Diffie-Hellman-Schlüsselvereinbarung

Mathematik in wxMaxima www.mathematik-verstehen.de Haftendorn Dez 2010

0.1 Handlinghilfen

0.2 Inhalt

1 Erzeugung des gemeinsamen Schlüssels

1.1 Verabredung der Grundlagen

Anton und Berta verabreden (offen) eine Primzahl p und eine kleinere Zahl g.

```
(%i39) p:next_prime(floor(sqrt(random(1.0)*10^160)));
       10^80;
(%o39)
```

473206942458495324844253704522061231690708409050224535784747869678338502998098 13

```
(%o40)
```

100000000000000000000000000000000000000000000000000000000000000000000000000000

```
(%i41) g:random(p);
(%o41)
```

816918886473814338162317583661407558081207182977026068319417709920724173832800 2

1.2 Jeder für sich erzeugt seine geheime Zahl

```
(%i42) anton:random(p); berta:random(p);
(%o42)
```

215344004239156190501696506656886025968085498485041035972393866368754754057185 76

```
(%o43)
```

103935771765721183736517222444270612425557901347277477762139577549165590688718 89

1.3 Jeder schickt dem Anderen seine Potenz von g

```
(%i44) alpha:power_mod(g,anton,p); beta:power_mod(g,berta,p);
(%o44)
```

348693653238911581396198026529428614872694327688553643254755288645138949876882 42

```
(%o45)
```

387743176219856954155237699992973040475775214669301206710101392206113813046577 98

1.4 Jeder potenziert das Empfangene

(%i46) ka:power_mod(beta,anton,p); kb:power_mod(alpha,berta,p);
(%o46)
30288356098560821992886662354555040567693500578619527555329382163073934585374444
(%o47)
30288356098560821992886662354555040567693500578619527555329382163073934585374444

Nun haben beide denselben Schlüssel, nämlich ka=kb.

2 Hilfsfunktionen

3 Symmetrische Kommunikation mit One-time-pad

3.1 Verschlüsseln mit One-time-pad und gemeinsamem Schlü

Anton will eine Nachricht an Berta senden

(%i56) m:txToZoo("Wollen wir Weihnachten Skifahren?");
[87,111,108,108,101,110,32,119,105,114,32,87,101,105,104,110,97,99,104,116,101,110
,32,83,107,105,102,97,104,114,101,110,63]
[59,83,80,80,73,82,4,91,77,86,4,59,73,77,76,82,69,71,76,88,73,82,4,55,79,77,74,69,
76,86,73,82,35]
(%o56) 59838080738204917786045973777682697176887382045579774697686738235

(%i57) m;ka;
(%o57) 59838080738204917786045973777682697176887382045579774697686738235
(%o58)
30288356098560821992886662354555040567693500578619527555329382163073934585374444

Nun werden die Nachricht m und der Schlüssel ka ziffernweise modulo 10 addie

(%i59) c:otp_en(m,ka);
(%o59) 89016336726764738678821535021137637633470882513188294914087955986 5

Dieses c sendet Anton an Berta

3.2 Entschlüsselung nit One-Time-Pad und gemeinsamem Sch

Berta erhält von Anton das c

(%i60) c; kb;
(%o60) 89016336726764738678821535021137637633470882513188294914087955986 5
(%o61)
30288356098560821992886662354555040567693500578619527555329382163073934585374444

Berta zieht nun Ziffernweise von links modulo 10 von c den Schlüssel ab.

(%i62) mm:otp_de(c,ka);
(%o62) 59838080738204917786045973777682697176887382045579774697686738235

```
(%i63) zooToTx(mm);
[59,83,80,80,73,82,4,91,77,86,4,59,73,77,76,82,69,71,76,88,73,82,4,55,79,77,74,69,
76,86,73,82,35]
[87,111,108,108,101,110,32,119,105,114,32,87,101,105,104,110,97,99,104,116,101,110
,32,83,107,105,102,97,104,114,101,110,63]
(%o63) Wollen wir Weihnachten Skifahren?
```

4 Angriffe

```
(%i73) /* bis 10000 dauert 8 sec bei p 80 Stellen*/
       block( for  i:1 thru 100 do( a:random(p),
                                    if power_mod(g,random(p),p)=alpha then print( a, " gefunden") ),
                                    print( " Pech, nicht gefunden"))$
Pech, nicht gefunden
```