RSA

Es waren einmal Alice und Bob und sie wollen sich Nachrichten schicken, die niemand ausser ihnen

Schlüsselerzeugung

Alice erzeugt sich ein Paar von RSA Schlüsseln P_A und S_A.

In[27]:=
```
p = Prime[1000]
```

Out[27]=
```
7919
```

In[28]:=
```
q = Prime[1001]
```

Out[28]=
```
7927
```

In[29]:=
```
n = p * q
```

Out[29]=
```
62773913
```

$m = \varphi(n)$

In[8]:=
```
m = (p - 1) (q - 1)
```

Out[8]=
```
62758068
```

Offentlicher Schlüssel von Alice

$e_A = 5$ –ggT$(e_A, m) = 1$

```
eA = 5;
GCD[eA, m]
```

Out[12]= 1

Öffentlicher Schlüssel $P_A = (5,\ 62773913)$

In[19]:=
```
PA[l_List] := PowerMod[#, 5, 62773913] & /@ l
```

Privater Schlüssel von Alice

Bestimme ein d_A mit $5\, d_A \equiv 1 \bmod 62758068$

```
dA = PowerMod[5, -1, 62758068]
```

Out[16]= 37654841

Privater Schlüssel $S_A = (37654841,\ 62773913)$

In[25]:=
```
SA[l_List] := PowerMod[#, 37654841, 62773913] & /@ l
```

Verschlüsselung

Bob schickt eine Nachricht an Alice:

In[18]:=
```
M = {11111, 22222, 33333, 44444, 55555};
```

Er verschlüsselt M mit dem öffentlichen Schlüssel von Alice(!):

In[23]:=
```
M_C = P_A [M]
```

Out[23]=
```
{32436701, 33591824, 35379218, 7781847, 47595043}
```

... und schickt M_C zu Alice.

Entschlüsselung

Alice wendet ihren privaten Schlüssel auf die empfangene Nachricht an:

In[26]:=
```
S_A [M_C ]
```

Out[26]=
```
{11111, 22222, 33333, 44444, 55555}
```

... und voila.

Signaturen

Bob erzeugt sich eigene RSA Schlüsseln. Er benutzt dieselben Primzahlen p und q wie Alice.

Offentlicher Schlüssel von Bob

$e_B = 7$ –ggT$(e_B, m) = 1$

In[32]:=
```
eB = 7;
GCD[eB, m]
```

Out[33]=
```
1
```

Öffentlicher Schlüssel $P_B = (7,\ 62773913)$

In[34]:=
```
PB[l_List] := PowerMod[#, 7, 62773913] & /@ l
```

Privater Schlüssel von Bob

Bestimme ein d_B mit $7\, d_B \equiv 1 \bmod 62758068$

In[35]:=
```
dB = PowerMod[7, -1, 62758068]
```

Out[35]=
```
26896315
```

Privater Schlüssel $S_B = (26896315,\ 62773913)$

In[36]:=
```
SB[l_List] := PowerMod[#, 26896315, 62773913] & /@ l
```

Verschicken von signierten Nachrichten

Bob schickt eine Nachricht an Alice:

In[18]:=
```
M = {11111, 22222, 33333, 44444, 55555};
```

Bevor er die Nachricht M mit dem öffentlichen Schlüssel von Alice verschlüsselt, wendet er auf M s

In[38]:=
```
M1 = SB[M]
```

Out[38]=
```
{61314990, 21744015, 29616562, 50841207, 55828570}
```

Jetzt wird M_1 verschlüsselt und verschickt.

In[39]:=
```
MS = PA[M1]
```

Out[39]=
```
{22494386, 25218070, 5553556, 51390317, 15520865}
```

Alice empfängt M_S und entschlüsselt sie mit ihrem privaten Schlüssel.

In[40]:=
```
M2 = SA[MS]
```

Out[40]=
```
{61314990, 21744015, 29616562, 50841207, 55828570}
```

Nun wendet sie den öffentlichen Schlüssel von Bob auf M_2 an.

In[41]:=
```
PB[M2]
```

Out[41]=
```
{11111, 22222, 33333, 44444, 55555}
```

Weil der öffentliche Schlüssel von Bob nur solche Nachrichten entschlüsseln kann, die mit seinem p
stammen.

Ende der Geschichte.