### Definition: Gaussian Bracket

This function is also called floor function. It is named after the mathematician Carl Friedrich Gauss.

The Gaussian brackets thus calculates the largest integer less than or equal to x x for a real number .

Example: Gaussian bracketDefinition: Modulo1.2.3.4.5. ⌊3.3⌋ = 3⌊14⌋ = 14⌊−4.6⌋ = −5⌊1234,9876⌋ = 1234⌊−76.1⌋ = −77.. . . .

For The definition looks more complicated than it actually is. The modulo function calculatesa mod ba ∈ ℤ is read “ and b ∈ ℤ \ {0}a modulo b. we define the modulo function ” amodb: = a− ba ·b mod : ℤ × (ℤ \ {0}) → ℤ by

nothing more than the remainder of the division Example: Modulo a divided by b.

Generation of the Key Pair2.4.1.3. 7It is 631 mod 5 = mod 3 = mod 6 = 3181 mod 7 = − 81776316−−20·7 = 81, because, because1·6 = 31, because7536 4·5 = 7·3 = 6, because−−11.571−−5.1661.42 ……·3 = 6·5 = 7 ·6 = 31·7 = 81−−2·3 = 61·5 = 7−−11·7 = 815·6 = 31−−6 = 05 = 2−−30 = 177 = 4

81−

Before we can encrypt messages with the RSA algorithm, we must first generate a key pair

consisting of a public and private key. To this end we proceed as follows:1.2. We randomly choose two prime numbers We calculate the product of the two prime numbers module. p and q with M := p · q.p ≠ q. We call M the RSA

3.We calculate Euler’s p − 1) · (q − φ function of M. Because Mφ( is a product of prime numbers andM) = φ(p · q) = φ(p) · φ(q) gcd(e,=

Euler’s φ function is multiplicative it applies that 1) φ(M) 1 < e < φ(Mφ(M)|(1 − ed(d, M) )) p

.

with . Thus

.

, thus . For this we

. The private key is the tuple . The numbers ,

the key pair has been generated and can be Example: Generation of a key pair

1. We choose the primes p := 11 and q := 13. In practice, we should choose the primes Let us proceed as described above:

as large as possible (because the larger the primes are, the more difficult the encryption is to crack). In this example, we will content ourselves with small numbers for the sake of clarity.

5. Now we use the extended Euclidean algorithm to determine the number φ(M) = 1 − ed.

we proceed as follows: It must apply that

Because of the choice of . We can put this in ed+x·φeM = 1 =φ(M) and getgcd23,120e,φx M

By inserting the values for d·23+x·120 = gcd and the following equation is obtainedd

We can now determine the values for and with the extended Euclidean algorithm. To do this, we apply the Euclidean algorithm to the numbers 23 and 120 and initially obtain the following equations:

We continue following the lemma of Bézout and rearrange the equations according to120=5·23+523=4·5+35=1·3+23=1·2+12=2·1+0 the remainders:Now we successively insert the equations into each other, starting with the last one:3 = 232 = 51 = 35 = 120−−−1·31·2−4·55·23

The numbers we are looking for are further interest.1==23==23=23=23323−−−−−−−−1·24·120+20·234·14·120+20·234·120+20·234·4·120+20·234·120+20·234·512−20+20·230−9−1··1205·523−−−−−−−1·3−5·1·1·1·1·1·1·111205·12012012020+26·2320120−−−−d := 47−5·235·235·235·23−5·2326·23−−−− and 1·21·1·−11··x := −9232321·2323+4·12023−−4·4·120+2−−4·5, but the number 124·1200−5·230·23 x is of no

=47·23+=23=23=23−

Now that we have generated the key pair, we can announce the public key. We keep the6. (We thus obtain as public key the tuple d, M) = (47, 143). (e, M) = (23, 143) and as private key the tuple

private key secret. In the following we will look at how these keys can be used to encrypt and decrypt messages using the RSA method.