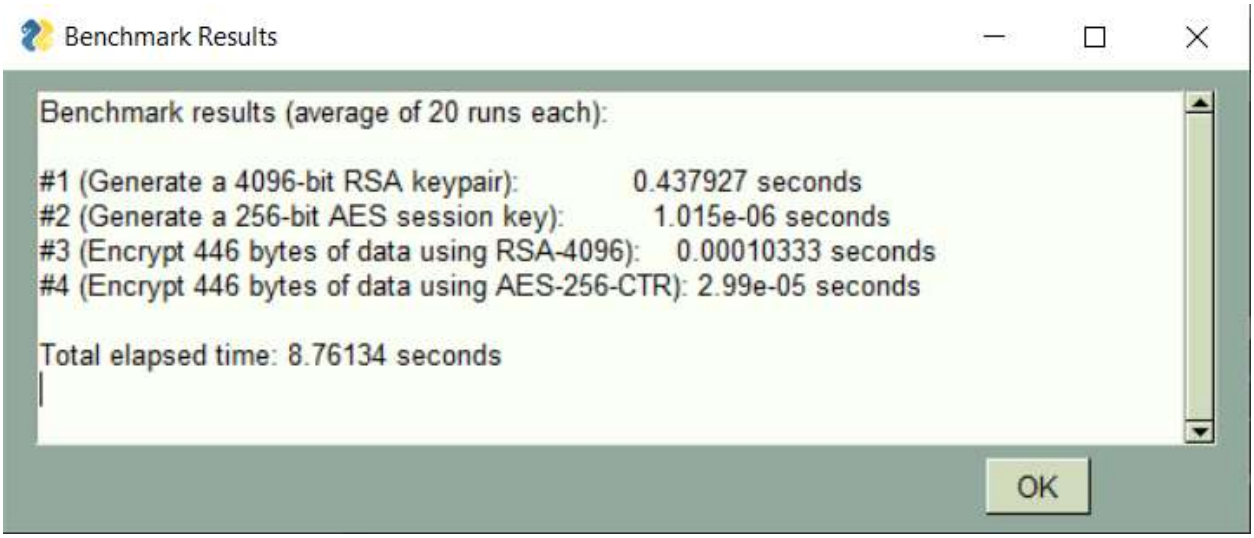
Bryce Behr, Thomas Hutchins, Christopher Tziovannis

COMP 448 – Project 3 Report

11/17/2023

The results of our project are as follows. Generating a 4096-bit RSA keypair took 0.437927 seconds. Generating a 256-bit AES session key took 1.015e-06 seconds. Encrypting 446 bytes of data using RSA-4096 took 0.00010333 seconds. Encrypting 446 bytes of data using AES-256-CTR took 2.99e-05 seconds.



The clearest takeaway from these results is that RSA is a much slower algorithm than AES. Both encryption and generating a key took significantly longer for RSA. On such a small scale the difference is almost negligible, but when you're talking about large-scale network communications, the difference would be extremely significant. Given these results, it makes sense that most real-world systems utilize "hybrid encryption." Generally, RSA is used to encrypt session keys upfront, and then faster algorithms like AES are used to encrypt the bulk of the message. This means that RSA is only needed a limited number of times to initialize the session. This approach allows industry professionals to take advantage of the strength and security that RSA provides while also mitigating the slow speeds through the use of faster algorithms such as AES.