RSA Encryption Algorithm

Additional Resources	https://www.di-mgt.com.au/rsa_alg.html
Author	Ansh Chandnani
Understanding Level	5

Summary

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone.

7 Steps of RSA

1. Select two prime numbers p and q where p < q
2. Calculate modulus (n)

$$n = p \cdot q$$

3. Calculate Euler Phi function { phi(n) }

$$\phi(n) = (p-1)(q-1)$$

4. Calculate public exponent (e)

$$'e' \; is \; a \; random \; integer \; such \; that,$$
$$(i) \; 1 < e < \phi$$
$$(ii) \; GCD(\phi, e) = 1$$

5. Calculate number 'd'

$$d \equiv e^{-1} \cdot mod(\phi(n))$$

An easier way to calculate 'd' is:

$$d = \frac{1 + mod(\phi(n))}{e}$$

$$\Rightarrow d = \frac{1 + k \cdot \phi(n)}{e}\ ,\ where\, 0 \leq k \leq e\ such\ that\ d\ is\ a\ whole\ number$$

Now, our public key is (e, n) and private key is (d, n)

6. Encryption formula:

$$C = M^{\,e}\ \%\, n$$

7. Decryption formula:

$$M = C^{\,d}\ \%\, n$$

NOTE:

1. GCD() refers to the Greatest Common Divisor Function.
2. mod() is different from the % mod function used in Python.
3. In real scenarios p and q are very large primes with the same number of digits. For the purpose of this tool and mental calculations, we shall restrict ourselves to relatively small primes.
4. M refers to Message, and C refers to Ciphertext and both are decimal encoded.

Additional References:

1. https://www.di-mgt.com.au/rsa_alg.html