RSA digital signature – documentation

Maciej Marcinkiewicz, Katarzyna Bielecka

January 20, 2022

1 Description of the used algorithm

RSA (Rivest-Shamir-Adleman) is a public key cryptosystem, which was invented in 1977. It is not the newest one but it is still commonly used for securing data transmisson. It can be used both for encryption as well as for digital signatures. In general, it makes use of the integer factorization problem, which in number theory is the decompositio of a composite number into a product of smaller integers. In case of these integers being prime it is then called prime factorization.

2 Fuctional description of the application

The RSA cryptosystem application provides the following functionalities: public and private key generation, digital signature generation and signature verification. Below, algorithms needed for each of those functionalities are described.

2.1 Keys generation

1. Generate two random, large prime numbers **p** and **q**
2. Compute $n = p * q$ and $\phi = (p-1) * (q-1)$
3. Find **e**, such that $1 < e < \phi$ and $\gcd(e, \phi) = 1$
4. Using the extended Euclidian algorithm produce a unique **d**, such that $1 < d < \phi$ and $e * d \equiv 1 (\text{mod } \phi)$
5. (n,e) is the resulting public key and d is the private key

2.2 Signature generation

1. Compute $h = sha512(m)$ where **h** is the hash of the message **m**
2. Compute $s = h^d \pmod n$
3. **s** is the generated signature

2.3 Signature verification

1. Compute $\tilde{h} = s^e \pmod n$
2. Compute $h =$sha512 (m) where **h** is the hash of the message **m**
3. If $\tilde{h}$ is equal to h then the signature is valid

3 Description of designed code structure

4 Tests

5 Bibliography

1. Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. (October 1996). Handbook of Applied Cryptography, Chapter 8

2. `https://en.wikipedia.org/wiki/RSA_(cryptosystem)`