SSN Lab Assignment: RSA

A. Bakker J. van der Ham U. Seddigh M. Pouw*

Feedback deadline:
September 28, 2017 10:00 CET

1 RSA

1. Create a 2048bit 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 encrypted text on your wiki page.

2. Assuming that you are generating a 1024bit RSA key and the prime factors have a 512bit length, what is the probability of picking the same prime factor twice ? Explain your answer. *Hint: How many primes with length 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 lead to a security vulnerability.

2 Optional

4. Here you can find the modulus (public information) of two **related** 1024bit RSA keys. Your keys are numbered using the list at `https://homepages.staff.os3.nl/~mick/ssn/`.

   Your task is to factor them i.e. retrieve p an 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 code or use existing code for simple arithmetic operations.*

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 encrypted data on your wiki.

*mick@os3.nl