SSN Lab Assignment:

RSA

RSA was first described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, or asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. Many protocols like SSH, OpenPGP, S/MIME, and SSL/TLS rely on RSA for encryption and digital signature functions. It is also used in software.

Programs—Browsers are an obvious example of establishing a secure connection over an insecure network like the Internet or validating a digital signature.

RSA signature verification is one of the most commonly performed operations in IT.

1. Create a 2048-bit RSA key pair using OpenSSL. Write your full name in a text file and encrypt it with your private key. Using OpenSSL, extract the public modulus and the exponent from the public key. Publish your public key and the base64-formatted encrypted text in your report. Verify that it is enough for decryption.

Hint: study OpenSSL params and encryption vs. verification vs decryption vs. signing

2. Assuming that you are generating a 1024-bit RSA key and the prime factors have a 512-bit length, what is the probability of picking the same prime factor twice?

Explain your answer

Hint: How many primes with length of 512bit or less exist?

3. Explain why using a good RNG is crucial for the security of RSA. Provide one reference to a real-world case where a poor RNG leads to a security vulnerability.

4. Here, you can find the modulus (public information) of two related 1024bit RSA keys. Your keys are numbered using the list. Your task is to factor them i.e. retrieve **p** and **q**. You may use any tools for this. Explain your approach.
Hints: study the RSA algorithm. What private information can two keys share? What practical attacks exist? You may have to write or use existing code for simple arithmetic operations. Be careful with bigInt values!

5. Now that you have the p and q for both keys, recreate the first public and private key using this script. Encrypt your name with the private key, and post the public key and the base64-formatted encrypted data in your report.