M = bericht dat je versleutelt

M < m

P, Q priemgetallen gekozen

m = P . Q

K = (P-1)\*(Q-1)

e = random gekozen getal dat voldoet aan onderstaande voorwaarde

e < K en gcd(e,K) = 1

{gcd,d,j}:=gcdext(e,K)

d > 0

als d < 0 dan => d + K

Uitleg

Als je gaat versleutelen moet je altijd hier aan denken. De sleutels komen altijd van voor wie het bericht is. Dus stel dat persoon A iets wilt sturen naar persoon B dan zal enkel de KEYs van persoon B gebruikt worden. Eerst de publieke door persoon A voor het versleutelen. En daarna de private voor het decrypteren.

Als iemand iets wilt handteken dat volgt dit het zelfde principe als een handtekening die je op papier zet. Eigenlijk jij mag deze gebruiken dus .. private key van jezelf. Als de andere gebruiker wilt kijken of het echt van jou is kan die jou publieke key gebruiken om dit zeker te weten.

Als je wilt versleutelen en handtekenen moet je dit altijd doen op de zelfde manier. Dus eerst moet je de boodschap handtekenen en daarna moet je deze versleutelen. Als daarna de andere gebruiker deze wilt lezen moet hij eerst deze decoderen en daarna de inverse van de handtekening hier op toe passen.

Voorbeeld

Twee personen willen communiceren A en B

Persoon A wilt een bericht versleutelen zodat enkel persoon B dit kan lezen.:

S(M)=mod(M^e(vanB),m(vanB))

Als Persoon B de gedecodeerde boodschap wilt decoderen van A

M=mod(S(M)^d(vanB),m(vanB))

Als Persoon A een gehand tekende, niet vercijferde boodschap verstuurt naar Persoon B

H(M) = mod(M^d(vanA),m(vanA))

Als Persoon B zeker wilt zijn dat het bericht van Persoon A komt.

M=mod(H(M)^e(vanA),m(vanA))

Als Persoon A een gehand tekende boodschap wilt handteken en versleutelen en versturen naar Persoon B

H(M) = mod(M^d(vanA),m(vanA))

S(H(M))=mod(H(M)^e(vanB),m(vanB))

Als Persoon B dit wilt lezen en zeker wilt zijn dat het bericht van persoon A komt.

H(M)=mod(S(H((M))^d(vanB),m(vanB))

M=mod(H(M)^e(vanA),m(vanA))