Asymmetric Key Cryptography

ANIMESH KUMAR

Student of NLIU, Bhopal

Contact Details:

Mail: kumar.animesh91@gmail.com

Mobile: +91-9713914470

Skype: animeshkumarr

ABSTRACT

Cryptography is a method of encrypting and decrypting the data. It is a science of protecting information by encrypting the data into an unreadable form. Cryptography enables you to transmit the data over the unsecured network like Internet in such a way that no other than the intended recipient can read it. The plaintext or the message is encrypted through the encryption technique which converts the message into the cipher text. When the recipient receives the cipher text, he decrypts it and gets the original message.[1]

Plaintext →Encryption → Cipher text →Decryption → Plaintext

TYPES OF CRYPTOGRAPHY

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric Key Cryptography

In this type of cryptography, the same key is used for both encryption and decryption. This cryptography technique is very fast but once the secrecy of key is compromised then anyone can read, modify and forge all the information encrypted with that key.[2]

Asymmetric Key Cryptography

This technique is popularly known as Public Key Cryptography. This cryptography uses a pair of keys, public key and private key. Public key encrypt the data whereas corresponding private key is needed to decrypt the data. The public key is known to all and the data is encrypted using the public key, if someone wants to read it then the corresponding private key is needed.[3]

[1] http://en.wikipedia.org/wiki/Cryptography

[2] Refer, *Cyber Crime and Corporate Liability by Rohas Nagpal*, (ISBN: 8184731450, 9788184731453)

[3] Cisspallinone.pdf

Strengths and Weaknesses of asymmetric key systems

Strengths

- Better key distribution than symmetric systems
- Better scalability than symmetric systems
- Can provide confidentiality, authentication, and non-repudiation

Weaknesses

- Works much slower than symmetric systems

Examples of asymmetric key algorithms

• RSA	(Ron **R**ivest,Adi **S**hamir,Leonard **A**dleman)
• Diffie-Hellman	(**Diffie-Hellman**)
• El Gamal	(Taher **E1Gamal**)
• DSA	(**D**igital **S**ignature **A**lgorithm)

How Does Public Key Cryptography Work?

We have established that symmetric cryptography provides limited security because two users use the same key, and although asymmetric cryptography enables the two users to use different keys, it is too slow when compared to symmetric methods. So some really smart people decided to use them together to accomplish a high level of security in an acceptable amount of time.

In the hybrid approach, the two different approaches are used in a complementary manner, with each performing a different function. A symmetric algorithm creates keys that are used for encrypting bulk data and an asymmetric algorithm creates keys that are used for automated key distribution.

When a secret key is used for bulk data encryption, this key is used to encrypt the message you want to send. When your friend gets the message you encrypted, you want him to be able to decrypt it. So you need to send him the necessary key to use to decrypt the message. You do not want this key to travel unprotected, because if the message was intercepted and the key was not protected, an evildoer could intercept the message that contains the necessary key to decrypt your message and read your information. If the secret key that is needed to decrypt your message is not protected, then there is no use in encrypting the message in the first place. So we use an asymmetric algorithm to encrypt the secret key. Why do we use the symmetric algorithm on the message and the asymmetric algorithm on the key? We said earlier that the asymmetric algorithm takes longer because the math is more complex. Because your message is most likely going to be longer than the length of the key, we use the faster algorithm on the message (symmetric) and the slower algorithm on the key (asymmetric).[4]

Points to Remember

- Asymmetric algorithm performs encryption and decryption by using public and private keys.
- Symmetric algorithm performs encryption and decryption by using a secret key.
- A secret key is used to encrypt the actual message.
- Public and private keys are used to encrypt the secret key.
- A secret key is synonymous to a symmetric key.
- An asymmetric key refers to a public or private key.

Public Key Infrastructure (PKI)

A public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party validation authority (VA) can provide this information on behalf of CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the registration authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation[5]

[4] cisspallinone.pdf

[5] http://en.wikipedia.org/wiki/Public-key_infrastructure

Public-key Cryptography Standards (PKCS)

PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)

PKCS#3 Diffie-Hellman Key Agreement Standard

PKCS#5 Password Based Encryption Standard

PKCS#6 Extended-Certificate Syntax Standard

PKCS#7 Cryptographic Message Syntax standard

PKCS#8 Private Key Information Syntax standard

PKCS#9 Selected Attribute Types

PKCS#10 RSA Certification Request

PKCS#11 Cryptographic Token Interface Standard

PKCS#12 Portable format for storing/transporting a user's private keys and certificates

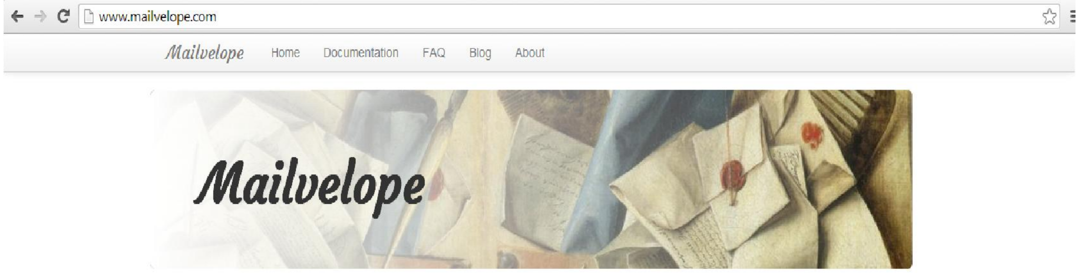
PKCS#13 Elliptic Curve Cryptography Standard

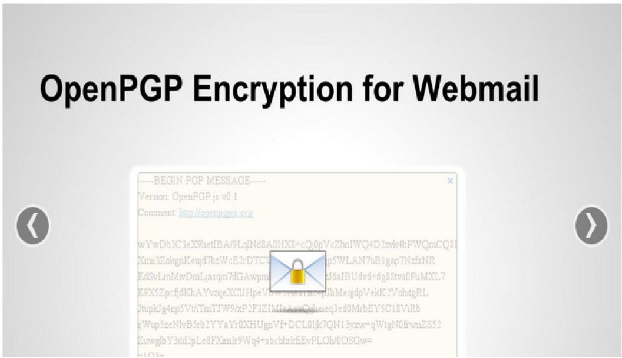
PKCS#15 Cryptographic Token Information Format Standard;[6]

[6] http://www.naavi.org/importantlaws/itrules/regulations_july92001.htm

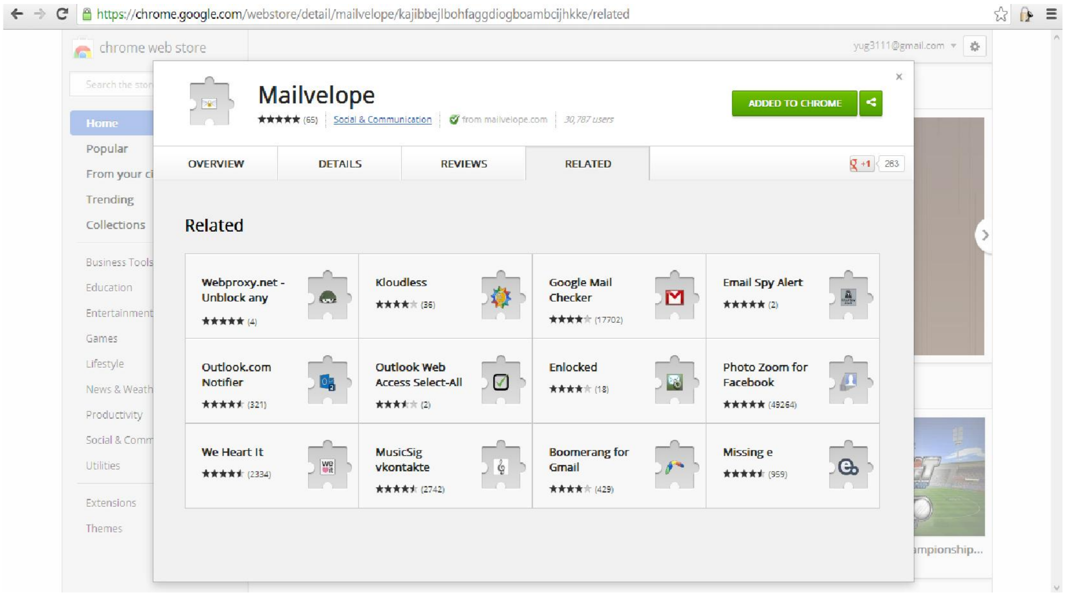
Practical Demonstration Of Asymmetric Key Cryptography

- Go to The URL http://www.mailvelope.com/

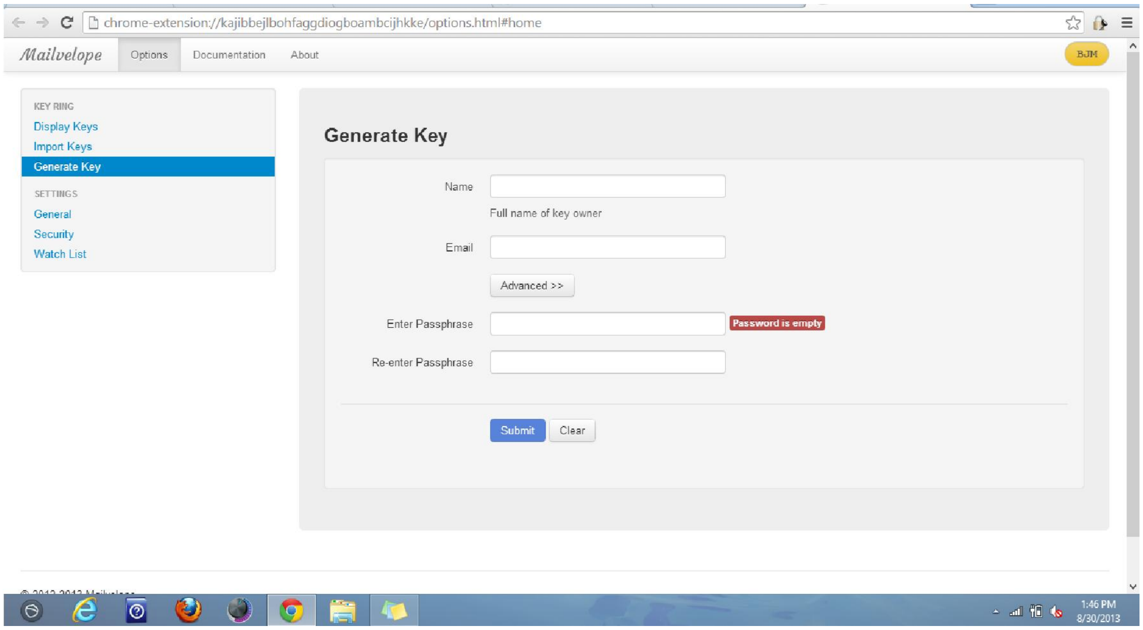




- Install it according to your browser



- Generate key pair



chrome-extension://kajibbejlbohfaggdiogboambcjjhkke/options.html#home

Generate Key

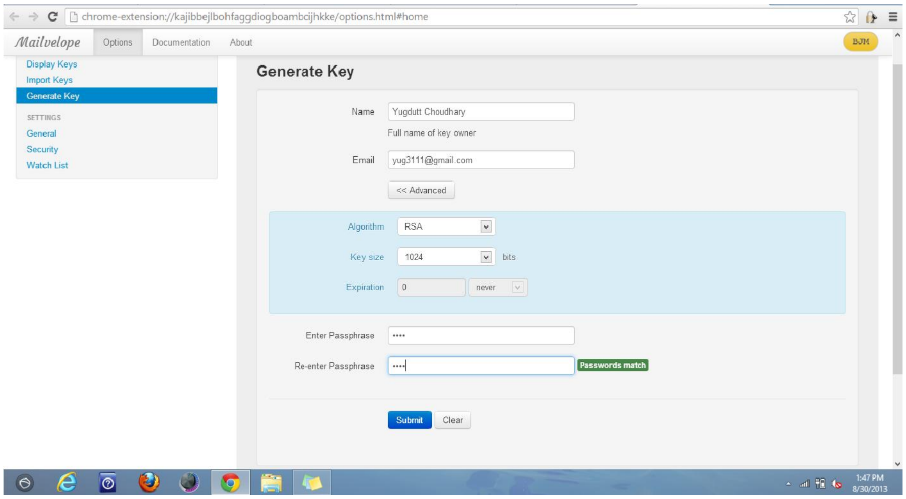
Name: (empty) — Full name of key owner

Email: (empty)

Enter Passphrase: (empty) — Password is empty

Re-enter Passphrase: (empty)

- Enter details



chrome-extension://kajibbejlbohfaggdiogboambcjjhkke/options.html#home

Generate Key

Name: Yugdutt Choudhary — Full name of key owner

Email: yug3111@gmail.com

Algorithm: RSA

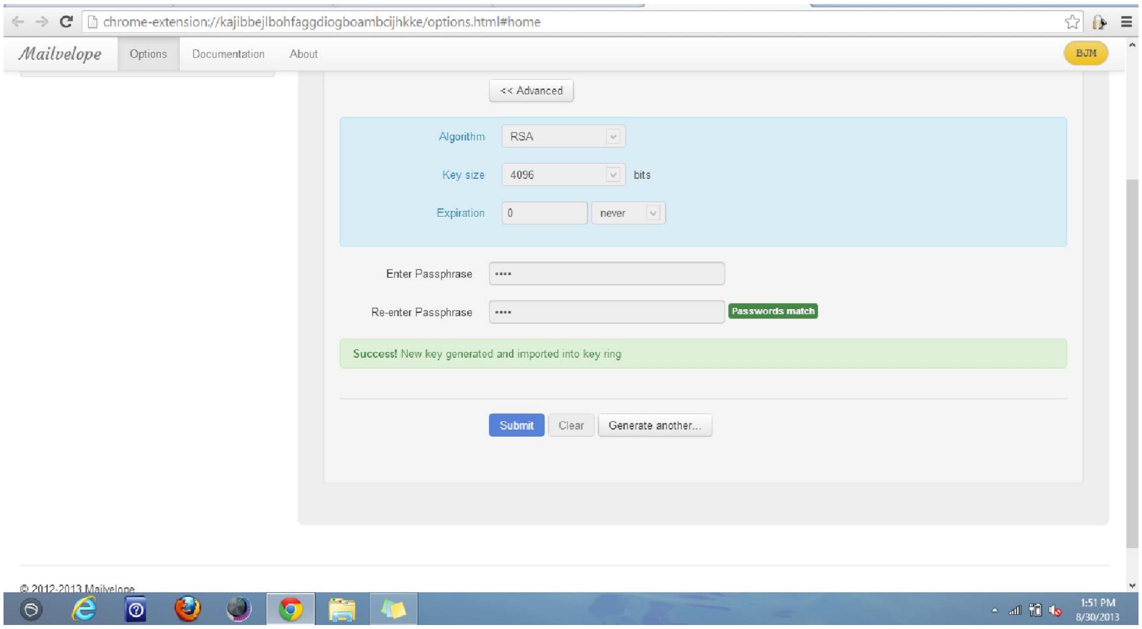
Key size: 1024 bits

Expiration: 0 never

Enter Passphrase: ••••

Re-enter Passphrase: •••• — Passwords match

- You will see a “Success” message



Algorithm: RSA

Key size: 4096 bits

Expiration: 0 never

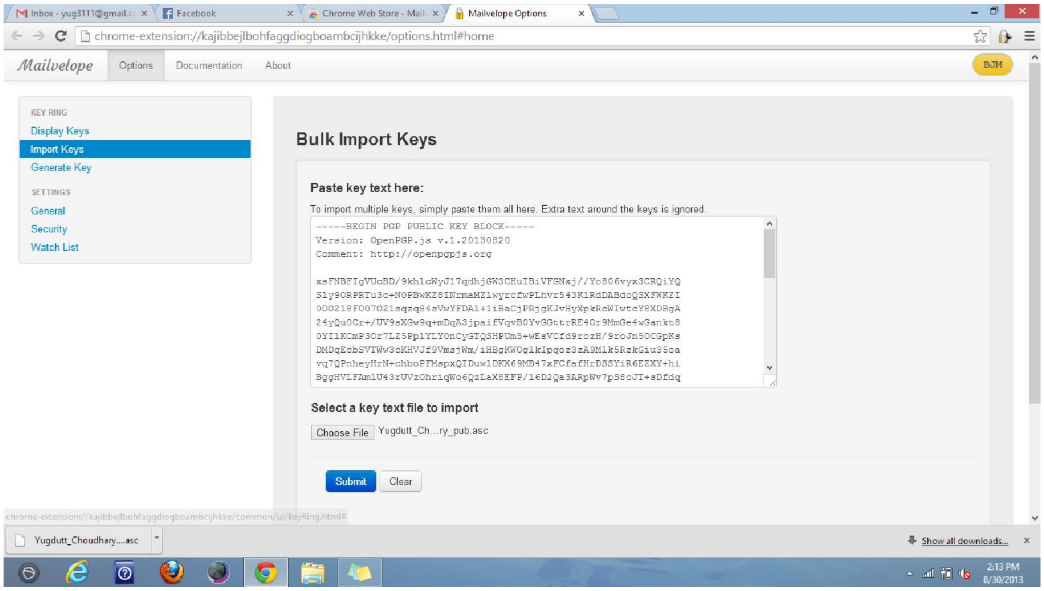
Enter Passphrase: ••••

Re-enter Passphrase: •••• Passwords match

Success! New key generated and imported into key ring

© 2012-2013 Mailvelope

- Import Keys



Bulk Import Keys

Paste key text here:

To import multiple keys, simply paste them all here. Extra text around the keys is ignored.

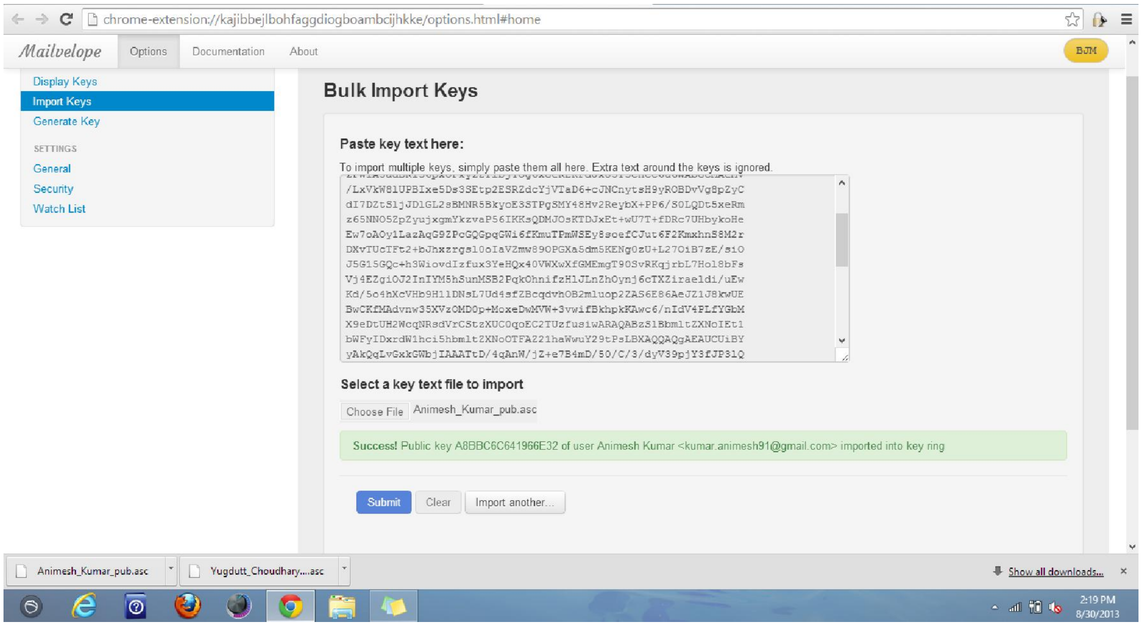
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v.1.20130820
Comment: http://openpgpjs.org

xsFNBFIgVUcBD/9kh1cWyJ17qdhjGW3CHuIBiVFGNxj//Yo806vyx3CRQiYQ
Sly9ORPRTu3c+N0PBwKZ8INrmaMZlwyrcfwPLhvr543K1RdDABdoQSXFWKZI
0OOZ18FO07OZ1sqzq84sVwYFDAl+1iBaCjPRjgKJvHyXpkRcWIwtcY8XDBgA
24yQu0Cr+/UV9sXGw9q+mDqA3jpaifVqvB0YvGGttrRE4Or9MmGe4wGankt8
0YI1KCmP3Or7LZ5Ppl YLY0nCyGTQSHPUm5+wEsVCfd9rozH/9roJn5OCGpKs
DMDqEcbSVTWw3cKHVJf9VmsjWm/iHBgKWOglkIpqoz3zA9Mlk5RzkGiu35oa
vq7QPnheyHrN+chboPFMspxQIDuwlDKX69MB47xFCfafHrDS5YiR6EZXY+hi
BggHVLFAm1U43rUVzOhriqWo6QzLaX8EFP/16D2Qa3ARpWv7pS8cJT+sDfdq
```

Select a key text file to import

Choose File Yugdutt_Ch...ry_pub.asc

- Export the Public Key to Other



Bulk Import Keys

Paste key text here:

To import multiple keys, simply paste them all here. Extra text around the keys is ignored.

```
/LxVkW81UPBIxe5Ds3SEtp2ESRZdcYjVTaD6+cJNCnytsH9yROBDvVg8pZyC
dI7DZtSljJDlGL2sBMNR5BkyoE3STPgSMY48Hv2ReybX+PP6/SOLQDt5xeRm
z65NNO5ZpZyujxgmYkzvaP56IKKsQDMJOsKTDJxEt+wU7T+fDRc7UHbykoHe
Ew7oAOy1LazAqG9ZPcGQGpqGWi6fKmuTPmWSEy8soefCJut6F2KmxhnS8M2r
DXvTUcTFt2+bJhxzrgsl0oIaVZmw89OPGXa5dm5KENg0zU+L27OiB7zE/siO
J5G15GQc+h3WiovdIzfux3YeHQx40VWXwXfGMEmgT90SvRKqjrbL7Hol8bFs
Vj4EZgiOJ2InIYM5hSunMSB2PqkOhnifzHlJLnZhOynj6cTXZiraeldi/uEw
Kd/5o4hXcVHb9H1lDNsL7Ud4sfZBcqdvhOB2mluop2ZAS6E86AeJZ1J8kwUE
BwCKfMAdvnw35XVzOMD0p+MoxeDwMVW+3vwifBkhpkKAwc6/nIdV4PLfYGbM
X9eDtUH2WcqNRsdVrCStzXUC0qoEC2TUzfusiwARAQABzSlBbmltZXNoIEt1
bWFyIDxrdW1hci5hbmltZXNoOTFAZ21haWwuY29tPsLBXAQQAQgAEAUCUiBY
yAkQqLvGxkGWbjIAAATtD/4qAnW/jZ+e7B4mD/50/C/3/dyV39pjY3fJP31Q
```

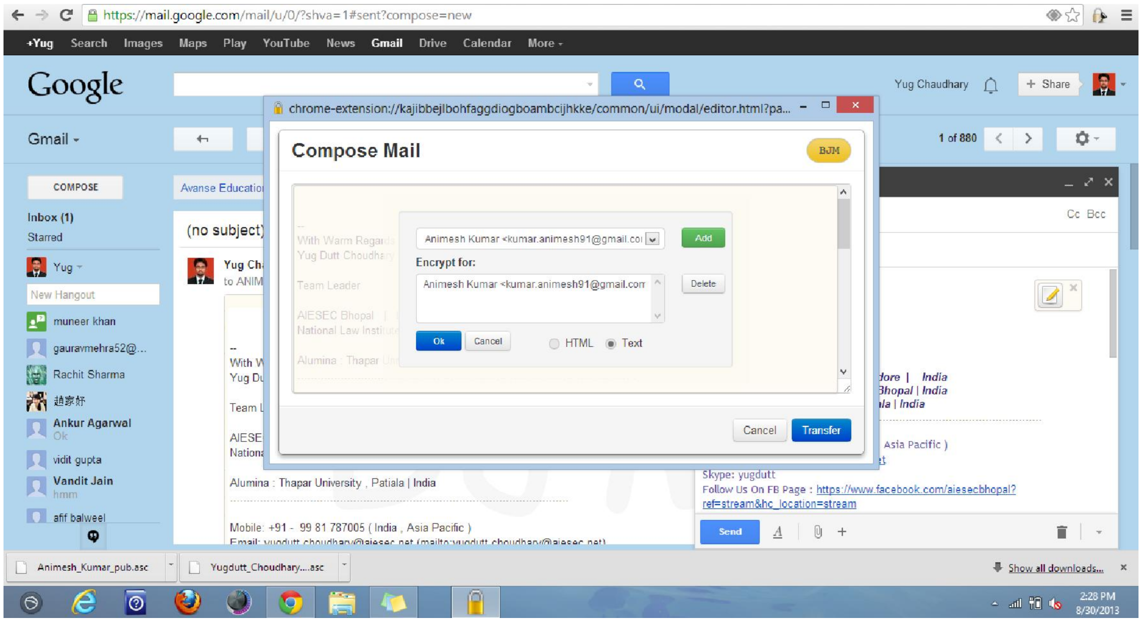
Select a key text file to import

Choose File Animesh_Kumar_pub.asc

Success! Public key A8BBC6C641966E32 of user Animesh Kumar <kumar.animesh91@gmail.com> imported into key ring

Submit   Clear   Import another...

- Compose Your mail and Click on mailvelope and add another party.



chrome-extension://kajibbejlbohfaggdiogboambcijhkke/common/ui/modal/editor.html?pa...

Compose Mail

Animesh Kumar <kumar.animesh91@gmail.co   Add

Encrypt for:

Animesh Kumar <kumar.animesh91@gmail.com   Delete

Ok   Cancel   ○ HTML ● Text

Cancel   Transfer

--
With Warm Regards
Yug Dutt Choudhary

Team Leader

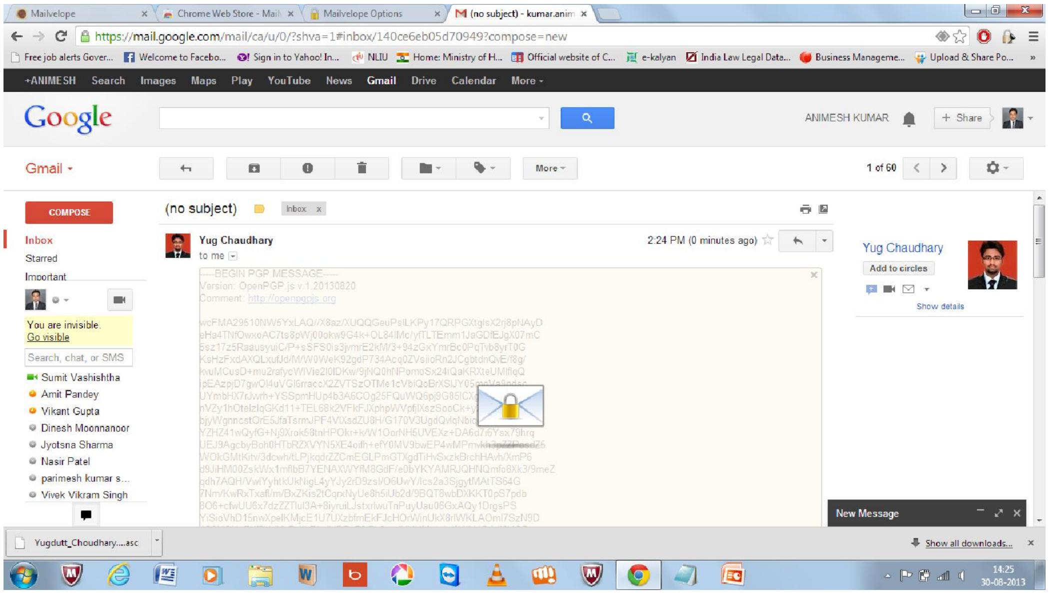
AIESEC Bhopal |
National Law Institute

Alumina : Thapar University , Patiala | India

Mobile: +91 - 99 81 787005 (India , Asia Pacific)

Skype: yugdutt
Follow Us On FB Page : https://www.facebook.com/aiesecbhopal?ref=stream&hc_location=stream

- Now enjoy the encrypted mail and send it.



(no subject)

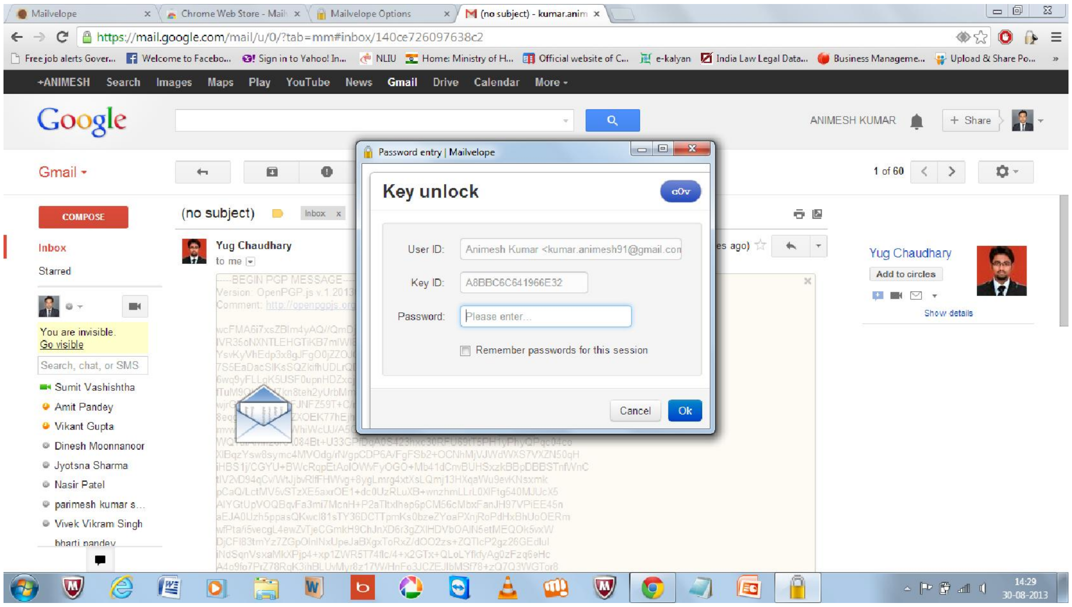
Yug Chaudhary
to me

2:24 PM (0 minutes ago)

```
-----BEGIN PGP MESSAGE-----
Version: OpenPGP.js v.1.20130820
Comment: http://openpgpjs.org

wcFMA29510NW5YxLAQ//X8az/XUQQGeuPsILKPy17QRPGXtglsX2rj8pNAyD
eHa4TNfOwxoAC7ts8pWj00okw9G4k+OL84IMc/yfTLTEmm1JaGDfEJgX07mC
5sz17z5RaausyuiC/P+sSFS0is3jvmrE2kM/3+94zGxYmrBc0PqTvb8yrT0G
KsHzFxdAXQLxufJd/M/W0WeK92gdP734Acq0ZVsiioRn2JCgbtdnQvE/f8g/
kvuMCusD+mu2rafycWIVie2I0IDKw/9jNQ0hNPomoSx24iQaKRXteUMIflqQ
```

- Unlock mail by using your private key



Key unlock

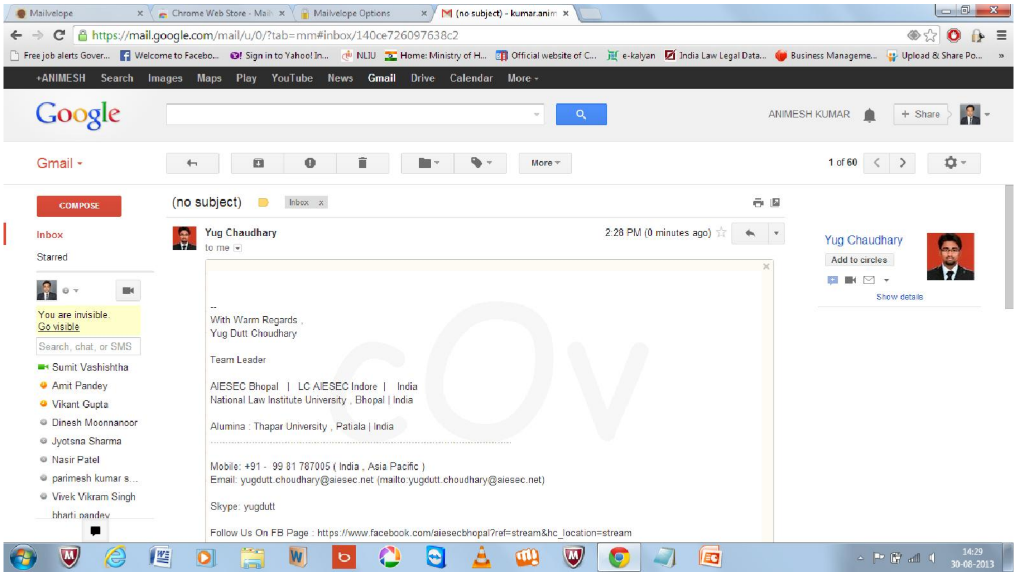
User ID: Animesh Kumar <kumar.animesh91@gmail.com

Key ID: A8BBC6C641966E32

Password: Please enter...

□ Remember passwords for this session

- Now you can decrypt the mail and read your confidential Information



--
With Warm Regards ,
Yug Dutt Choudhary

Team Leader

AIESEC Bhopal | LC AIESEC Indore | India
National Law Institute University , Bhopal | India

Alumina : Thapar University , Patiala | India

Mobile: +91 - 99 81 787005 (India , Asia Pacific)
Email: yugdutt.choudhary@aiesec.net (mailto:yugdutt.choudhary@aiesec.net)

Skype: yugdutt

Follow Us On FB Page : https://www.facebook.com/aiesecbhopal?ref=stream&hc_location=stream

Citation:

Mail id used in practical is of Animesh Kumar (kumar.animesh91@gmail.com) & Yugdutt Chaudhary(yug3111@gmail.com)