RSA digital signature – documentation

Maciej Marcinkiewicz, Katarzyna Bielecka

January 19, 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

3 Description of designed code structure

4 Tests