Asymmetric (Public-Key) Cryptography

In this assignment students will:

1. Understand common terms associated with asymmetric cryptography (e.g. Asymmetric Cryptography, Key-Pair, Private Key, Public Key, Public Key Infrastructure)
2. Explain why a cybercriminal may want to use asymmetric cryptography
3. Generate their own private and public keys
4. Encrypt and decrypt communications using keypairs

Reading

Use the reading entitled "Understanding Asymmetric Cryptography" to answer the questions below:

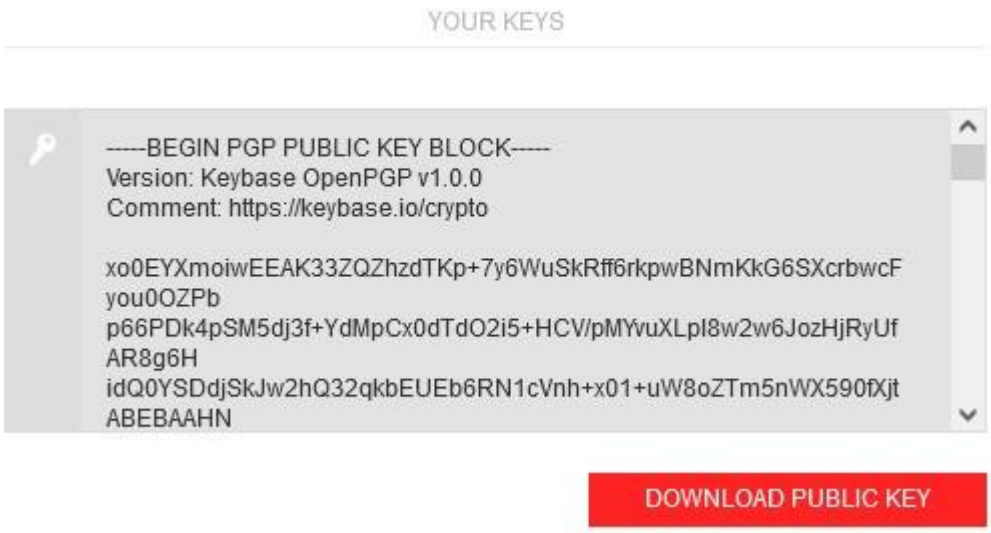
1. Explain why encrypted online communications between people (or machines) require a separate public and private key. **(10 pts)** **They require them so that the information may stay hidden from the public eye so that it may be safe from being stolen.**
2. Describe the difference between symmetric and asymmetric cryptography. **(10 pts)** **Symmetric encryption deals with timeframes while asymmetric does not deal with specific timeframes. Symmetric also uses the same key to encrypt and decrypt, while asymmetric uses two separate keys, public and private, to encrypt and decrypt.**
3. Describe how someone can prove they are the sender of a message using public and private keys. **(10 pts)** **They can create a hash and encrypt it, then send the hash to the receiver to compare it after decryption.**
4. How can someone share their public key? **(5 pts)** **He can share it online on accounts or websites he owns.**
5. How can asymmetric cryptography be used to verify the author of a message? **(10 pts)** **By receiving the hash of the encrypted original message, you can decrypt the hash and then compare the two hashes given to check for alteration.**

Part 2: Working With Keys

Go to https://pgpkeygen.com/ and generate a sample keypair. Your keypair is linked to a name and an email.

This is just for practice, so you can see what a keypair looks like, so use a fictitious email (you just need to use a standard format - sometext@email.com, and the application will accept it. You will be asked to select other options and you can choose whatever you like.

6. Take a screenshot of your public key and place it in the document. **(5 pts)**

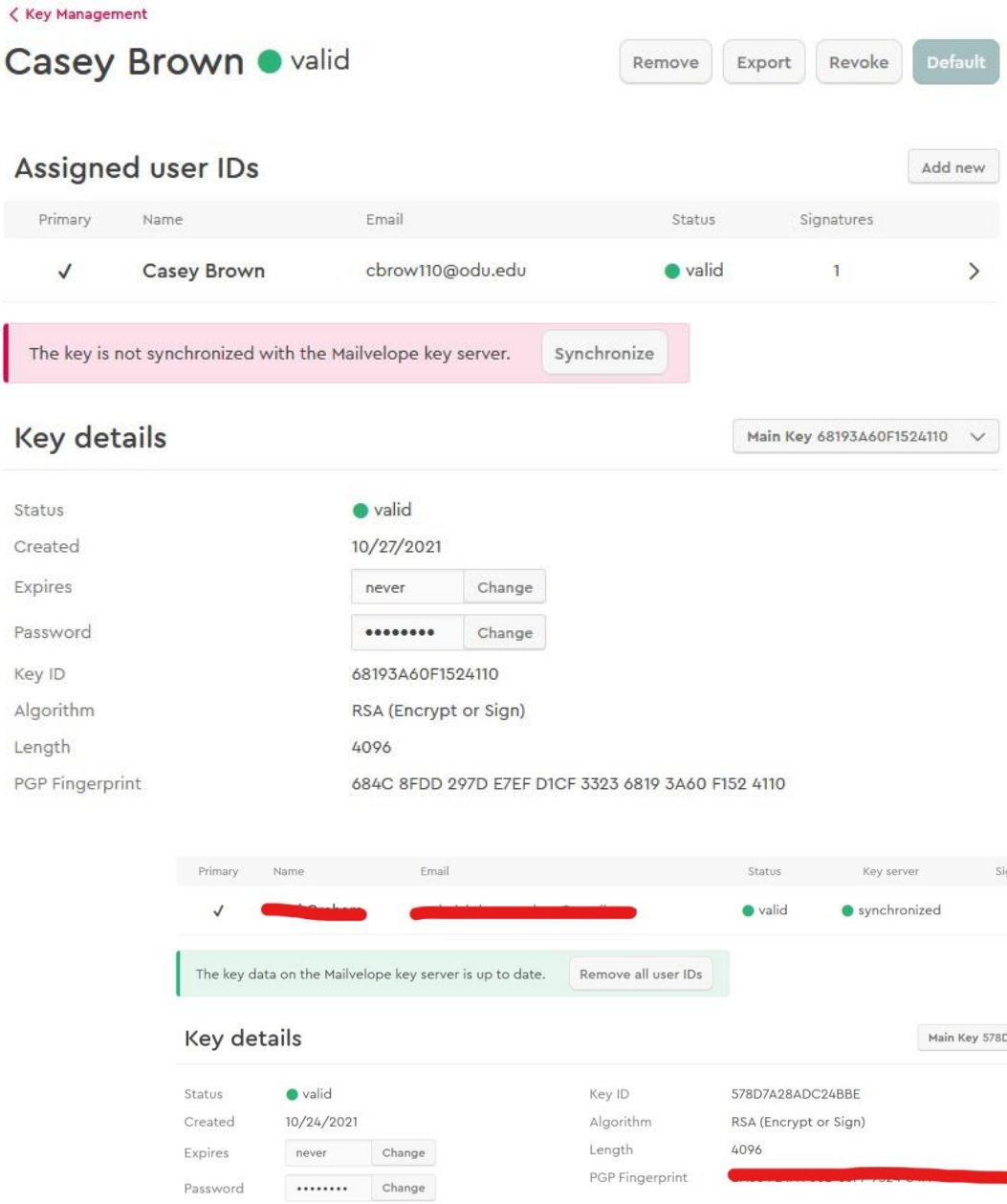


7. Download your keys. What is the extension of the keys? **(5 pts)** **The extension is a .asc extension.**
8. Why do you need a passphrase? **(5 pts)** **You need a passphrase to make sure you don't lose your keys.**

Now, let's make a real keypair that you can use to encrypt or sign messages if you like in the future. You will be using Mailvelope. It is a browser add-on for Firefox, Chrome, and Edge.

Install the add-on, and then generate your own key. Use a real email that belongs to you this time.

9. Place a screenshot like the one below of your key details into your assignment (without the strikethroughs.) You do this by going to "key management" and then clicking on the key. You have a PGP fingerprint, which is an MD5 hash of your key, and you have a Key ID, which is the last 16 digits of the hash. You can usually search for keys via the email or the Key ID. **(10 pts)**



10. Your public key has been automatically uploaded to Mailvelope's keyserver: [Mailvelope Key Server]. Find your key and screenshot the top where your email is like the sample below. **(10 pts)**

Email: cbrow110@odu.edu

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBGF5qcIBEADNj8/Cs+zlGn9DcpYp3AgepjpqcChSXr5wFF+64BmnOLbz
ReAmESCKbq3yTDrAh3Vb58aF3XyrRudVxDuBKnKR0w6uQzTzfzvp2YvxvNWB
z70LD8TC/8rW7z8krjXOT4BCJ7JD0GMFzZ3OJ0pomvCFJWSJX4jiv0C+4/Kz
hTWZnq0q7xAYwXoVZ+6g/yB6V6t9yZXYVK0aT2ozi5hnFirRcuUY0R/CD0SY
1QF7Ll+8h1js5mKaeEn4ZkJlUQnRxfbGYlJKvgfqLAXSENDCSKHRJUVIr6CQ
IbCEsT60VBebPaaqxvfRrpX3sJcusoQotZtJUku4lIqkmBBmstidlyveCC3D
```

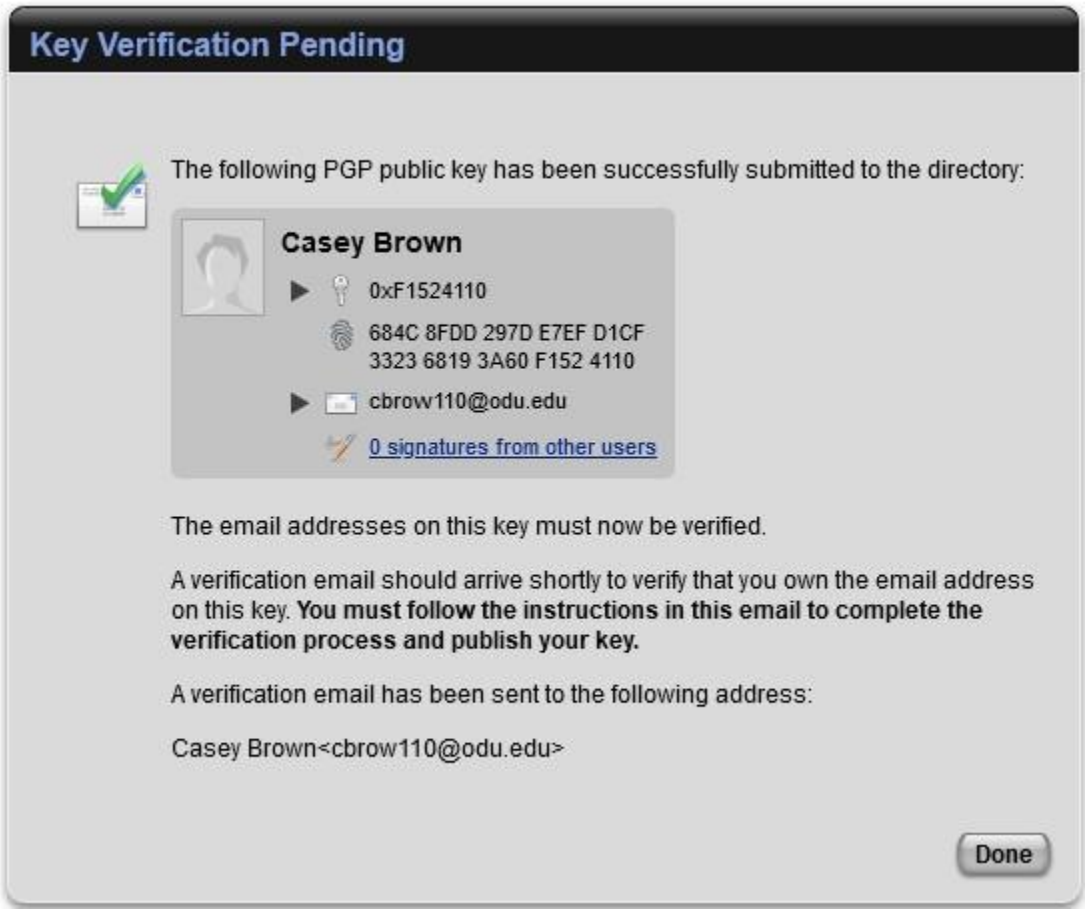
Mailvelope Key Server

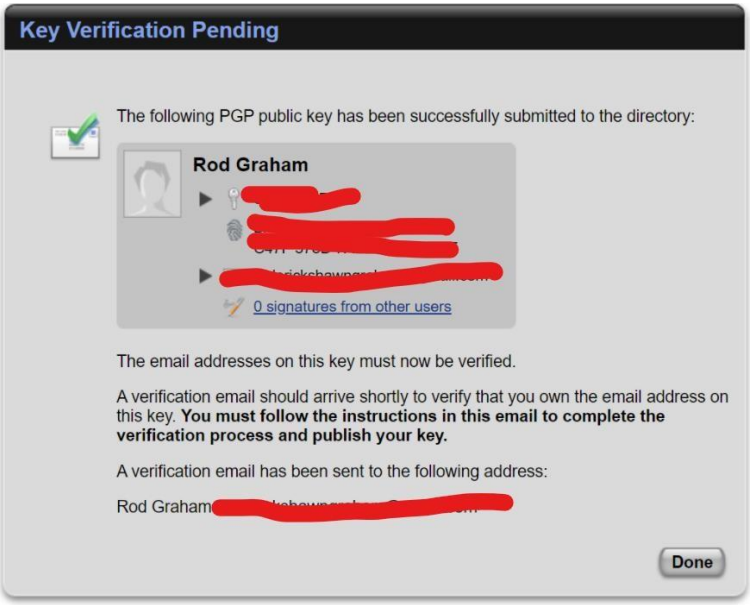
Home Manage Keys GitHub

Email: [redacted]

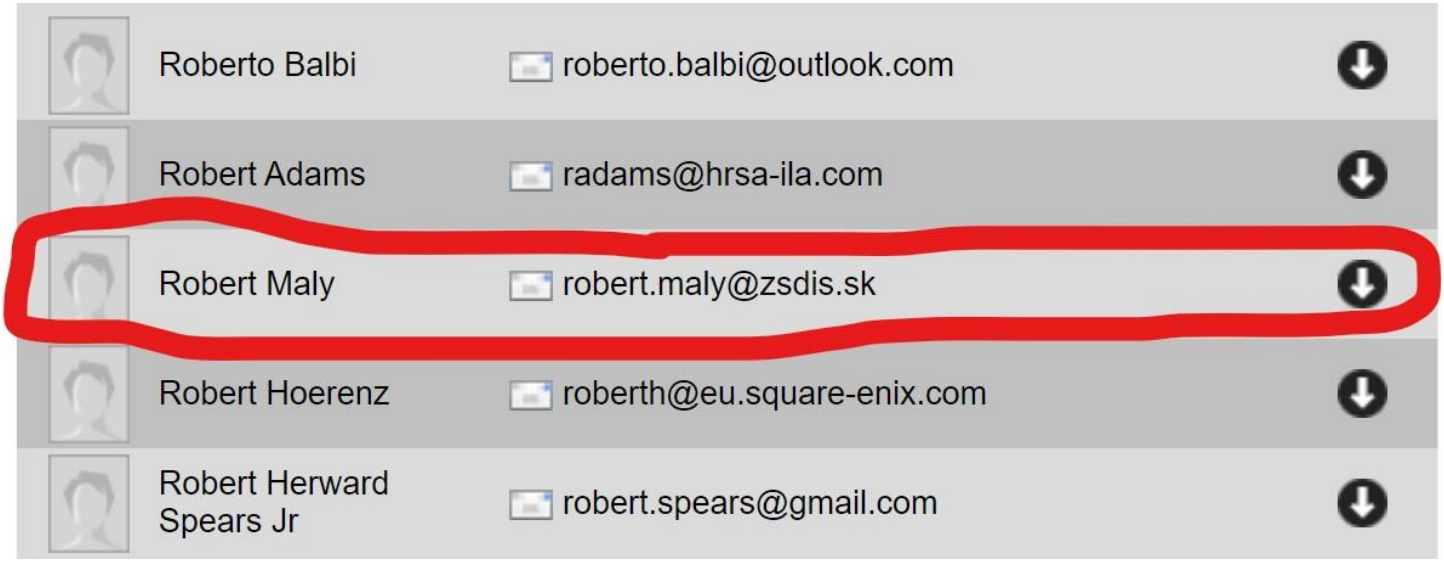
```
-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBGF19AgBEADBMlGyfFX/mkyjwl3ttsSQgXs6CNGpAO1n6rULEwZJ3tcS
t6ydQ2aLVhRU5p5JTm4b0B4dI160tndFt03QhC+jy2IXH4VhaBjqJcC/o7X4
9QVxZ5oPMMuRzco5NmCsWVmxETo1LZLSma87qnmJdZcycBTTBMfXvGhMjERP
dURR67F9zs2s6jTvu/dN3KZhwm+BdbLly7YNG7mKTKIXCLJb7dG4qvIHZZGi
wkLD9F4z44JpieERjBNiCKi5/qgBx2rzQyeejbIssPbcFfXFQmKg+Sos3Ay5
vY89DNctlzjan6Ug32qtaiVo7c9r+HyMuuLDqj9IOlUGs+bXj7xCtTabwLIy
N8GwpUX/Sv2SYQF1C7BAk/JVDAE7uKpTCusrYDr+RSCK2dSJErA7EhFCHvly
dMotWzx7jn02cuWzRPEKmwazS8P6Ka0rfZ0Md8b3SNsNyIdLyF9M2ACPWzZE
PLQrIW3aSNYjZq4eKT5/JR1eNtkI+fXDJp4jZGXJi/KVfQyk7CVBHDSn1eZb
```

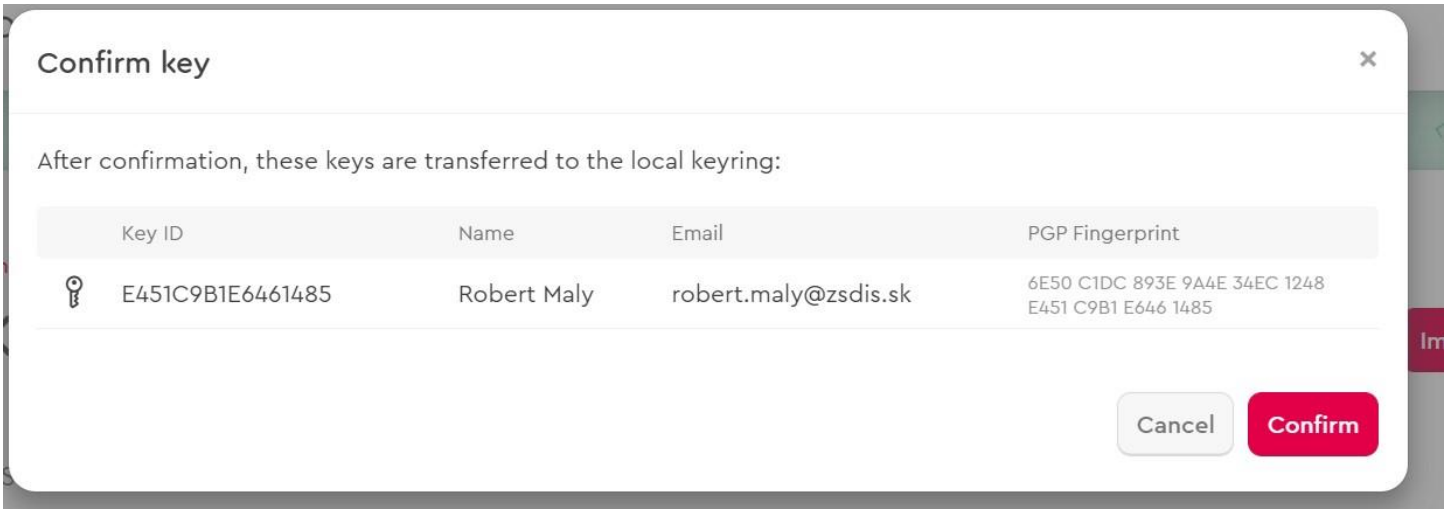
11. There are other key servers as well. PGP Global Directory is one such server. It does not seem to have as many keys as some others. The Ubuntu Keyserver and the MIT servers have more keys (including some old ones of mine!). But I like the interface of PGP Global, and they also ask the person submitting keys to verify their email. Submit your key to the PGP Global Directory and past this image below into your assignment (without the strikethroughs). **(10 pts)**





12. In order to send someone an encrypted message, you need to find (or be given) their public key and import it into mailvelope like so. My key ID is 578D7A28ADC24BBE. Send me an encrypted email that I can decrypt. **(10 pts)**


Roberto Balbi
roberto.balbi@outlook.com
Robert Adams
radams@hrsa-ila.com
Robert Maly
robert.maly@zsdis.sk
Robert Hoerenz
roberth@eu.square-enix.com
Robert Herward Spears Jr
robert.spears@gmail.com


Confirm key
After confirmation, these keys are transferred to the local keyring:
Key ID
Name
Email
PGP Fingerprint
E451C9B1E6461485
Robert Maly
robert.maly@zsdis.sk
6E50 C1DC 893E 9A4E 34EC 1248 E451 C9B1 E646 1485
Cancel
Confirm