Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Monitor, drinnen enthält.

Automatisch generierte Beschreibunga)Nach meiner Funktion ist g eine Primitivwurzel

b)

g^a mod p= 5^7 mod 23

7 binär= 111

5^0=1

5^1= 1\*1\*5=5

5^10=5\*5=25 mod 23=2

5^11=2\*5=10

5^110=10\*10=100 mod 23=8

5^111=8\*5=40 mod 23= 17

Alice verschickt 17

B=20

G^a mod p)^b mod p= g^ab mod p = K

5^(20\*7) mod 23 = 5^140 mod 23

Satz von Euler

Phi(23)=22

5^140=5^22 \* 5^22 \*5^22 \*5^22\*5^22\*5^22 \*5^8=5^8 mod 23

8=1000

5^0=1

5^1=5

5^10=5\*5=25 mod 23 = 2

5^100=2\*2= 4

5^1000=4\*4=16 mod 23

K=16

5^20 mod 23

20=10100

5^1=5

5^10=25 mod 23=2

5^101= 2\*2\*5= 20

5^1010=400 mod 23 = 9

5^10100= 9\*9 = 81 mod 23 = 81 -69= 12

Bob sendet 12

c)

mA=6

5^6 mod 23

5^110 mod 23

5^1=5

5^10=5\*5mod 23= 2

5^11=10

5^110=100 mod 23=8

An Alice 8

mB=4

5^4 mod 23

4=100

5^1=5

5^10=25 mod 23 =2

5^100=4

An Bob 4

Alice

Kam=g^am mod p

=5^7\*6 mod 23= 5^42 mod 23

42=101010

5^1=5

5^10=2

5^100=4

5^101=20

5^1010=400=9

5^10100=81 mod 23= 81 -69= 12

5^10101=60 mod 23 = 14

5^101010=196 mod 23=8

Kam = 8

Kbm= g^bm mod p= 5^20\*4 mod 23

5^80 mod 23= 5^22\*5^22 \*5^22 \*5^14 mod 23= 5^14 mod 23

14= 1110

5^1=5

5^11= 5\*5\*5= 10

5^110=100 mod 23 = 8

5^111= 8\*5 = 40 mod 23 = 17

5^1110= 17\*5= 50 +35 = 85 mod 23 =13

Kbm= 13

