Carnegie Mellon University: Cryptography

**Solution and insights for lab-5 problems**

**Author’s name: Abel Jotie**

**Date: Dec. 7, 2024**

**Code related:**

2a) python3 certificate\_verification/RSA\_verify.py certificate/abel\_certificate.txt keys/perk\_public\_rsa\_key.txt keys/abel\_signature.txt

2b) python3 certificate\_verfication/system\_param\_verify.py

python3 code/key\_encapsulation/kem\_gen\_ciphertext.py code/client/key\_pub\_perk.b64 code/server/cipher\_output1.b64 code/server/shared\_secret1.b64