**CSCI 530: Security Systems**

**Lab Assignment 1: Due 20th September 2024**

**Name: Saketh Anne**

**USC Email:** [**annes@usc.edu**](mailto:annes@usc.edu)

**USC ID: 3725520208**

**Answer 1: Listing the available GPG keys**

(base) sakethanne@Sakeths-Air ~ % gpg --list-keys annes@usc.edu

gpg: checking the trustdb

gpg: marginals needed: 3 completes needed: 1 trust model: pgp

gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u

gpg: next trustdb check due at 2027-09-15

pub ed25519 2024-09-15 [SC] [expires: 2027-09-15]

3D53E2C37A44FAB9D1D2D0A6C142AABD63CE2F01

uid [ultimate] Saketh Anne <annes@usc.edu>

sub cv25519 2024-09-15 [E] [expires: 2027-09-15]

**Answer 2: Printing the contents of the key file**

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

Comment: B00B B2B1 96C7 1D93 CEE5 0E63 82B7 0D78 06D5 7BC7

Comment: Computer Security Systems USC CSci530 <csci530@usc.edu>

xjMEZPScNRYJKwYBBAHaRw8BAQdAKu4fpaXGp6xxwbr37O5+qcDcic7yCMQlY7l3

2Rpklb3NN0NvbXB1dGVyIFNlY3VyaXR5IFN5c3RlbXMgVVNDIENTY2k1MzAgPGNz

Y2k1MzBAdXNjLmVkdT7CmQQTFgoAQRYhBLALsrGWxx2TzuUOY4K3DXgG1XvHBQJk

9Jw1AhsDBQkFo5qABQsJCAcCAiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEIK3DXgG

1XvHqVYBALHO0gRfaDpiKKXOhbI7oDkf3+DAUrTL08zP4JYH/zIbAP0Teei9l6PZ

utrWec2jnhfEj0fFQ+OCnXCcll+19nWLB844BGT0nDUSCisGAQQBl1UBBQEBB0AF

rVQvVSptXbIZFz1xuPSDGDt0N+lB6h24/j3aSeO8dQMBCAfCfgQYFgoAJhYhBLAL

srGWxx2TzuUOY4K3DXgG1XvHBQJk9Jw1AhsMBQkFo5qAAAoJEIK3DXgG1XvH0yEA

/AncQbhZ3zWDdwn0eiCg9OuL0TWwXws9GvgKOoVTMpeIAP4yAQ5KV7eVKxCmfoSZ

i50HgejxjIvFTzPmXwmzN4BRDw==

=DTb+

-----END PGP PUBLIC KEY BLOCK-----

**Answer 3: Printing the contents of the encrypted message (.asc) file from Question 10**

-----BEGIN PGP MESSAGE-----

hF4D+Be7nw4htg8SAQdAnjzlmVt18D7AeqmOgR4ZHxaZb3HO9qmVSRUWonnoTyIw

dSBi3+3p6M+iAodPyQ+Cq11Xg+1sWAyw8wj3cNiZzOUOMmkyJb9/tIs51KulCxHb

1MAQAQkCEAukduezew0nbq3vsxTZqVnw2IDXCl+iQA58W6XE0R+lRsH5xVRtlnZJ

pp50cc+ELFkZenYpCYx5RxiSrPQ48Xjf02GbWzGDPQLn+p5sNcBk1g1D5TpIP3su

0lvZWSsjS2FBZdinZdJHyIipjo8e0GyJQ7CDKB9dCXfjq2KmmddpGDIoDiGE40SX

eAUxznjo7rrDb1LJQcDfC40ISHfOwCQM3d7VeiwzOpoiHsG4VSk7IXeXBEJFxFWQ

ij67c+FWI6q4gjZr7yeMVMRUwg==

=nfjR

-----END PGP MESSAGE-----

**Answer 4: Printing the contents of the file sent back by csci530**

The token is '**sCssa**'

-----BEGIN PGP MESSAGE-----  
  
hF4Debi7xzO5qyISAQdAU6TQJsrzjtAGQr3EgnqqJajyZbjM7R4mZQDDx/fA/D8w  
KLR8Klnk13qH6danUHu4wUzpES73rUSWtT+Q7DP138D5OjruocjUH9/k0ahXb2eg  
0sAeAYFCqZ+0wjq/qtcNArx5NBZtUG6rLTGK6kSiWcoz3mw07bsCixLdWG7NCGKW  
LDThsk3I95GUZvoUO1uxsEZrD5YQWylQWxa4kAX+w/cVvv2hOK07YT7vh1QqOqxC  
CbqAgfGsvoTvP+G0ylpEGNcDffrvfUbSwekHvV1C8ieBdYS5kmuCeN7GxWfe/LOJ  
qW8pTdOhhPyTl8JT/kpdZui6K9K6P9TUygrY6hdMrezwCTl5Kv1kpOshfGp35w+E  
nQO6FNUht5d3I4tw4dZFQrNu4Jcxo3c7J+iGhzlizvam  
=hoeU  
-----END PGP MESSAGE-----

(base) sakethanne@Sakeths-Air ~ % gpg --decrypt encsignedresponse.asc

gpg: encrypted with cv25519 key, ID 79B8BBC733B9AB22, created 2024-09-15

"Saketh Anne <annes@usc.edu>"

Your token is 'sCssa'gpg: Signature made Sun Sep 15 22:25:29 2024 PDT

gpg: using EDDSA key B00BB2B196C71D93CEE50E6382B70D7806D57BC7

gpg: issuer "csci530@usc.edu"

gpg: Good signature from "Computer Security Systems USC CSci530 <csci530@usc.edu>" [unknown]

gpg: WARNING: The key's User ID is not certified with a trusted signature!

gpg: There is no indication that the signature belongs to the owner.

Primary key fingerprint: B00B B2B1 96C7 1D93 CEE5 0E63 82B7 0D78 06D5 7BC7