Paul Parker

CS373

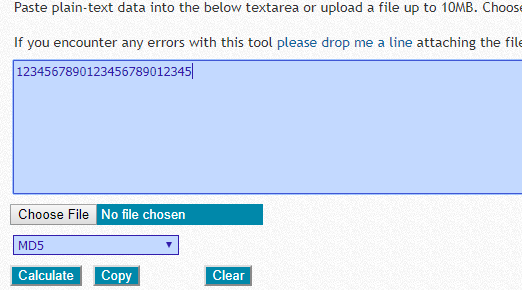
Homework Unit 3

1.

String: 1234567890123456789012345

Binary: 00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001 00110000 00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001 00110000 00110001 00110010 00110011 00110100 00110101

MD5 Hash:

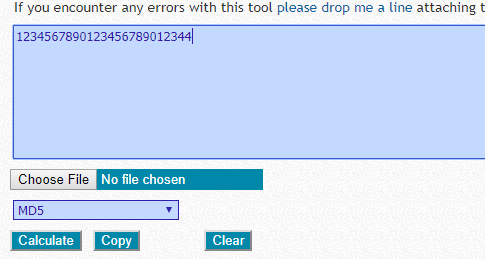


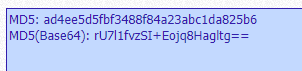


String one bit different: 1234567890123456789012344

Binary: 00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001 00110000 00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001 00110000 00110001 00110010 00110011 00110100 00110100

MD5 Hash:

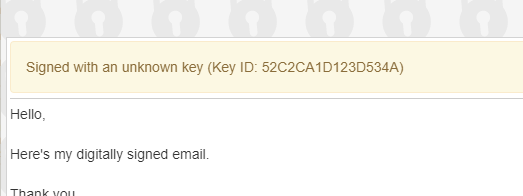




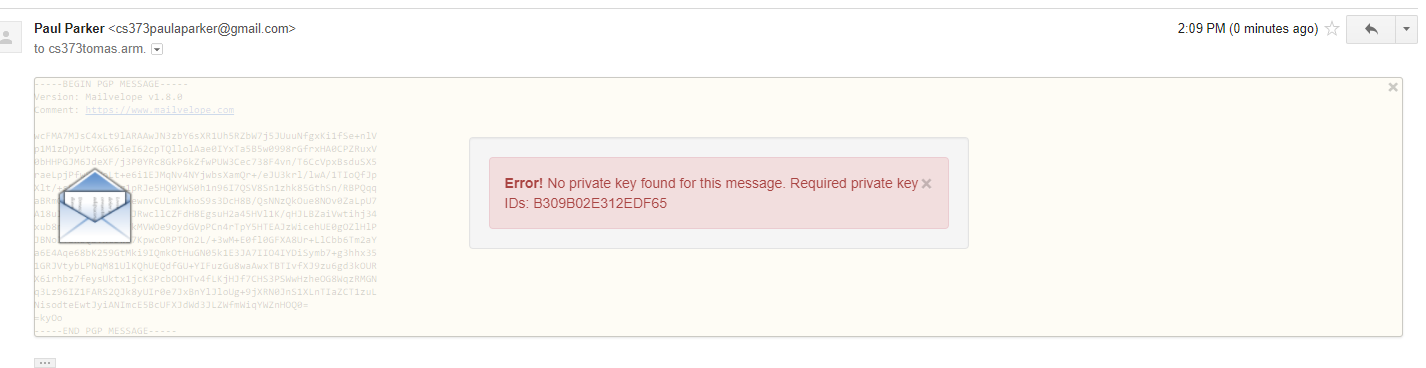
Vastly different results are good because it means that the text cannot be decrypted as easily. If flipping one bit only had a small change on the hash then it would be easier to tell the content of a hash by comparing it to other none hashes. I made sure only one bit was changed by converting the string to binary then flipping the last bit and converting the binary back into a string.

2.

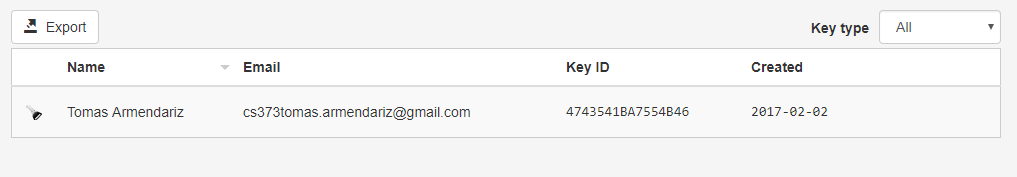
Decrypting the mail with an unknown key:



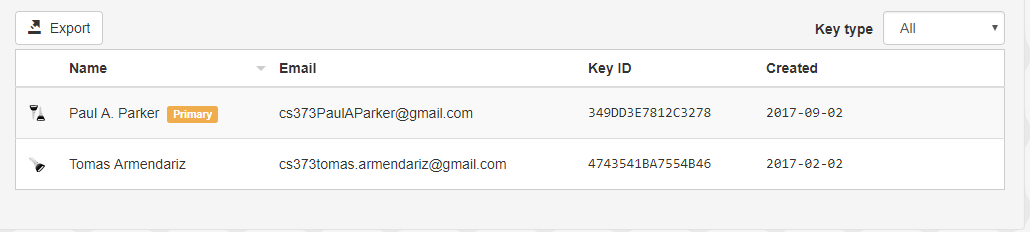
Sent e-mail encrypted with a public key that is now unreadable without the private key:



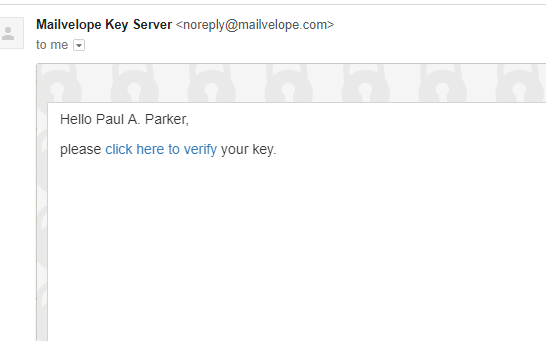
Public key pulled from e-mail from instructor:



Generated public and private key set:



Decrypted confirmation e-mail:



a. What can you do with YOUR private key?

I can use my private keys to sign encrypted e-mails proving they are from me and decrypt encrypted e-mails.

b. What can someone else do with YOUR public key?

Someone can use my public key to encrypt e-mails.

c. How usable is this tool for the average person? Realize that you are doing more work in this lab to understand the process – it would be simpler just generate keys and start using it.

It’s not the most cumbersome thing to set up. It basically does all the work for you. There’s just a few extra clicks to get to information and needing to remember the password.

d. What do you think is the biggest impediment to using Mailvelope?

Probably the biggest impediment is using a browser that supports the plugin. If someone wanted to use Outlook or Thunderbird for mail or something then they might be out of luck.