Michael Christensen
October 28, 2013
CS 465

Project 6 (PGP and S/MIME)

Email Platforms and Tools Used:

For PGP I used Gmail with the Chrome extension Mailvelope, which was relatively simple to use (compared to S/MIME tools) because the extension itself can generate public/private key pairs as well as easily import your friends' public keys into the key ring. To encrypt a message, you use Gmail's message editor to create the message and then click on the extension's lock button to encrypt the message using each recipient's imported public keys. When a message signed by another person arrives, the extension can easily decrypt the messages when I enter in the pass-phrase securing my private key. For S/MIME, I retrieved a free certificate from StartCom Ltd and imported this certificate (a .p12) into Thunderbird. With that, I could sign a message to my peer so that he would have my certificate and be able to encrypt messages to me (and using the reverse process, vice versa).

Difference between PGP and S/MIME:

PGP (Pretty Good Privacy) is a model of trust used to digitally sign and encrypt Internet communication like email via a web of trust. Two parties each generate public/private key pairs and exchange the public keys (a la RSA) , which is where this trust comes into play. There are no certificates involved in this exchange, so I must have confidence that the key given to me from the other person is what it was originally when it was created by my friend, and that my friend really gave it to me (rather than it being the product of some attacker/man-in-the-middle). Then to send a message, if a signature is desired, Party A uses his private key to sign the message, and if encryption is desired, uses Party B's public key to encrypt it. Party B then uses her private key to decrypt the message and uses Party A's public key to verify the signature (since only A knows A's private key, supposedly).

S/MIME (Secure Multipurpose Internet Mail Extension) on the other hand relies on a hierarchal, top-down model of certificate authorities instead of a web of trust between parties like PGP. Both parties obtain and install a certificate from a certificate authority, which allow them to bind their public key to their identifying information and allow others to confirm this binding when receiving their messages.

Parts of the process that were difficult to use/understand:

The two most difficult parts of the process were figuring out how S/MIME works exactly (since the Internet does a poor job explaining it anywhere) and figuring out how to properly create, import, and verify digital certificates into my mail client (Thunderbird). I had one error where the email client wouldn't let me send the message I was attempting to sign because it (the mail client) couldn't verify the certificate I had imported, despite the same process working flawlessly on my companion's mail client. I solved the problem by disabling the verification temporarily because I was positive the certificate I was using (mine) was authentic since I had just generated it straight from the CA. I did, however, verify my companion's certificate to be sure it was authentic.

Past experience with secure email and prospect for continued use of secure email technology in the future:

I have no past experience with secure email, the reason being that I had 1. never heard of the idea of securing email (naively thinking that web mail clients like Gmail were secure enough) and 2. never had need to secure any my communication (or didn't realize the need to). I also don't intend to use this in the future because of the hassle it was to set up anything with the recipients of my messages, especially encrypting messages via S/MIME, which was the most confusing method. I may consider using secure mail if Gmail integrates the Mailvelope extension's functionality directly into the client so

that more people are exposed to it, but then that might involve trusting Gmail itself as a third party, which is something we're trying to avoid.

Who I worked with and the ease/difficulty of preparation for exchange:

I worked with Mike Curtis for this project to exchange our emails in PGP and S/MIME. It was fairly easy to prepare using the Mailvelope since both of us regularly use Chrome and Gmail. S/MIME, on other hand, presented difficulties because we approached obtaining certificates differently (some websites make it easier and more obvious than others), but we eventually found it was easiest if we agreed on the same website we found was easiest and the same mail client (Thunderbird) so we could help each other with the set-up.

Screen-shots attached in the following pages (*which according to the directions do not count toward the 2 page limit*).

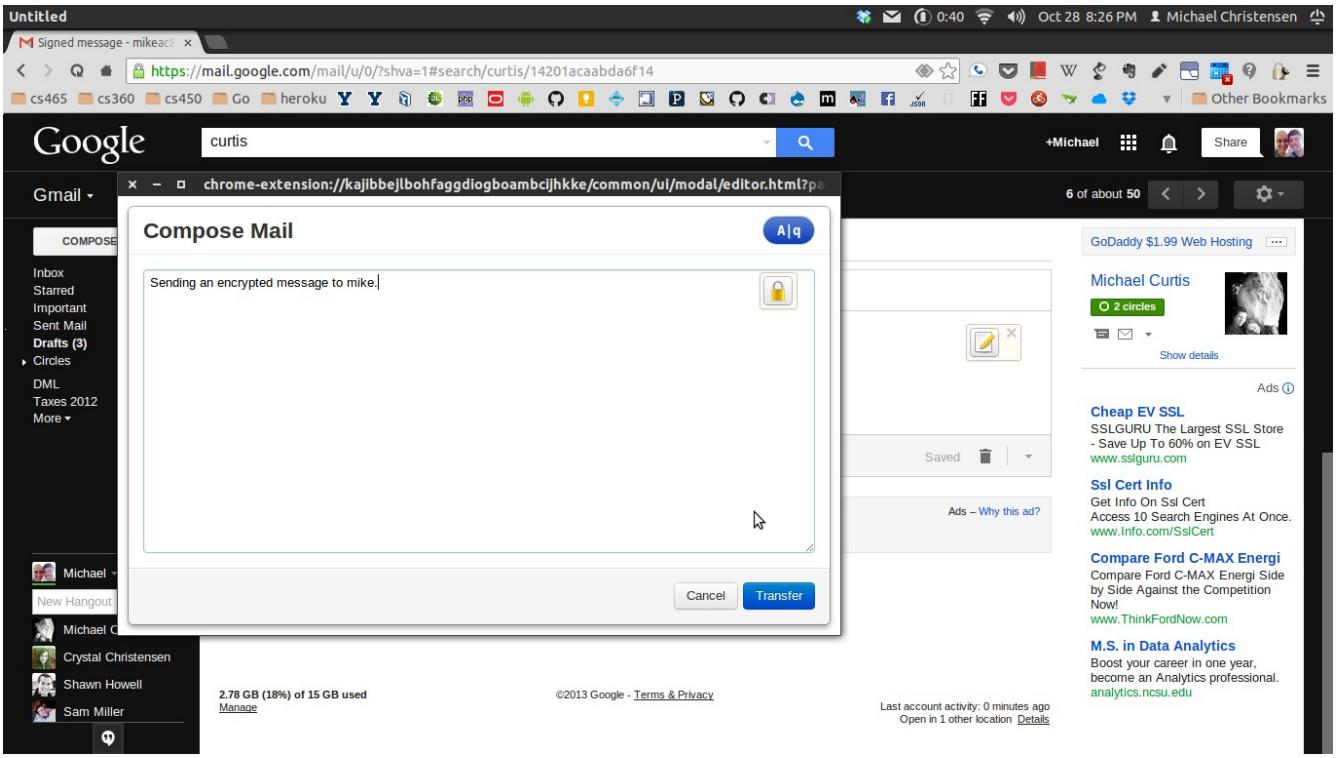
Self-Grading:

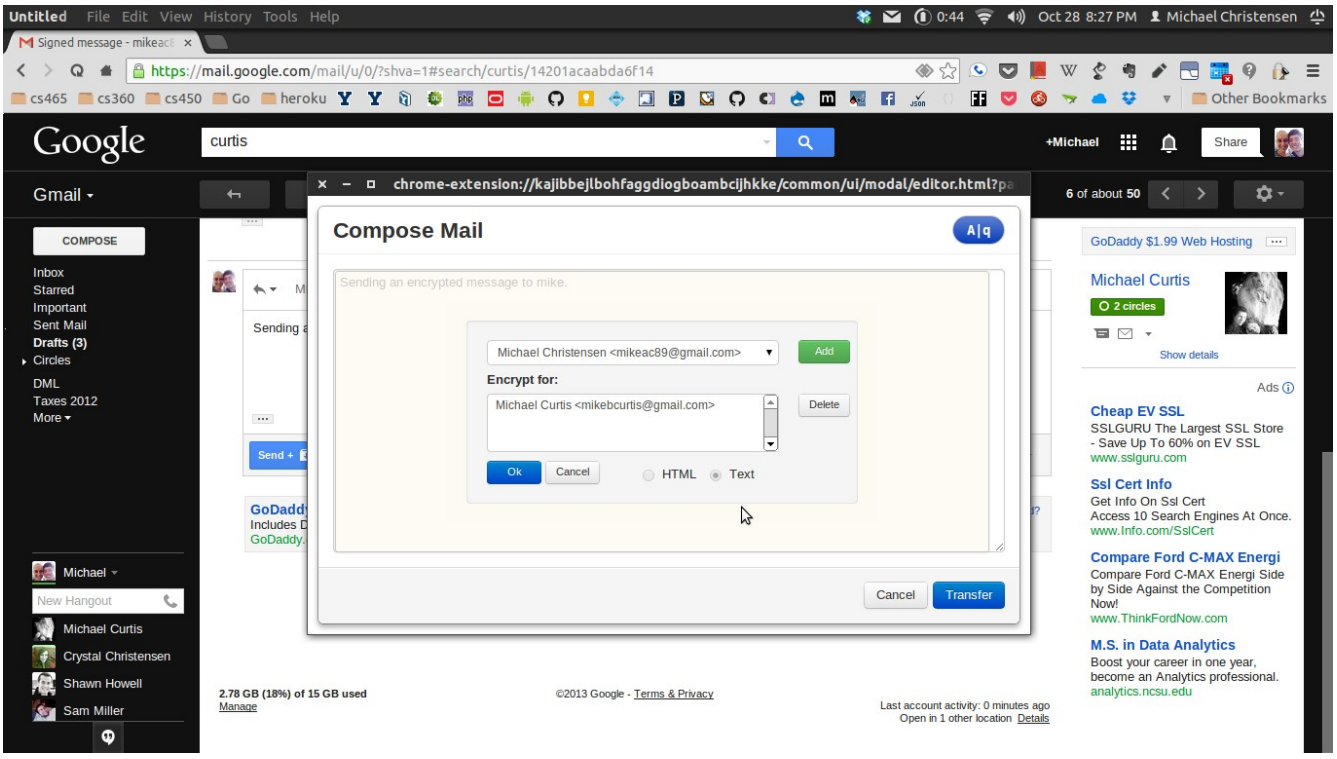
Well written report within the length guidelines – 20/20 pts
Successfully exchanged both PGP and S/MIME messages – 20/20 pts
Successfully exchanged email with a fellow student – 10/10 pts
Total: 50/50

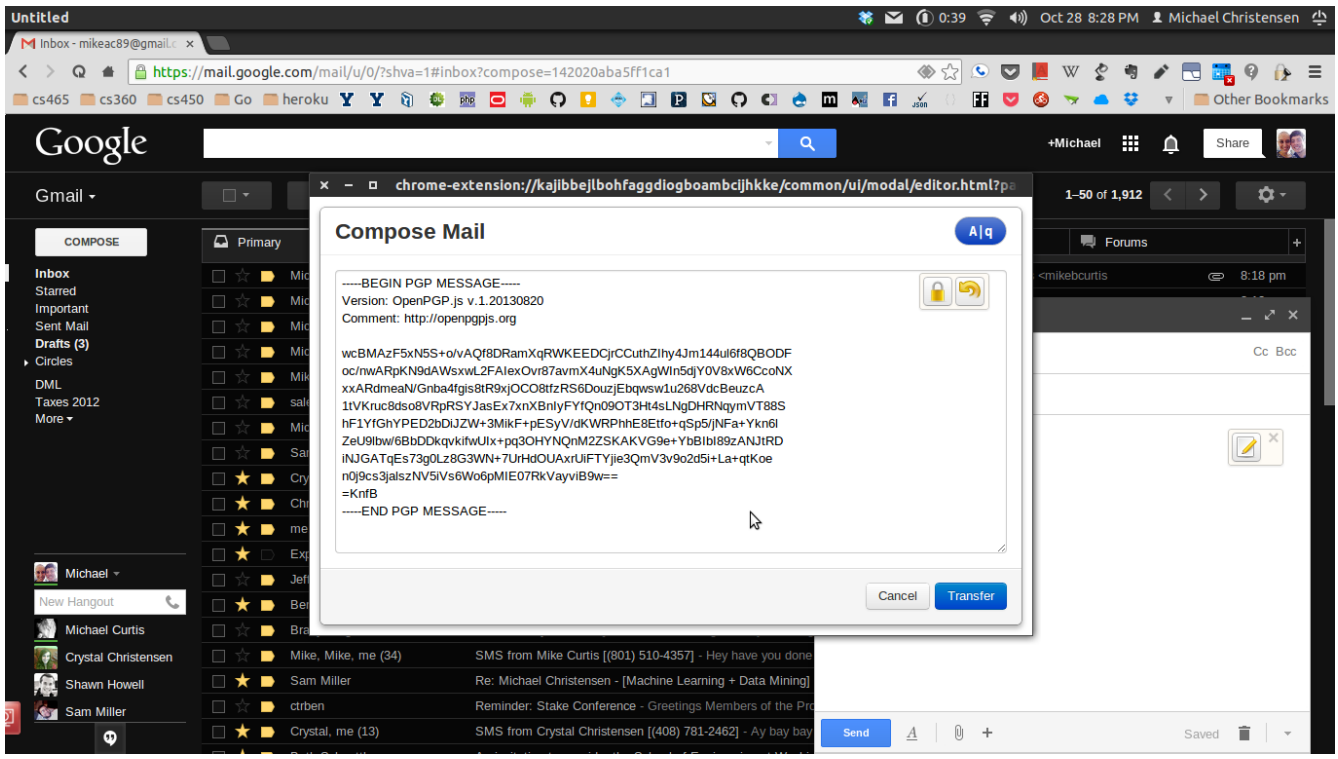
Screenshots of the process (evidence we did it):

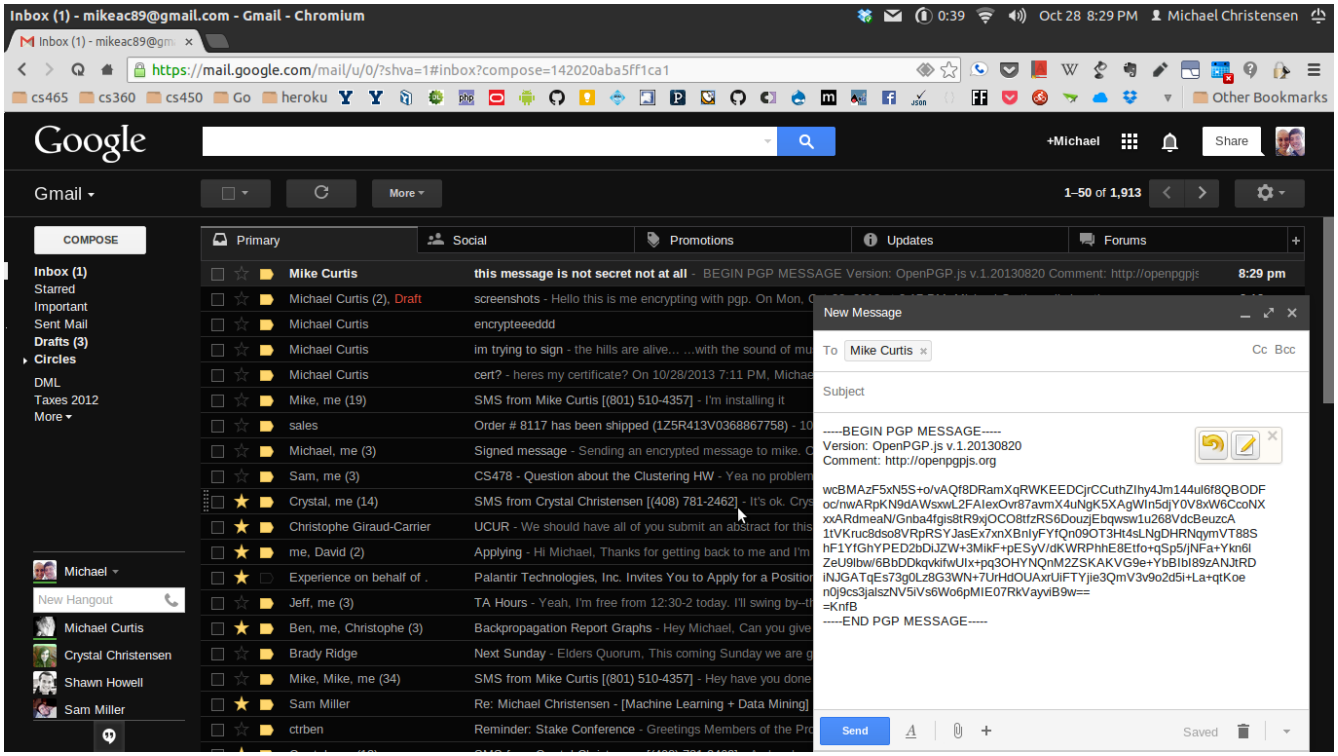
PGP:

Me Sending to Mike Curtis:

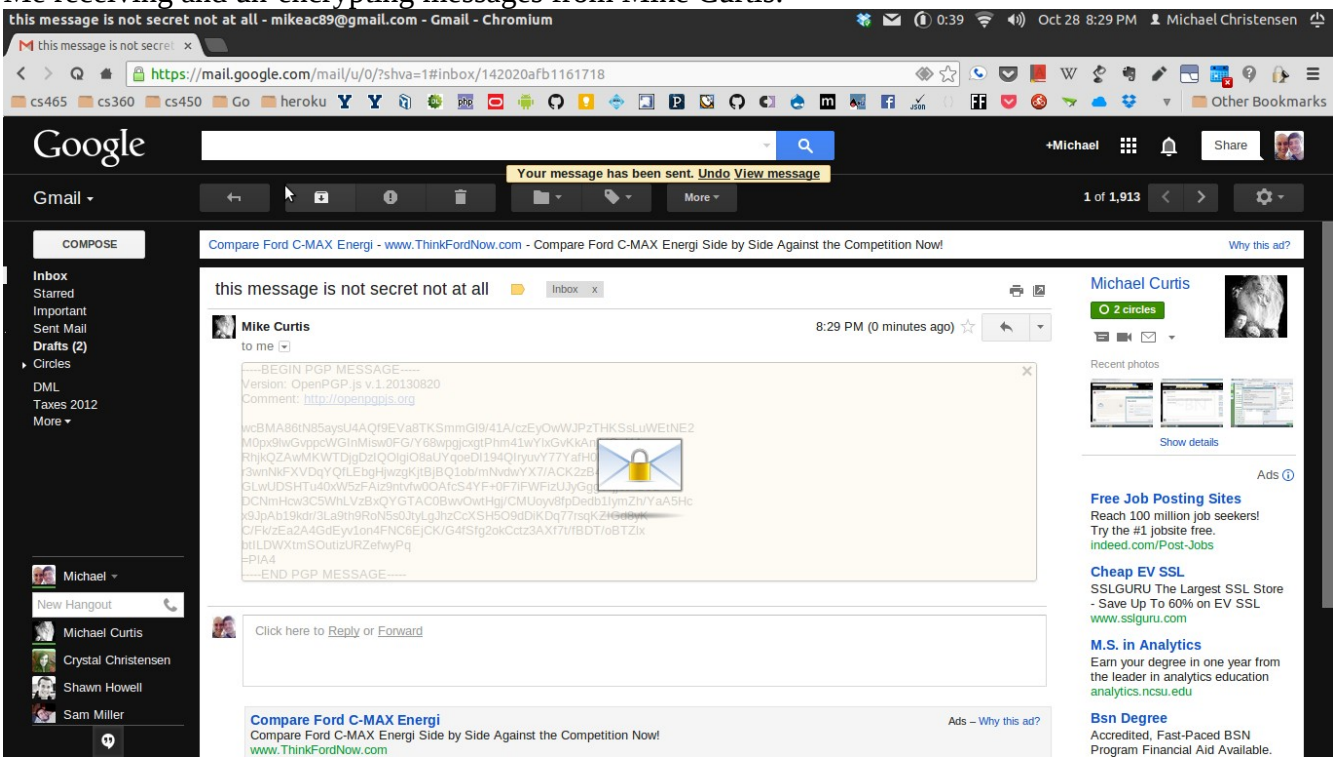


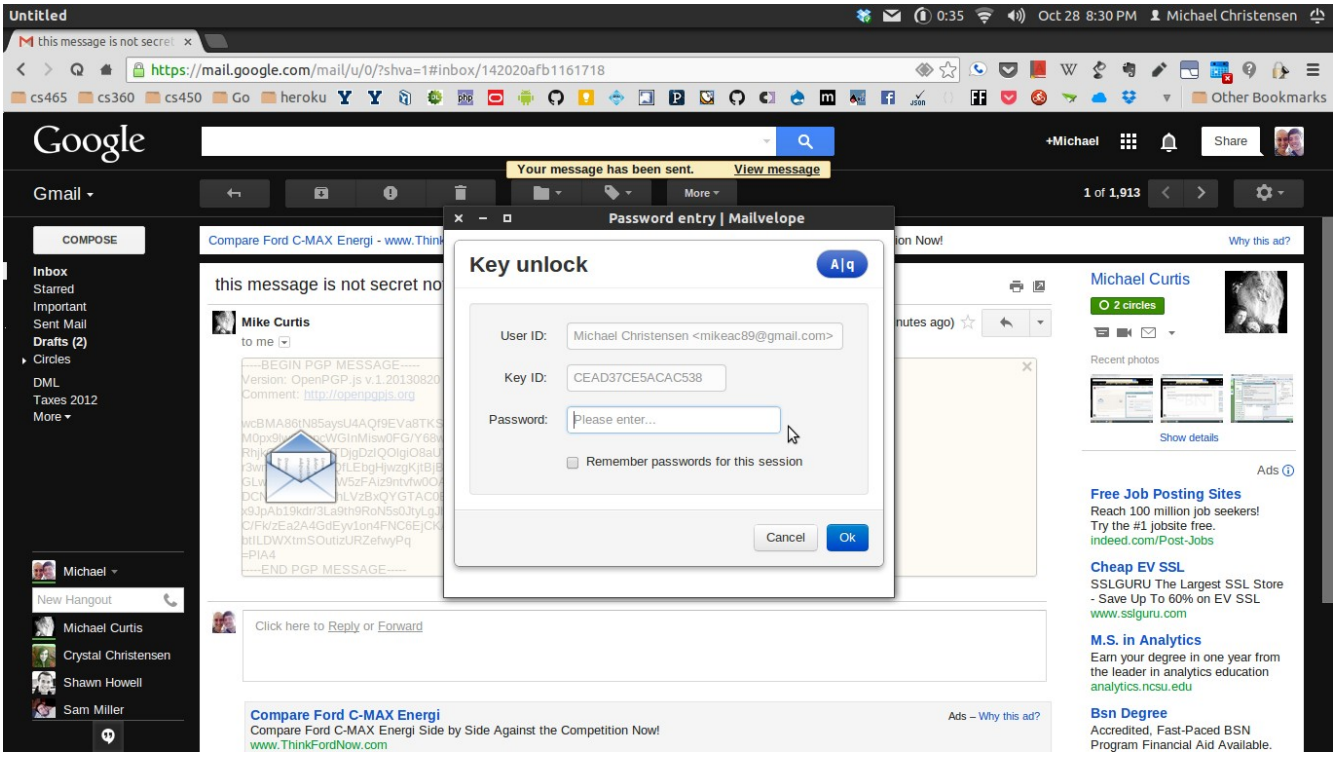


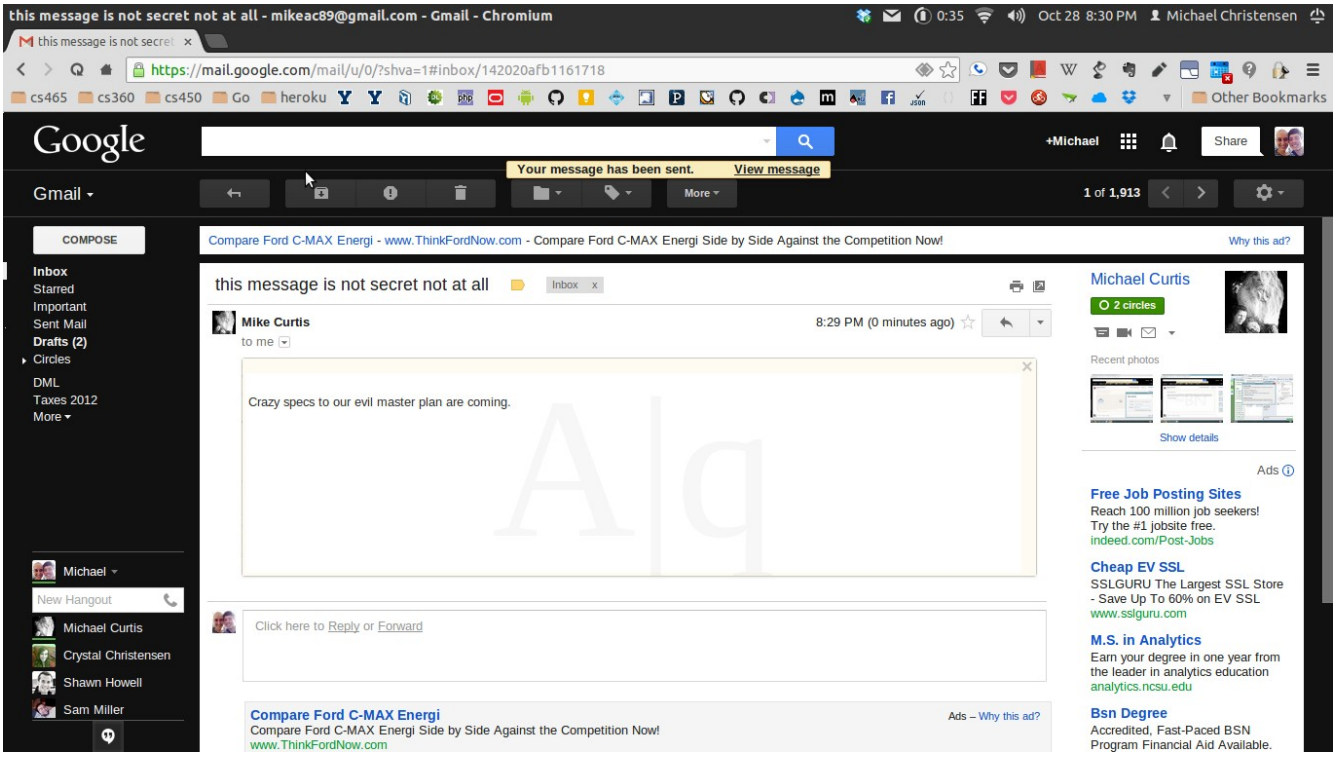

Untitled
Oct 28 8:28 PM
Michael Christensen
Inbox - mikeac89@gmail.c
https://mail.google.com/mail/u/0/?shva=1#inbox?compose=142020aba5ff1ca1
Other Bookmarks
Google
+Michael
Share
Gmail
chrome-extension://kajibbejlbohfaggdiogboambcijhkke/common/ui/modal/editor.html?p
1–50 of 1,912
Compose Mail
COMPOSE
Inbox
Starred
Important
Sent Mail
Drafts (3)
Circles
DML
Taxes 2012
More
Primary
Forums
-----BEGIN PGP MESSAGE-----
Version: OpenPGP.js v.1.20130820
Comment: http://openpgpjs.org
wcBMAzF5xN5S+o/vAQf8DRamXqRWKEEDCjrCCuthZIhy4Jm144ul6f8QBODF
oc/nwARpKN9dAWsxwL2FAIexOvr87avmX4uNgK5XAgWIn5djY0V8xW6CcoNX
xxARdmeaN/Gnba4fgis8tR9xjOCO8tfzRS6DouzjEbqwsw1u268VdcBeuzcA
1tVKruc8dso8VRpRSYJasEx7xnXBnlyFYfQn09OT3Ht4sLNgDHRNqymVT88S
hF1YfGhYPED2bDiJZW+3MikF+pESyV/dKWRPhhE8Etfo+qSp5/jNFa+Ykn6l
ZeU9lbw/6BbDDkqvkifwUIx+pq3OHYNQnM2ZSKAKVG9e+YbBIbl89zANJtRD
iNJGATqEs73g0Lz8G3WN+7UrHdOUAxrUiFTYjie3QmV3v9o2d5i+La+qtKoe
n0j9cs3jalszNV5iVs6Wo6pMIE07RkVayviB9w==
=KnfB
-----END PGP MESSAGE-----
Cancel
Transfer
Michael
New Hangout
Michael Curtis
Crystal Christensen
Shawn Howell
Sam Miller
Mike, Mike, me (34)
SMS from Mike Curtis [(801) 510-4357] - Hey have you done
Sam Miller
Re: Michael Christensen - [Machine Learning + Data Mining]
ctrben
Reminder: Stake Conference - Greetings Members of the Pro
Crystal, me (13)
SMS from Crystal Christensen [(408) 781-2462] - Ay bay bay
Cc Bcc
Send
Saved


Inbox (1) - mikeac89@gmail.com - Gmail - Chromium
Oct 28 8:29 PM
Michael Christensen
https://mail.google.com/mail/u/0/?shva=1#inbox?compose=142020aba5ff1ca1
Other Bookmarks
Google
+Michael
Share
Gmail
More
1–50 of 1,913
COMPOSE
Inbox (1)
Starred
Important
Sent Mail
Drafts (3)
Circles
DML
Taxes 2012
More
Primary
Social
Promotions
Updates
Forums
Mike Curtis
this message is not secret not at all - BEGIN PGP MESSAGE Version: OpenPGP.js v.1.20130820 Comment: http://openpgpjs
8:29 pm
Michael Curtis (2), Draft
screenshots - Hello this is me encrypting with pgp. On Mon,
Michael Curtis
encrypteeeddd
Michael Curtis
im trying to sign - the hills are alive,... ...with the sound of mu
Michael Curtis
cert? - heres my certificate? On 10/28/2013 7:11 PM, Michae
Mike, me (19)
SMS from Mike Curtis [(801) 510-4357] - I'm installing it
sales
Order # 8117 has been shipped (1Z5R413V0368867758) - 10
Michael, me (3)
Signed message - Sending an encrypted message to mike.
Sam, me (3)
CS478 - Question about the Clustering HW - Yea no problem
Crystal, me (14)
SMS from Crystal Christensen [(408) 781-2462] - It's ok. Crys
Christophe Giraud-Carrier
UCUR - We should have all of you submit an abstract for this
me, David (2)
Applying - Hi Michael, Thanks for getting back to me and I'm
Experience on behalf of .
Palantir Technologies, Inc. Invites You to Apply for a Positio
Jeff, me (3)
TA Hours - Yeah, I'm free from 12:30-2 today. I'll swing by--t
Ben, me, Christophe (3)
Backpropagation Report Graphs - Hey Michael, Can you give
Brady Ridge
Next Sunday - Elders Quorum. This coming Sunday we are g
Mike, Mike, me (34)
SMS from Mike Curtis [(801) 510-4357] - Hey have you done
Sam Miller
Re: Michael Christensen - [Machine Learning + Data Mining]
ctrben
Reminder: Stake Conference - Greetings Members of the Pro
New Message
To
Mike Curtis
Cc Bcc
Subject
-----BEGIN PGP MESSAGE-----
Version: OpenPGP.js v.1.20130820
Comment: http://openpgpjs.org
wcBMAzF5xN5S+o/vAQf8DRamXqRWKEEDCjrCCuthZIhy4Jm144ul6f8QBODF
oc/nwARpKN9dAWsxwL2FAIexOvr87avmX4uNgK5XAgWIn5djY0V8xW6CcoNX
xxARdmeaN/Gnba4fgis8tR9xjOCO8tfzRS6DouzjEbqwsw1u268VdcBeuzcA
1tVKruc8dso8VRpRSYJasEx7xnXBnlyFYfQn09OT3Ht4sLNgDHRNqymVT88S
hF1YfGhYPED2bDiJZW+3MikF+pESyV/dKWRPhhE8Etfo+qSp5/jNFa+Ykn6l
ZeU9lbw/6BbDDkqvkifwUIx+pq3OHYNQnM2ZSKAKVG9e+YbBIbl89zANJtRD
iNJGATqEs73g0Lz8G3WN+7UrHdOUAxrUiFTYjie3QmV3v9o2d5i+La+qtKoe
n0j9cs3jalszNV5iVs6Wo6pMIE07RkVayviB9w==
=KnfB
-----END PGP MESSAGE-----
Send
Saved
Michael
New Hangout
Michael Curtis
Crystal Christensen
Shawn Howell
Sam Miller

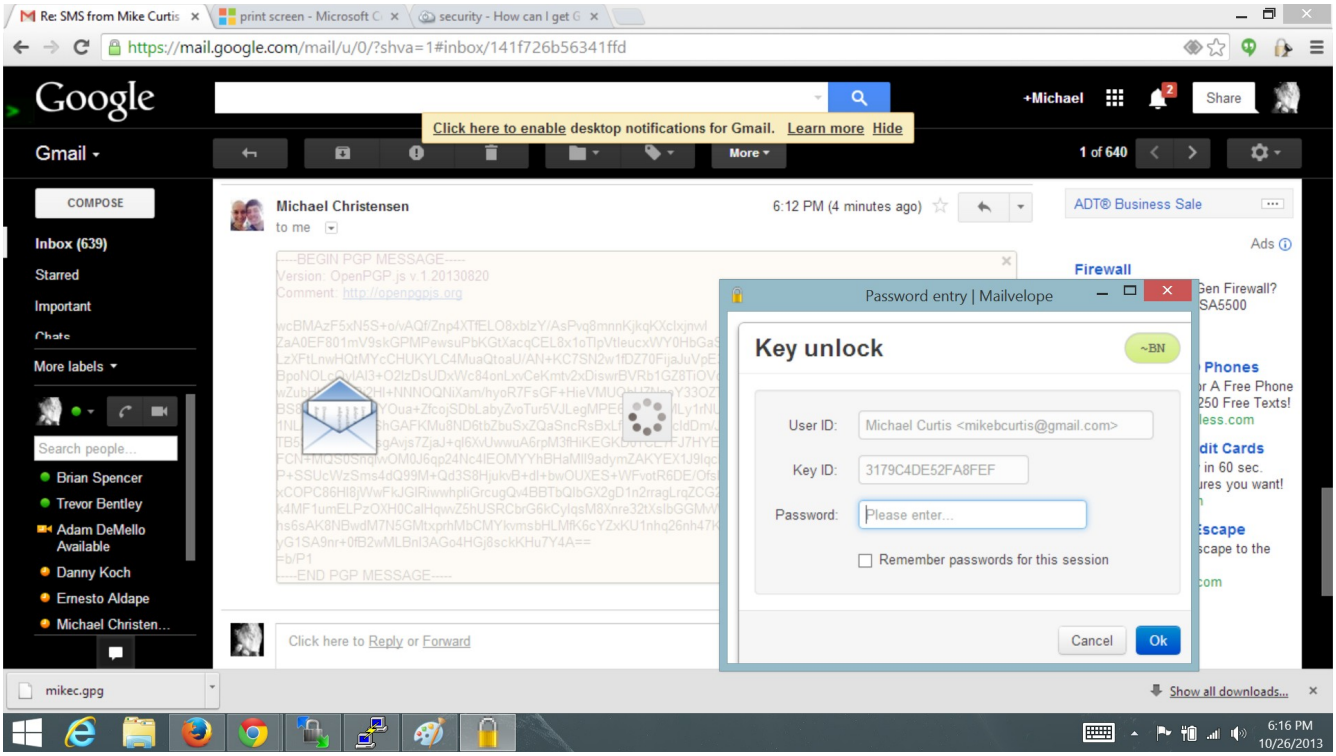
Me receiving and un-encrypting messages from Mike Curtis:

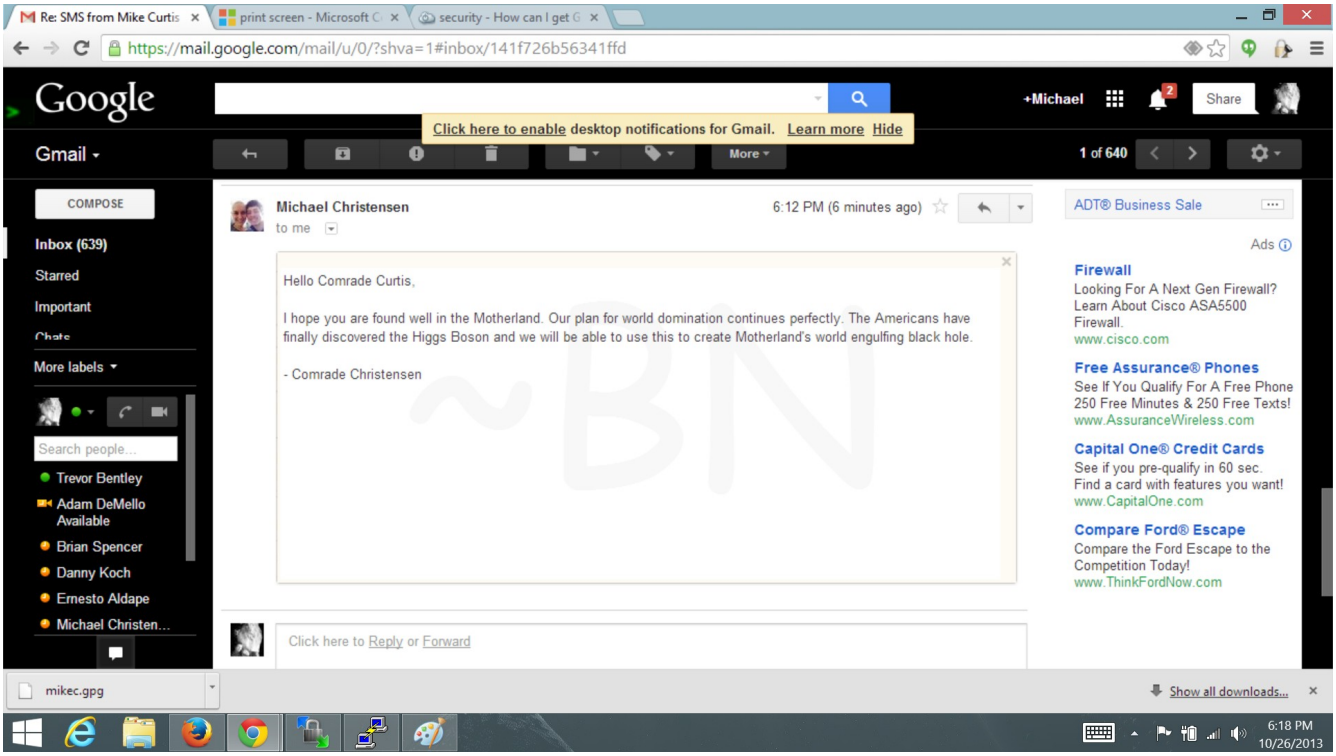






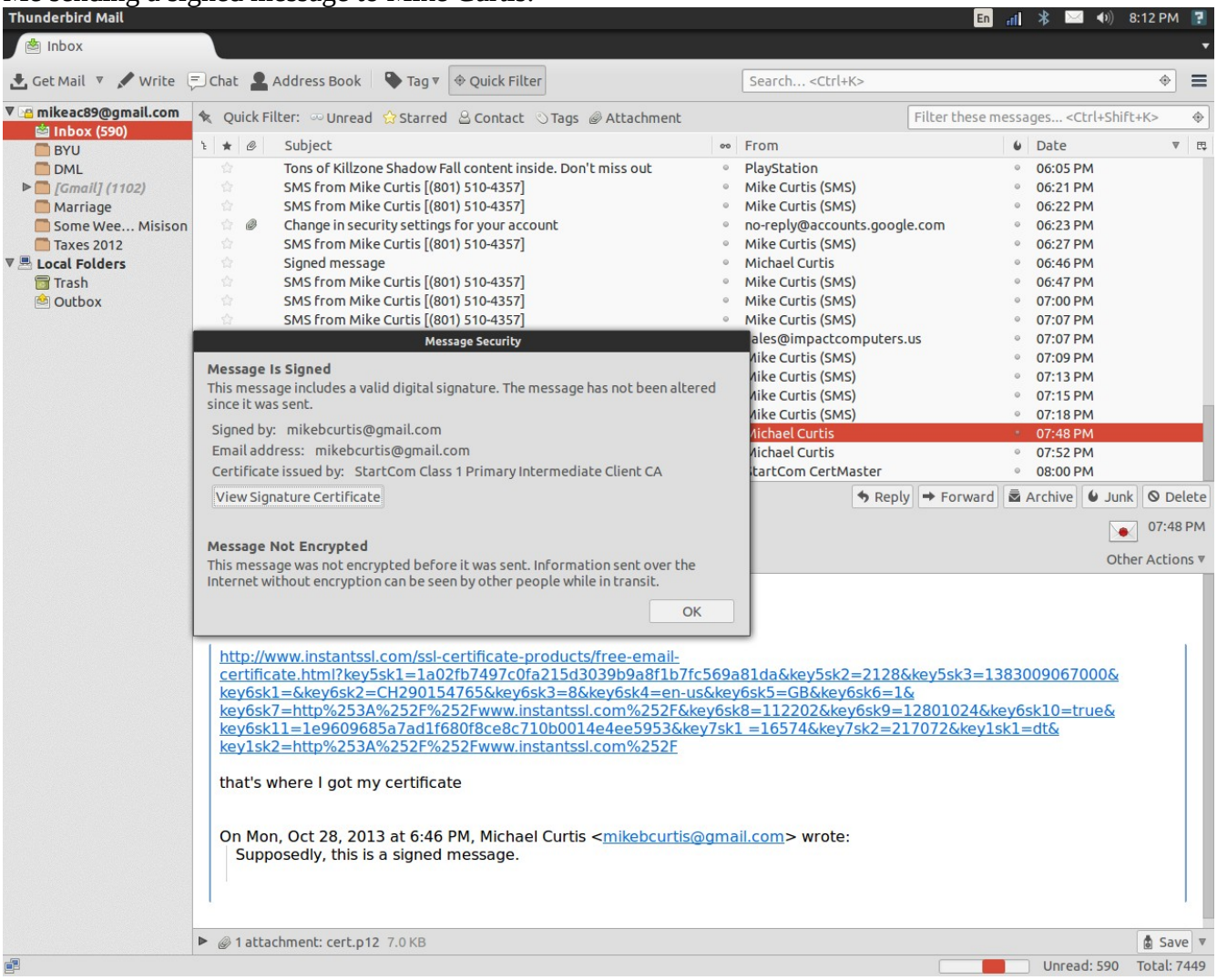
Mike Curtis Decrypting my Encrypted Messages:



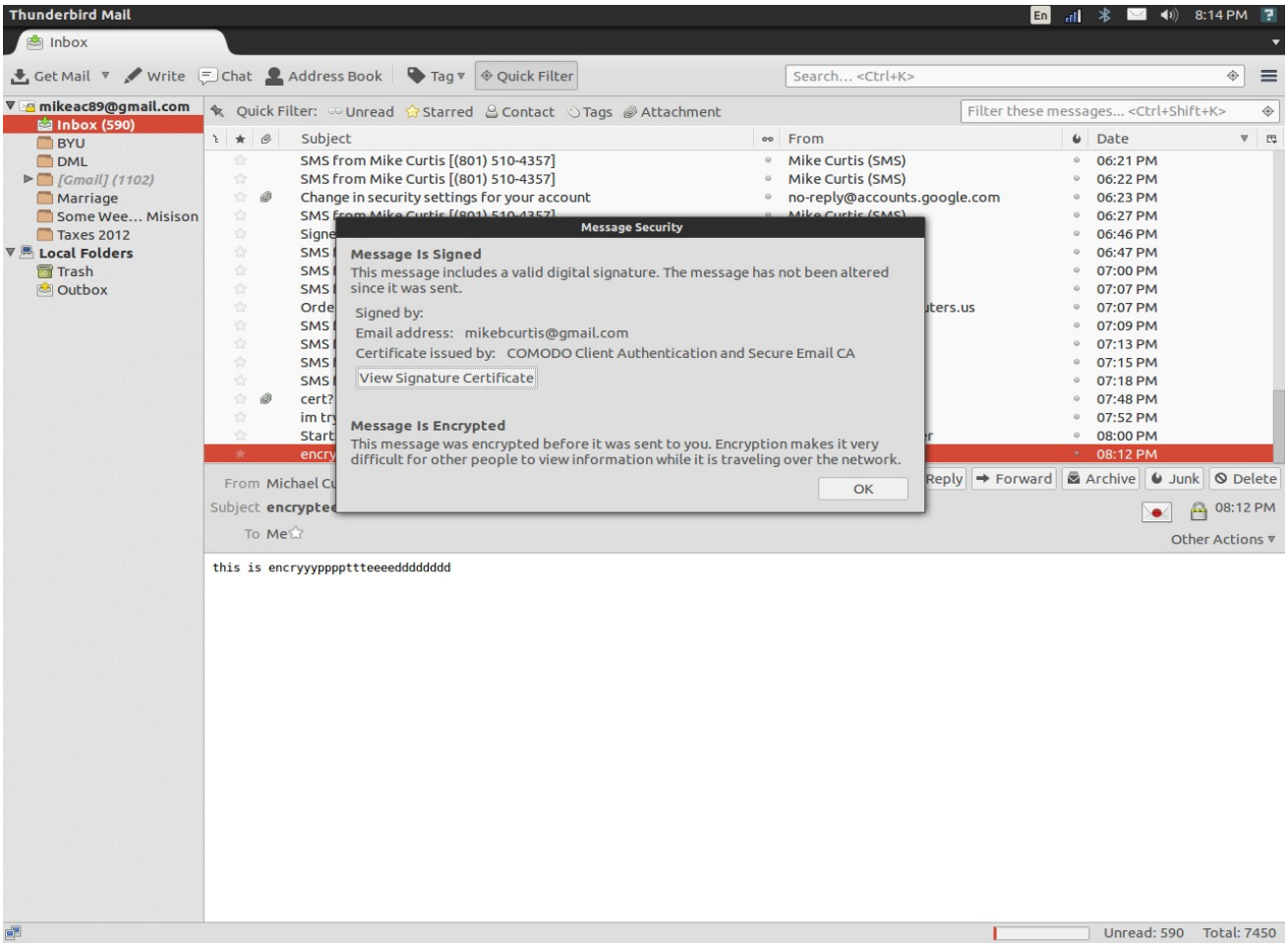

Re: SMS from Mike Curtis
print screen - Microsoft C
security - How can I get G
https://mail.google.com/mail/u/0/?shva=1#inbox/141f726b56341ffd
Google
+Michael
Share
Click here to enable desktop notifications for Gmail. Learn more Hide
Gmail
More
1 of 640
COMPOSE
Inbox (639)
Starred
Important
Chats
More labels
Search people...
Trevor Bentley
Adam DeMello
Available
Brian Spencer
Danny Koch
Ernesto Aldape
Michael Christen...
Michael Christensen
to me
6:12 PM (6 minutes ago)
Hello Comrade Curtis,
I hope you are found well in the Motherland. Our plan for world domination continues perfectly. The Americans have finally discovered the Higgs Boson and we will be able to use this to create Motherland's world engulfing black hole.
- Comrade Christensen
~BN
Click here to Reply or Forward
ADT® Business Sale
Ads
Firewall
Looking For A Next Gen Firewall? Learn About Cisco ASA5500 Firewall.
www.cisco.com
Free Assurance® Phones
See If You Qualify For A Free Phone 250 Free Minutes & 250 Free Texts!
www.AssuranceWireless.com
Capital One® Credit Cards
See if you pre-qualify in 60 sec. Find a card with features you want!
www.CapitalOne.com
Compare Ford® Escape
Compare the Ford Escape to the Competition Today!
www.ThinkFordNow.com
mikec.gpg
Show all downloads...
6:18 PM
10/26/2013

S/MIME:

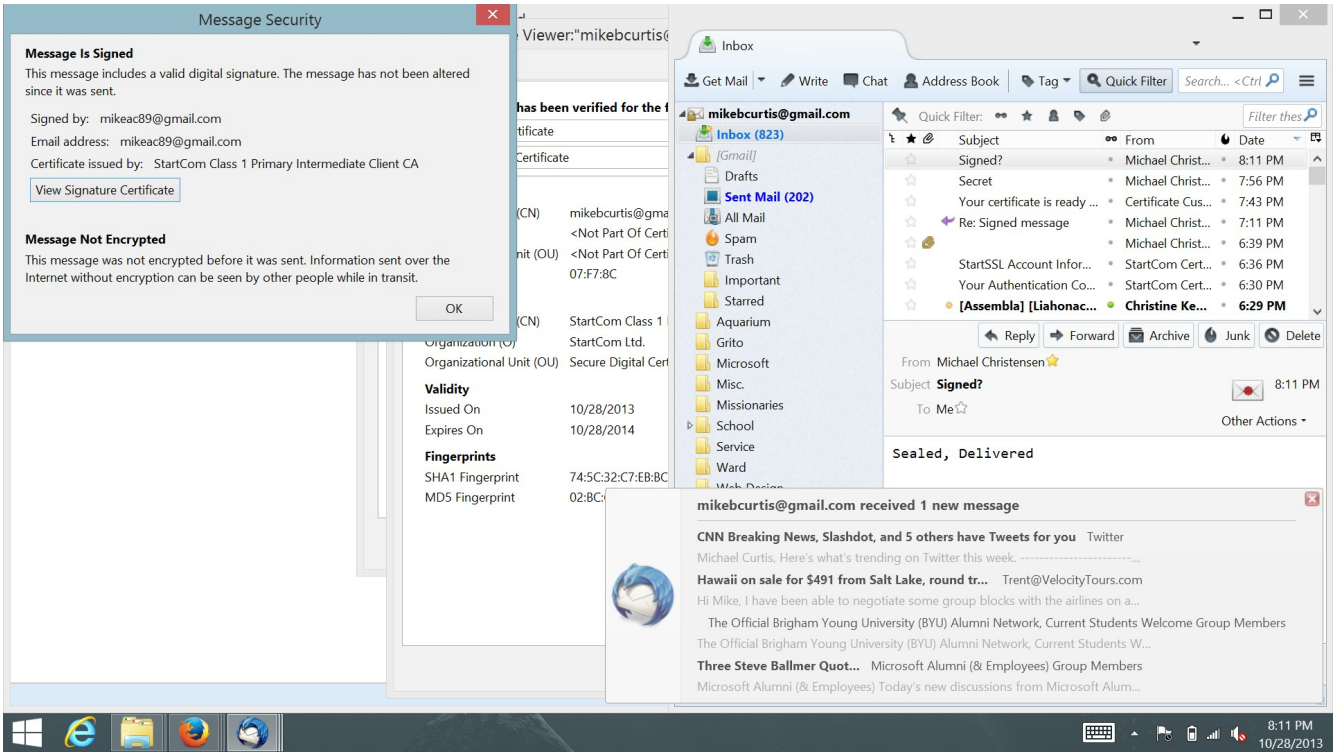
Me sending a signed message to Mike Curtis:



Me sending a signed and encrypted message to Mike Curtis:



Mike Curtis receiving my Signed Message:



Mike Curtis receiving my Signed and Encrypted Message: