3gO05mVvLEgA
nA0GS+U4qvkqQaajzYDgYYLDWI2EAKCHMTwQSpacDtnUQHsir9o9Hg9ElYhGBBARAgAGBQJH
brNaAAoJEBQE3gO05mVvb7QAnjgHv8WeOdnCPgDayggFo1MxoGMQAJ9NYa8eY+KYehCU0LaY
XsWvaPWt+IhGBBARAgAGBQJIsaK1AAoJEMGK+58uA5QCc60An3fT1GtPVpXveKfrCj9LHKF9
q1pRAJwLfg86IIQIiiwwCrivXSmMzVHjdYhGBBARAgAGBQJIsaK1AAoJEMGK+58uA5QClr0A
oLf1EKOMRGKiz/Hr6lL7GY7kjc23AKDBuN1Q/hcnRE4yJR2HGkSSR7pRyYhGBBARAgAGBQJI
snoDAAoJEI9jj5YbMEXONTYAn2pMaYO4mUsNCX3Fc/rvu8T/7UcuAKCTWYEzRWtQBE8u6pCa
7DP8caq9zYhGBBARAgAGBQJIsnoDAAoJEI9jj5YbMEXOdFwAoN7uPBH1CLkWn/rAdPkbcRTt
rhEKAJ4z5Qhp9uFLlm3o37fXZA4EWBEmoIhGBBARAgAGBQJItY5rAAoJEPeywcGzRb3TFc4A
n2B6TEC7VHpvj0vScEl4ekepQNHNAJ4tgYeCRU8VbGVvG8dpOfVGvSFO24hGBBARAgAGBQJI
tY5rAAoJEPeywcGzRb3THHEAniVimjRyOk8b4RAl320W2tbBlSi5AJ9V/73PMPlIZ71U+ThR
S8rPCMjWgIhGBBARAgAGBQJIvv8qAAoJEKCH7faj48CLP4AAoIPX2uoe83yLCfHaaqdx6gC7
RmTyAKCm/jixMf7WgNUGMgVkcqQoYufzsYhGBBARAgAGBQJIvv8qAAoJEKCH7faj48CLUZ0A
nRRlD1awy7uFja83bI0zxqGS+JNeAKCKKUFubU4BWJBOM2YQHeFb6zq6X4hGBBARAgAGBQJJ
aNHyAAoJEIE3fkqHaLHSHxwAn0C5NXscK031RwVqv1wo2E7kfUI5AJ404vypvD5If5cLA0YY
8fq6kjaTaohGBBARAgAGBQJJaNHyAAoJEIE3fkqHaLHSTFwAn1TOJh62+/WKHJennTMTG1KL
NMuDAJ0eOfZ/W+tf+91g0hg0SNbGupJnxIhGBBIRAgAGBQJIDd3XAAoJEFknPM1VMOx2Qm0A
oKPcBwEFwXQKartP4BxeX7+myV8aAKDHIOdkTqASGDeFG89YRoJkufIMKYhGBBMRAgAGBQJI
tuVvAAoJEB2H5UlzZHz/gD0AoLXpSPvOjrP1Iz8D1NoiU/AXmHbMAKCbt4WZqeMPOA5zX4dj
osdT1GZbgohGBBMRAgAGBQJItuVvAAoJEB2H5UlzZHz/q/MAoI7itLls8UtASG6JKZCxFJsV
52xUAKCvHFIzSnlx/qgejjJLypj+3OJz24hgBBMRAgAgBQJHVnIUAhsDBgsJCAcDAgQVAggD
BBYCAwECHgECF4AACgkQpldmHVvob7k+qACdErf6oxLd+7pjER861kxqrTtI9bIAoIABXgAH
mGFi2l4m/uqC88lUeVGWiQIcBBABAgAGBQJIuO5AAAoJEFeTDasLhrBnOJMQAKfKcXrHcl0M
+Ua4ZJZlHWxcv3yw4xp1bTTXsIynOuQc2GwoUn9PVbVOewtt/s972hnMukLVu35pV4yaDCoo
OqezWx5tGYUC6SQGgY1HWQ2u0dFsdHc6qPVfrelmieLCSlkpc49hmGePZBBh8CsmlSBs6MGg
0CUjkv3ghXPpOCoRvSkgVLRF5rpYmrC6dEjWxBIBeANFjnqtXA1KT1PJogWMBdFQ0uDtJoBi
mpZapR0cv4iWJS+XlG59eZELnpRjiO9N1FgjglwRQuxDBofo0pTw2lFcLvn1CWOsRDoX3ZiW
FdF7Rg21Nj3SX887sgU2KY3OOus53VVRfi9s8jzYOnLo7B9oj9GwRFn8hKYJhDTBV92iaSuu
```

Windows market share

- Need an easy way to do it on Windows
  - – 84% market share



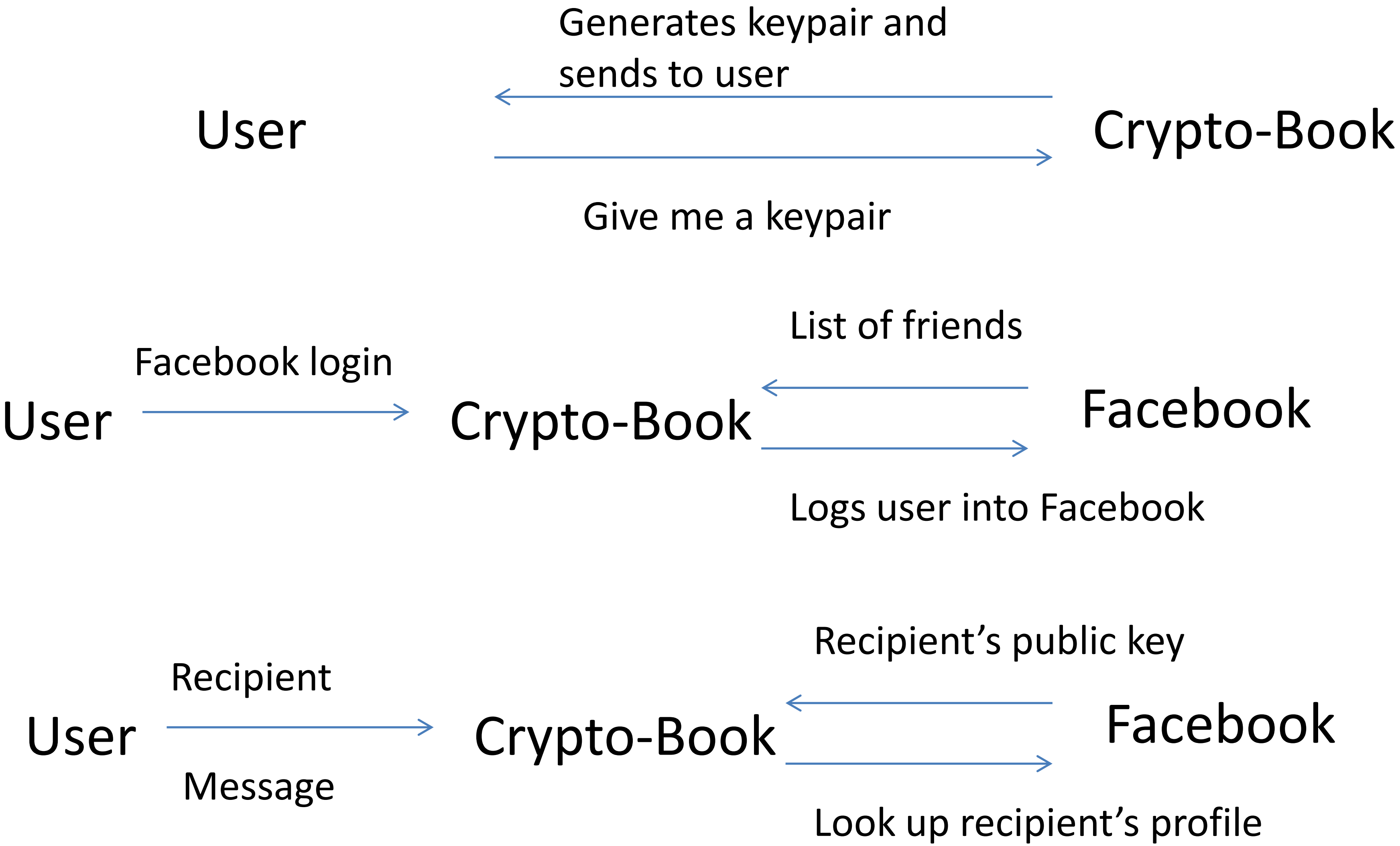
To make encryption easy

- Easy way to generate key
- Easy way to publish key
- Easy way to find friends’ keys
- Easy way to use friends’ keys to send them encrypted messages

My solution: Crypto-Book

- Allows you to easily create and share your public key
  - One click key generation
- Simple interface to send friends encrypted messages through Facebook
- Fully integrated decrypter app allows you to read encrypted messages
  - Cross platform: Windows, Mac/Linux
  - One click install on Windows

System overview



Generates keypair and sends to user

User

Crypto-Book

Give me a keypair

List of friends

Facebook login

User

Crypto-Book

Facebook

Logs user into Facebook

Recipient's public key

Recipient

User

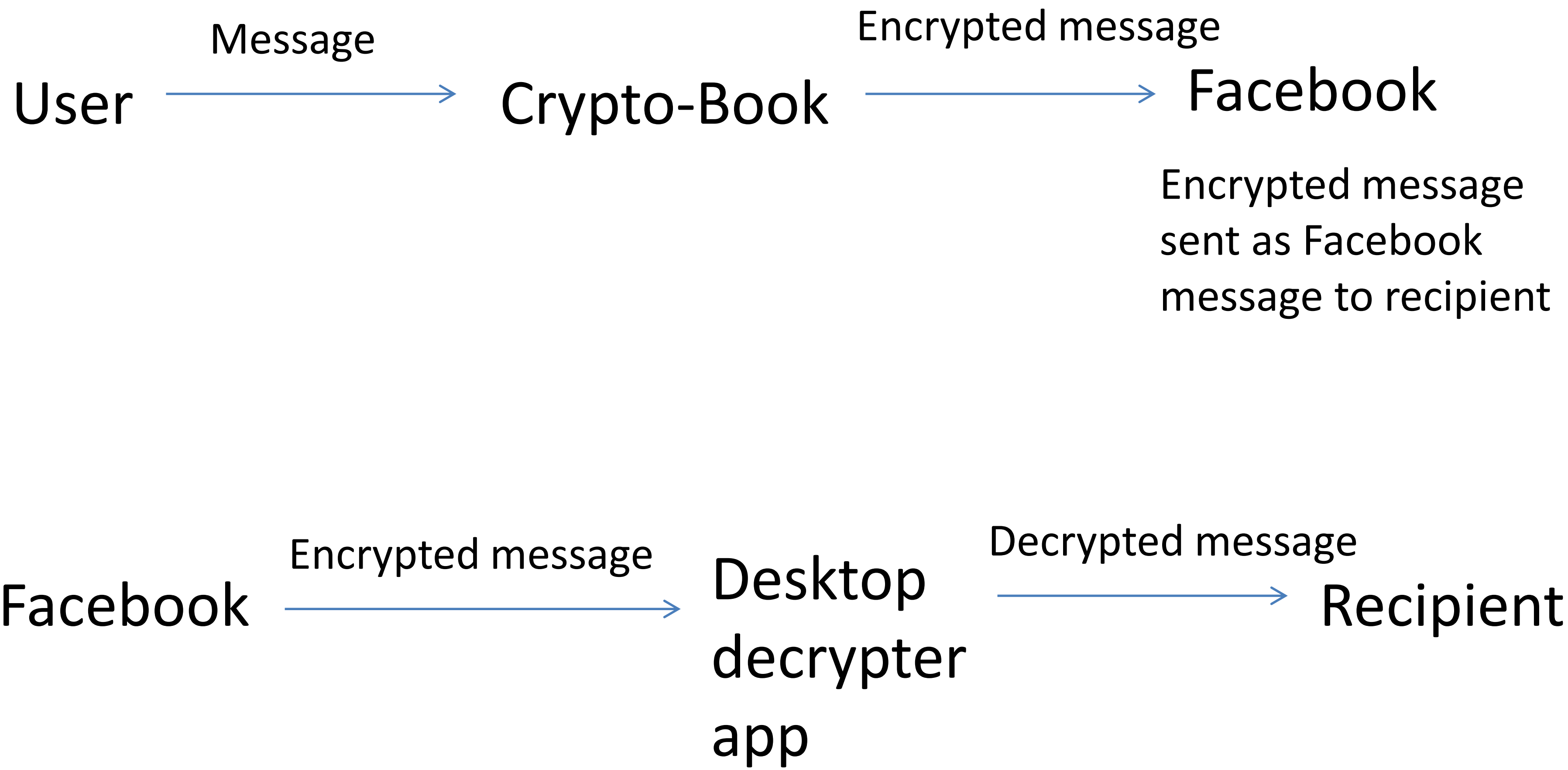
Crypto-Book

Facebook

Message

Look up recipient's profile

System overview



User

Message

Crypto-Book

Encrypted message

Facebook

Encrypted message sent as Facebook message to recipient

Facebook

Encrypted message

Desktop decrypter app

Decrypted message

Recipient

Design choices

- Key generation
  - Chose to generate server side to improve usability
  - Cannot read messages unless have access to your Facebook
  - Also have a desktop key generator
- Key publication uses URL shortener
  - Improves usability
  - Could use full form URL but more confusing

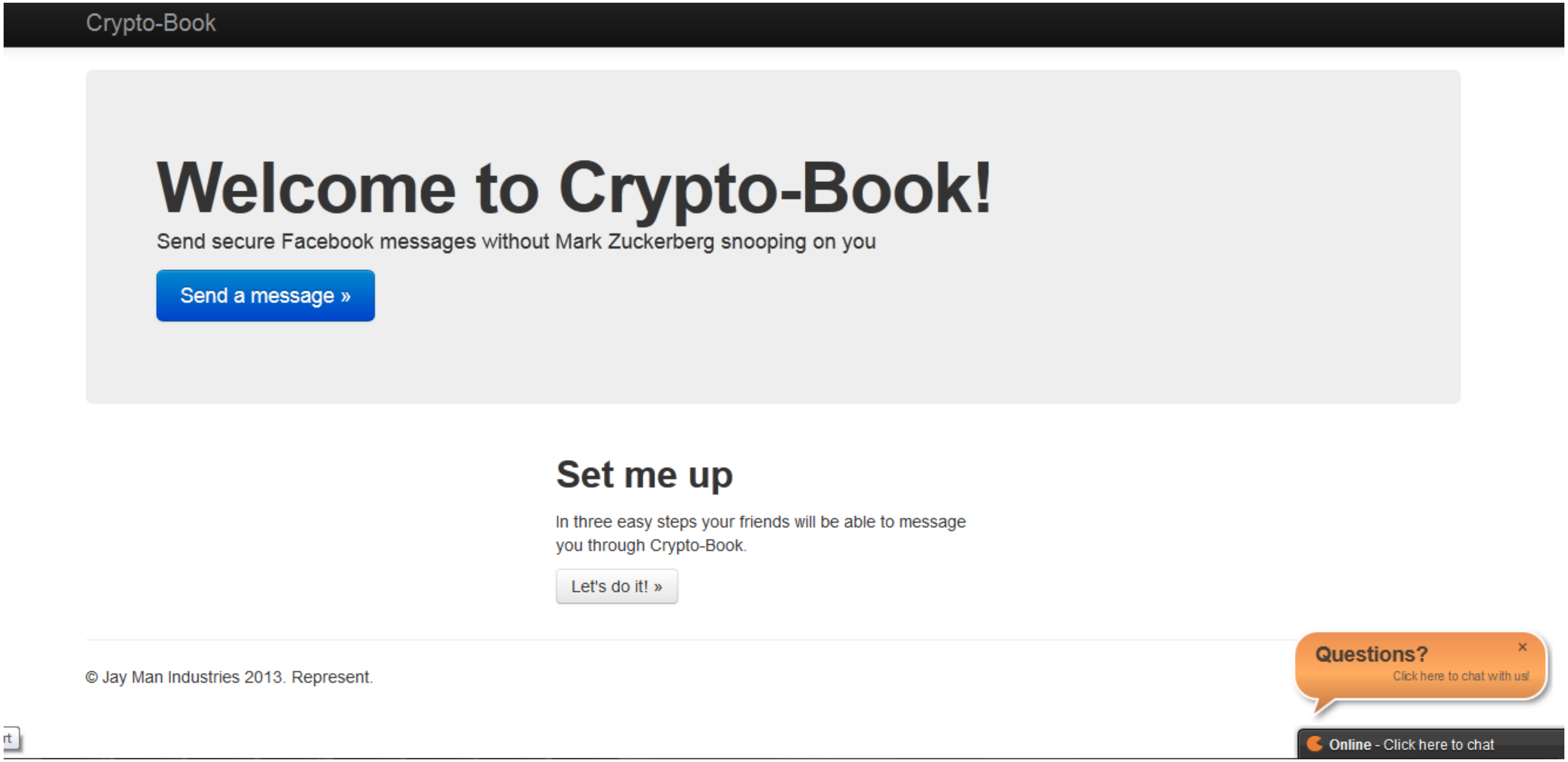
Design choices

- Sending messages
  - Trust Crypto-book as has access to plaintext
  - Nothing is stored
  - Chose this option as makes system more usable
  - Goals are:
    - avoid Facebook’s indefinite logging,
    - hide message histories from hackers and Facebook software,
    - don’t let government get access to message histories,
    - if you forget to log out of public machine others don’t have access
  - Focus on top notch usability with best effort security
    - Top notch security with best effort usability with has failed to be taken up by users

Design choices

- Sending messages
  - Originally encrypted messages offline however requires another app
  - Cannot directly message Facebook friend from desktop app, cannot post to their wall, have to post to own wall and cannot tag people, cannot log into Facebook without web browser access
- Decryption
  - Desktop app – prevents Facebook getting access to your private key
  - Decrypt on Facebook would compromise security by giving Facebook access to your encrypted messages

My solution: Crypto-Book



Crypto-Book

Welcome to Crypto-Book!

Send secure Facebook messages without Mark Zuckerberg snooping on you

Send a message »

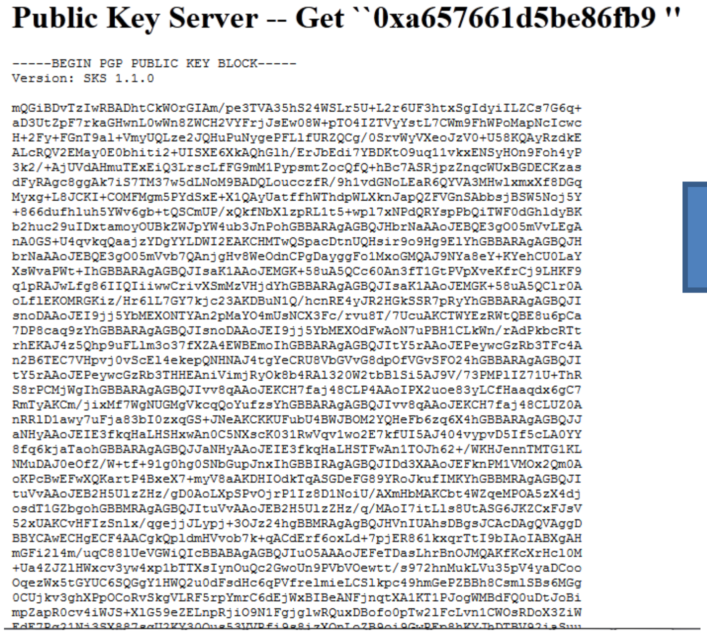
Set me up

In three easy steps your friends will be able to message you through Crypto-Book.

Let's do it! »

© Jay Man Industries 2013. Represent.

Public key



Public Key Server -- Get ``0xa657661d5be86fb9 ''

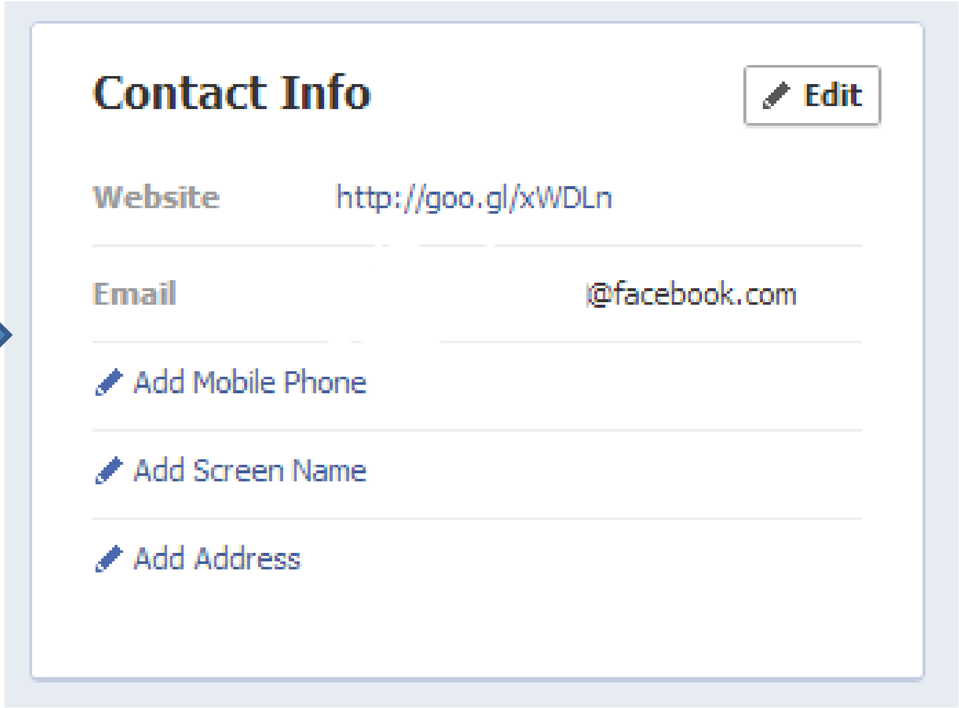
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQGiBDvTzIwRBADhtCkWOrGIAm/pe3TVA35hS24WSLr5U+L2r6UF3htxSgIdyiILZCs7G6q+
aD3UtZpF7rkaGHwnL0wWn8ZWCH2VYFrjJsEw08W+pTO4IZTVyYstL7CWm9FhWPoMapNcIcwc
H+2Fy+FGnT9al+VmyUQLze2JQHuPuNygePFLlfURZQCg/0SrvWyVXeoJzV0+U58KQAyRzdkE
ALcRQV2EMay0E0bhiti2+UISXE6XkAQhGlh/ErJbEdi7YBDKtO9uq11vkxENSyHOn9Foh4yP
3k2/+AjUVdAHmuTExEiQ3LrscLfFG9mM1PypsmtZocQfQ+hBc7ASRjpzZnqcWUxBGDECKzas
dFyRAgc8ggAk7iS7TM37w5dLNoM9BADQLoucczfR/9h1vdGNoLEaR6QYVA3MHwlxmxXf8DGq
Myxg+L8JCKI+COMFMgm5PYdSxE+X1QAyUatffhWThdpWLXknJapQZFVGnSAbbsjBSW5Noj5Y
+866dufhluh5YWv6gb+tQSCmUP/xQkfNbXlzpRL1t5+wpl7xNPdQRYspPbQiTWF0dGhldyBK
b2huc29uIDxtamoyOUBkZWJpYW4ub3JnPohGBBARAgAGBQJHbrNaAAoJEBQE3gO05mVvLEgA
nA0GS+U4qvkqQaajzYDgYYLDWI2EAKCHMTwQSpacDtnUQHsir9o9Hg9ElYhGBBARAgAGBQJH
brNaAAoJEBQE3gO05mVvb7QAnjgHv8WeOdnCPgDayggFo1MxoGMQAJ9NYa8eY+KYehCU0LaY
XsWvaPWt+IhGBBARAgAGBQJIsaK1AAoJEMGK+58uA5QCc60An3fT1GtPVpXveKfrCj9LHKF9
q1pRAJwLfg86IIQIiiwwCrivXSmMzVHjdYhGBBARAgAGBQJIsaK1AAoJEMGK+58uA5QClr0A
oLflEKOMRGKiz/Hr6lL7GY7kjc23AKDBuN1Q/hcnRE4yJR2HGkSSR7pRyYhGBBARAgAGBQJI
snoDAAoJEI9jj5YbMEXONTYAn2pMaYO4mUsNCX3Fc/rvu8T/7UcuAKCTWYEzRWtQBE8u6pCa
7DP8caq9zYhGBBARAgAGBQJIsnoDAAoJEI9jj5YbMEXOdFwAoN7uPBH1CLkWn/rAdPkbcRTt
rhEKAJ4z5Qhp9uFLlm3o37fXZA4EWBEmoIhGBBARAgAGBQJItY5rAAoJEPeywcGzRb3TFc4A
n2B6TEC7VHpvj0vScEl4ekepQNHNAJ4tgYeCRU8VbGVvG8dpOfVGvSFO24hGBBARAgAGBQJI
tY5rAAoJEPeywcGzRb3THHEAniVimjRyOk8b4RAl320W2tbBlSi5AJ9V/73PMPlIZ71U+ThR
S8rPCMjWgIhGBBARAgAGBQJIvv8qAAoJEKCH7faj48CLP4AAoIPX2uoe83yLCfHaaqdx6gC7
RmTyAKCm/jixMf7WgNUGMgVkcqQoYufzsYhGBBARAgAGBQJIvv8qAAoJEKCH7faj48CLUZ0A
nRRlD1awy7uFja83bI0zxqGS+JNeAKCKKUFubU4BWJBOM2YQHeFb6zq6X4hGBBARAgAGBQJJ
aNHyAAoJEIE3fkqHaLHSHxwAn0C5NXscK031RwVqv1wo2E7kfUI5AJ404vypvD5If5cLA0YY
8fq6kjaTaohGBBARAgAGBQJJaNHyAAoJEIE3fkqHaLHSTFwAn1TOJh62+/WKHJennTMTG1KL
NMuDAJ0eOfZ/W+tf+91g0hg0SNbGupJnxIhGBBIRAgAGBQJIDd3XAAoJEFknPM1VMOx2Qm0A
oKPcBwEFwXQKartP4BxeX7+myV8aAKDHIOdkTqASGDeFG89YRoJkufIMKYhGBBMRAgAGBQJI
tuVvAAoJEB2H5UlzZHz/gD0AoLXpSPvOjrP1Iz8D1NoiU/AXmHbMAKCbt4WZqeMPOA5zX4dj
osdT1GZbgohGBBMRAgAGBQJItuVvAAoJEB2H5UlzZHz/q/MAoI7itLls8UtASG6JKZCxFJsV
52xUAKCvHFIzSnlx/qgejjJLypj+3OJz24hgBBMRAgAgBQJHVnIUAhsDBgsJCAcDAgQVAggD
BBYCAwECHgECF4AACgkQpldmHVvob7k+qACdErf6oxLd+7pjER861kxqrTtI9bIAoIABXgAH
mGFi2l4m/uqC88lUeVGWiQIcBBABAgAGBQJIuO5AAAoJEFeTDasLhrBnOJMQAKfKcXrHcl0M
+Ua4ZJZlHWxcv3yw4xp1bTTXsIynOuQc2GwoUn9PVbVOewtt/s972hnMukLVu35pV4yaDCoo
OqezWx5tGYUC6SQGgY1HWQ2u0dFsdHc6qPVfrelmieLCSlkpc49hmGePZBBh8CsmlSBs6MGg
0CUjkv3ghXPpOCoRvSkgVLRF5rpYmrC6dEjWxBIBeANFjnqtXA1KT1PJogWMBdFQ0uDtJoBi
mpZapR0cv4iWJS+XlG59eZELnpRjiO9N1FgjglwRQuxDBofo0pTw2lFcLvn1CWOsRDoX3ZiW
EdF7Rg21Nj3SY887sgU2KY30Ous53VVRfi9s8jzYOnLoZB9oi9GwREp8hKYJhDTBV92iaSuu
```

http://www.crypto-book.com/key?val=48,-127,-97,48,13,6,9,42,-122,72,-1
22,-9,13,1,1,1,5,0,3,-127,-115,0,48,-127,-119,2,-127,-127,0,-122,-15,-85,-103,-33,-112,-107,-36,-126,-110,96,-124,81,-30,-54,74,9,59,4,-52,-5,63,-81,54,-40,-35,123,15,94,-23,14,-94,112,-98,98,91,-89,23,-110,41,-78,-49,-44,122

http://goo.gl/b46v7

Publishing your key on Facebook

http://goo.gl/b46v7



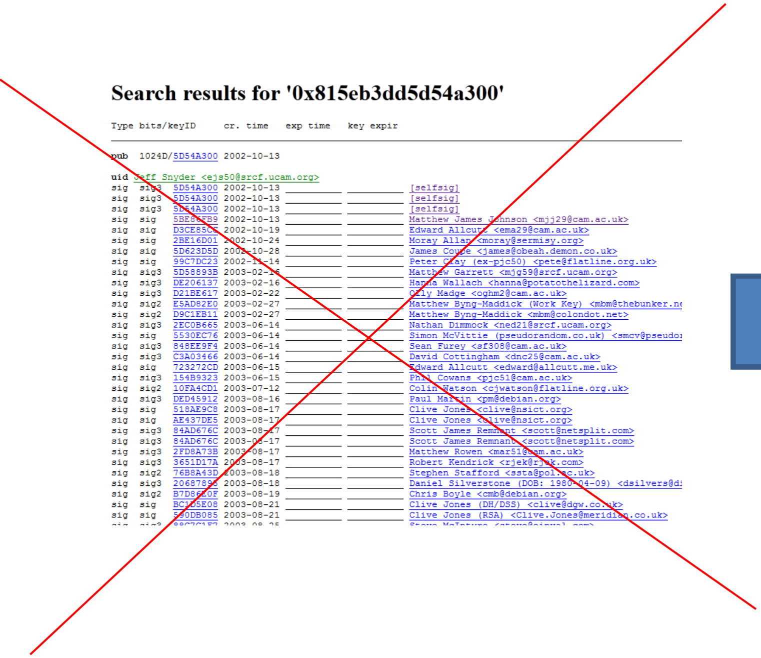
Contact Info

Website	http://goo.gl/xWDLn
Email	@facebook.com

Using a key

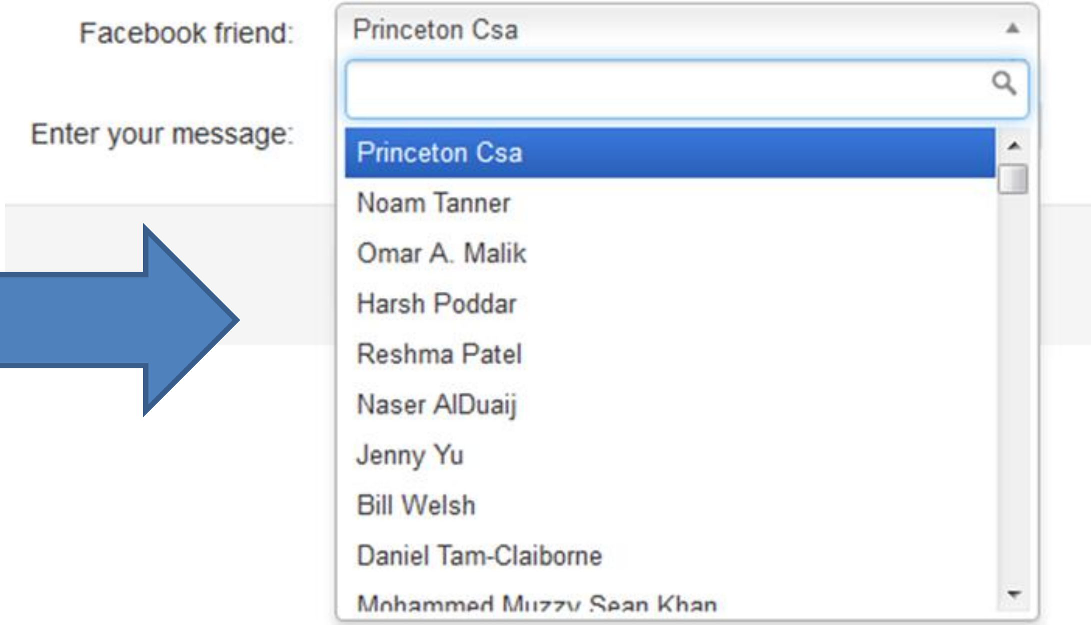
- Fully integrated with Facebook
- Send a message through crypto-book.com
- Log in with Facebook
- Choose friend to send to
  - Automatically looks up key
- Enter message
  - Encrypt with friend’s public key and sent through Facebook

Key lookup



Search results for '0x815eb3dd5d54a300'

```
Type bits/keyID     cr. time   exp time   key expir
----------------------------------------------------------------------
pub  1024D/5D54A300 2002-10-13

uid  Jeff Snyder <ejs50@srcf.ucam.org>
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig3  5D54A300 2002-10-13 __________ __________ [selfsig]
sig  sig   5BE86FB9 2002-10-13 __________ __________ Matthew James Johnson <mjj29@cam.ac.uk>
sig  sig   D3CE85C6 2002-10-19 __________ __________ Edward Allcutt <ema29@cam.ac.uk>
sig  sig   2BE16D01 2002-10-24 __________ __________ Moray Allan <moray@sermisy.org>
sig  sig   5D623D5D 2002-10-28 __________ __________ James Coupe <james@obeah.demon.co.uk>
sig  sig   99C7DC23 2002-11-14 __________ __________ Peter Clay (ex-pjc50) <pete@flatline.org.uk>
sig  sig3  5D58893B 2003-02-16 __________ __________ Matthew Garrett <mjg59@srcf.ucam.org>
sig  sig3  DE206137 2003-02-16 __________ __________ Hanna Wallach <hanna@potatothelizard.com>
sig  sig3  D21BE617 2003-02-22 __________ __________ Olly Madge <oghm2@cam.ac.uk>
sig  sig2  E5AD82E0 2003-02-27 __________ __________ Matthew Byng-Maddick (Work Key) <mbm@thebunker.ne
sig  sig2  D9C1EB11 2003-02-27 __________ __________ Matthew Byng-Maddick <mbm@colondot.net>
sig  sig3  2EC0B665 2003-06-14 __________ __________ Nathan Dimmock <ned21@srcf.ucam.org>
sig  sig   5530EC76 2003-06-14 __________ __________ Simon McVittie (pseudorandom.co.uk) <smcv@pseudo
sig  sig3  848EE9F4 2003-06-14 __________ __________ Sean Furey <sf308@cam.ac.uk>
sig  sig3  C3A03466 2003-06-14 __________ __________ David Cottingham <dnc25@cam.ac.uk>
sig  sig   723272CD 2003-06-15 __________ __________ Edward Allcutt <edward@allcutt.me.uk>
sig  sig3  154B9323 2003-06-15 __________ __________ Phil Cowans <pjc51@cam.ac.uk>
sig  sig2  10FA4CD1 2003-07-12 __________ __________ Colin Watson <cjwatson@flatline.org.uk>
sig  sig3  DED45912 2003-08-16 __________ __________ Paul Martin <pm@debian.org>
sig  sig   518AE9C8 2003-08-17 __________ __________ Clive Jones <clive@nsict.org>
sig  sig   AE437DE5 2003-08-17 __________ __________ Clive Jones <clive@nsict.org>
sig  sig3  84AD676C 2003-08-17 __________ __________ Scott James Remnant <scott@netsplit.com>
sig  sig3  84AD676C 2003-08-17 __________ __________ Scott James Remnant <scott@netsplit.com>
sig  sig3  2FD8A73B 2003-08-17 __________ __________ Matthew Rowen <mar51@cam.ac.uk>
sig  sig3  3651D17A 2003-08-17 __________ __________ Robert Kendrick <rjek@rjek.com>
sig  sig2  76B8A43D 2003-08-18 __________ __________ Stephen Stafford <ssta@pol.ac.uk>
sig  sig3  20687896 2003-08-18 __________ __________ Daniel Silverstone (DOB: 1980-04-09) <dsilvers@di
sig  sig2  B7D86E0F 2003-08-19 __________ __________ Chris Boyle <cmb@debian.org>
sig  sig   BC1D5E08 2003-08-21 __________ __________ Clive Jones (DH/DSS) <clive@dgw.co.uk>
sig  sig   590DB085 2003-08-21 __________ __________ Clive Jones (RSA) <Clive.Jones@meridian.co.uk>
```

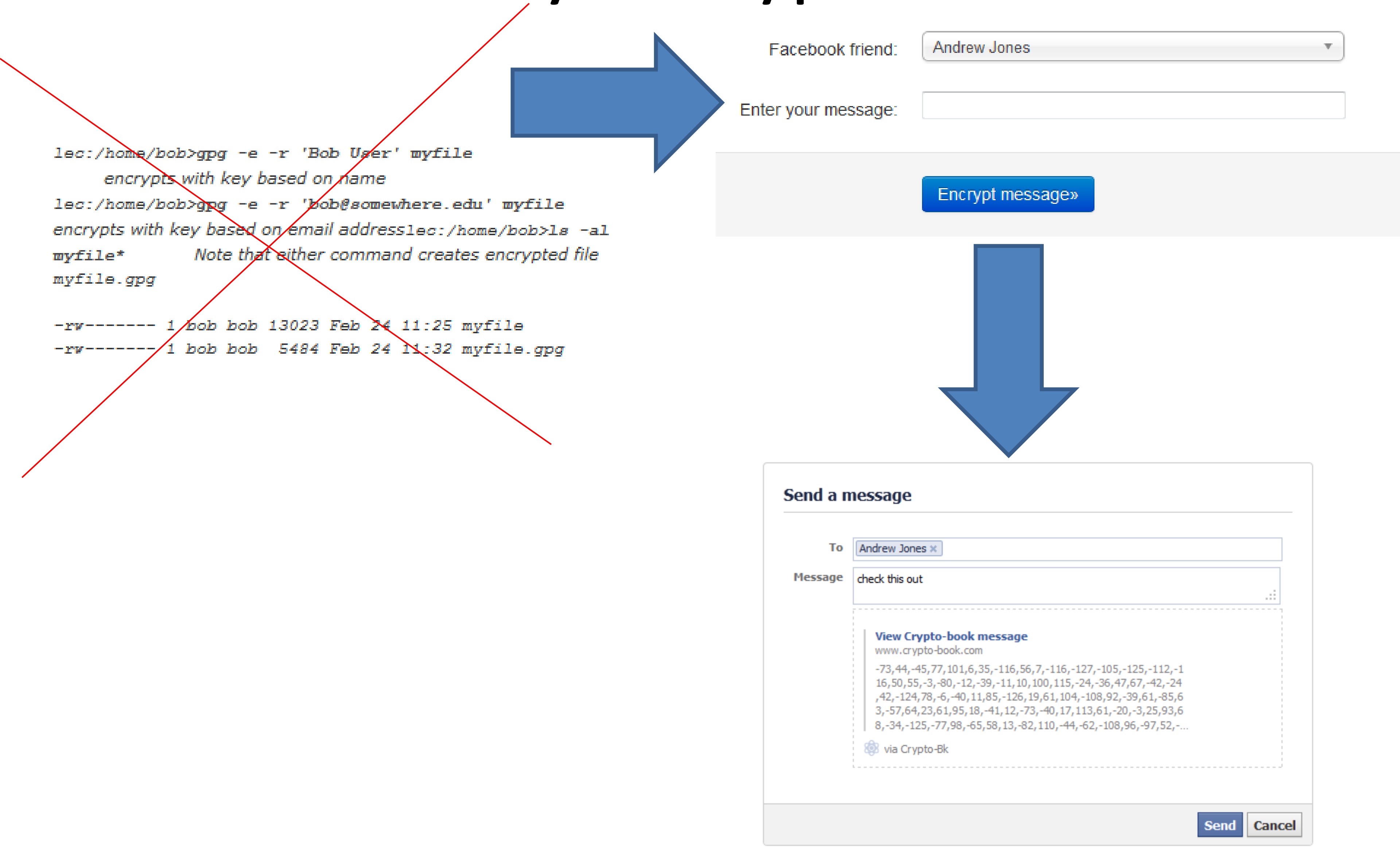


Facebook friend: Princeton Csa

Enter your message:

- Princeton Csa
- Noam Tanner
- Omar A. Malik
- Harsh Poddar
- Reshma Patel
- Naser AlDuaij
- Jenny Yu
- Bill Welsh
- Daniel Tam-Claiborne
- Mohammed Muzzy Sean Khan

Easy encryption



```
lec:/home/bob>gpg -e -r 'Bob User' myfile
     encrypts with key based on name
lec:/home/bob>gpg -e -r 'bob@somewhere.edu' myfile
encrypts with key based on email addresslec:/home/bob>ls -al
myfile*       Note that either command creates encrypted file
myfile.gpg

-rw-------- 1 bob bob 13023 Feb 24 11:25 myfile
-rw-------- 1 bob bob  5484 Feb 24 11:32 myfile.gpg
```

Facebook friend: Andrew Jones

Enter your message:

Send a message

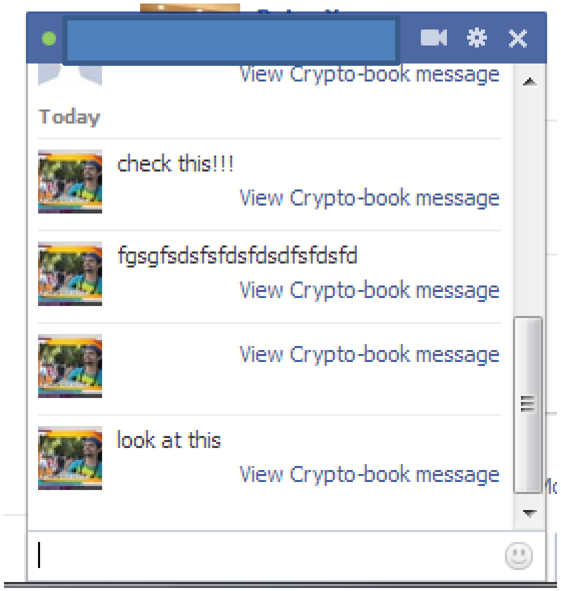
To: Andrew Jones

Message: check this out

View Crypto-book message
www.crypto-book.com
-73,44,-45,77,101,6,35,-116,56,7,-116,-127,-105,-125,-112,-1
16,50,55,-3,-80,-12,-39,-11,10,100,115,-24,-36,47,67,-42,-24
,42,-124,78,-6,-40,11,85,-126,19,61,104,-108,92,-39,61,-85,6
3,-57,64,23,61,95,18,-41,12,-73,-40,17,113,61,-20,-3,25,93,6
8,-34,-125,-77,98,-65,58,13,-82,110,-44,-62,-108,96,-97,52,-...

via Crypto-Bk

Easy decryption



[redacted]

View Crypto-book message

Today

check this!!!
View Crypto-book message

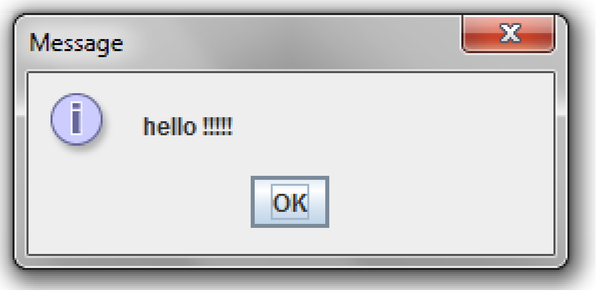
fgsgfsdsfsfdsfdsdfsfdsfd
View Crypto-book message

View Crypto-book message

look at this
View Crypto-book message

Click to view message

Message displayed to user



Message

hello !!!!!

Areas for future work

- Make it easier to deploy on Mac/Linux
- Further testing on different environments
- Signing as well as encryption
- Use identity based encryption
  - Have to trust IBE servers, anytrust model
  - Facebook have access to your private key
- Anonymity through linkable ring signatures

www.crypto-book.com

Demonstrate the app