Diffie-Hellman-Angriff, p etwa 100

Diffie-Hellman Angriff Haftendorn 2013 (15), www.mathematik-verstehen.de

p:=101 ▸ 101 gefunden durch kry\nextprime(100) ▸ 101

g:=83 ▸ 83 Anton wählt a:=59 ▸ 59 Berta wählt b:=41 ▸ 41

Anton: alpha:=kry\pmod(g,a,p) ▸ 99 Berta: beta:=kry\pmod(g,b,p) ▸ 50

Anton: kry\pmod(beta,a,p) ▸ 29 Berta: kry\pmod(alpha,b,p) ▸ 29

****

Mister X fängt ab: p ▸ 101 g ▸ 83 alpha ▸ 99 beta ▸ 50

Er muss dazu unter den Potenzen von g diejenigen suchen, die alpha oder beta ergeben.

Er braucht nur eine solche Lösung von g^{x1}=**alpha** ▸ $83^{x1}=99$ oder von g^{x2}=**beta** ▸ $83^{x2}=50$

Siehe die Visualisierung dieser Fragestellung mit der gewöhnlichen Exponentialfunktion an.

Die Lösungen kann man in den Ganzen Zahlen nicht gebrauchen.

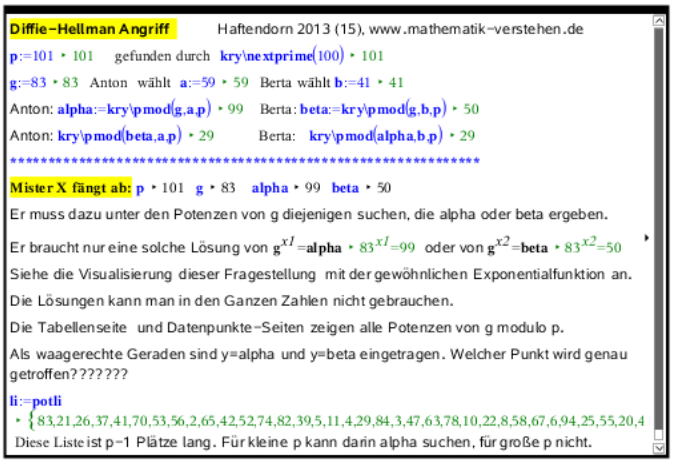
Die Tabellenseite und Datenpunkte-Seiten zeigen alle Potenzen von g modulo p.

Als waagerechte Geraden sind y=alpha und y=beta eingetragen. Welcher Punkt wird genau getroffen??????

li:=potli

▸ {83,21,26,37,41,70,53,56,2,65,42,52,74,82,39,5,11,4,29,84,3,47,63,78,10,22,8,58,67,6,94,25,55,20,4

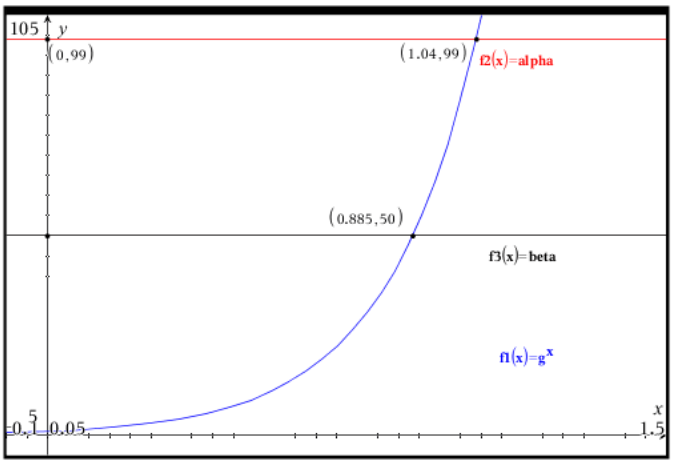
Diese Liste ist p-1 Plätze lang. Für kleine p kann darin alpha suchen, für große p nicht.

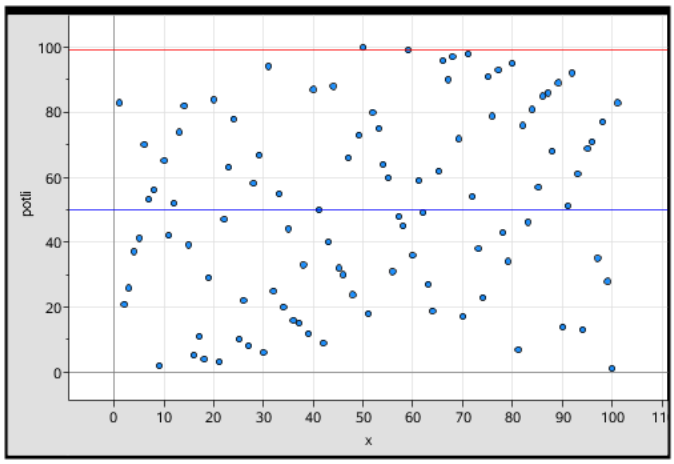


Mister X kennt: p,g,alpha,beta

Wenn er dann **a** durch Suchen herausbekommt, kann er **beta**^{a} rechnen und hat **k**

Wenn er dann **b** durch Suchen herausbekommt, kann er **alpha**^{b} rechnen und hat **k**





	A x	B potli	C	D	E	F	G
=	=seq(i,i,1,'						
1	1	83					
2	2	21					
3	3	26					
4	4	37					
5	5	41					
6	6	70					
7	7	53					
8	8	56					
9	9	2					
10	10	65					
11	11	42					

A x:=seq(i,i,1,'p)

Diffie-Hellman-Angriff, p etwa 1000

Diffie-Hellman Angriff Haftendorn 2013(15), www.mathematik-verstehen.de

p:=1117 gefunden durch kry\nextprime(1111) ▸ 1117

g:=787 Anton wählt a:=159 ▸ 159 Berta wählt b:=741 ▸ 741

Anton: alpha:=kry\pmod(g,a,p) ▸ 974 Berta: beta:=kry\pmod(g,b,p) ▸ 413

Anton: kry\pmod(beta,a,p) ▸ 598 Berta: kry\pmod(alpha,b,p) ▸ 598

****

Mister X fängt ab: p ▸ 1117 g ▸ 787 alpha ▸ 974 beta ▸ 413

Er muss dazu unter den Potenzen von g diejenigen suchen, die alpha oder beta ergeben.

Er braucht nur eine solche Lösung g^{x1}=**alpha** ▸ $787^{x1}=974$ oder von g^{x2}=**alpha** ▸ $787^{x2}=974$

Siehe die Visualisierung dieser Fragestellung mit der gewöhnlichen Exponentialfunktion an.

Die Lösungen kann man in den Ganzen Zahlen nicht gebrauchen.

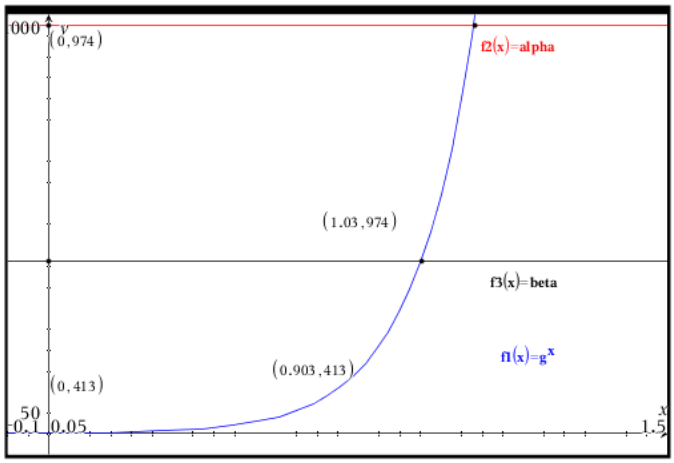
Die Tabellenseite und Datenpunkte-Seiten zeigen alle Potenzen von g modulo p.

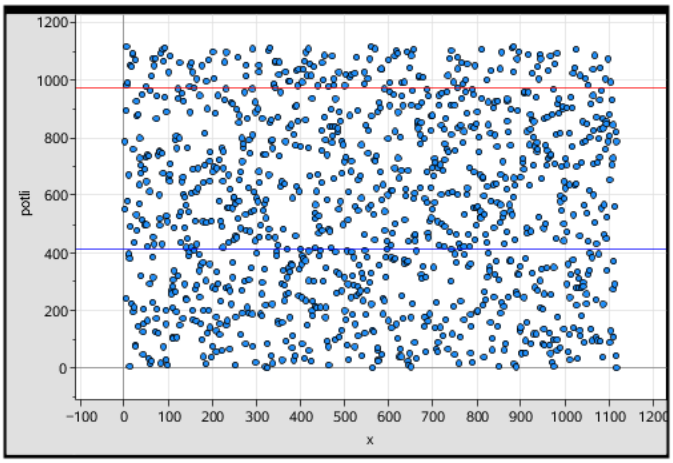
Als waagerechte Geraden sind y=alpha und y=beta eingetragen. Welcher Punkt wird genau getroffen??????

li:=potli

▸ {787,551,241,894,985,1114,990,581,394,669,396,9,381,491,1052,227,1046,1090,1091,761,195,436,

Diese Liste ist p-1 Plätze lang. Für kleine p kann darin alpha suchen, für große p nicht.





	A x	B potli	C	D	E	F	G
=	=seq(i,i,1,'						
1	1	787					
2	2	551					
3	3	241					
4	4	894					
5	5	985					
6	6	1114					
7	7	990					
8	8	581					
9	9	394					
10	10	669					
11	11	396					

x:=seq(i,i,1,'p)

Diffie-Hellman-Angriff, p etwa 10000

Diffie-Hellman Angriff Haftendorn 2013 (15), www.mathematik-verstehen.de

p:=10007 ▸ 10007 gefunden durch kry\nextprime(10000) ▸ 10007

g:=6784 ▸ 6784 Anton wählt a:=2169 ▸ 2169 Berta wählt b:=5741 ▸ 5741

Anton: alpha:=kry\pmod(g,a,p) ▸ 9088 Berta: beta:=kry\pmod(g,b,p) ▸ 7100

Anton: kry\pmod(beta,a,p) ▸ 1301 Berta: kry\pmod(alpha,b,p) ▸ 1301

****

Mister X fängt ab: p ▸ 10007 g ▸ 6784 alpha ▸ 9088 beta ▸ 7100

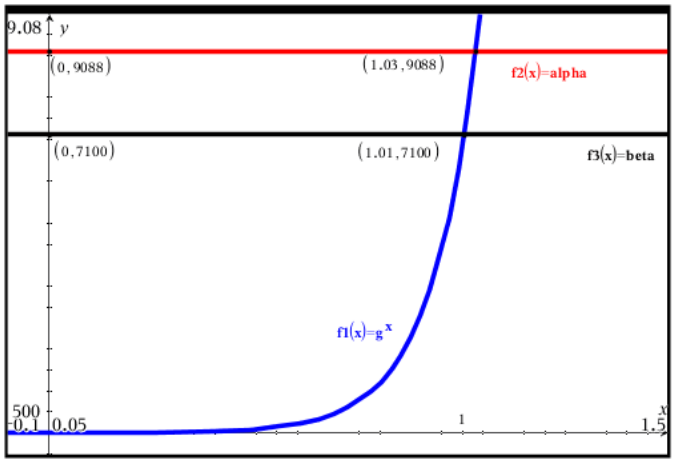
Er muss dazu unter den Potenzen von g diejenigen suchen, die alpha oder beta ergeben.

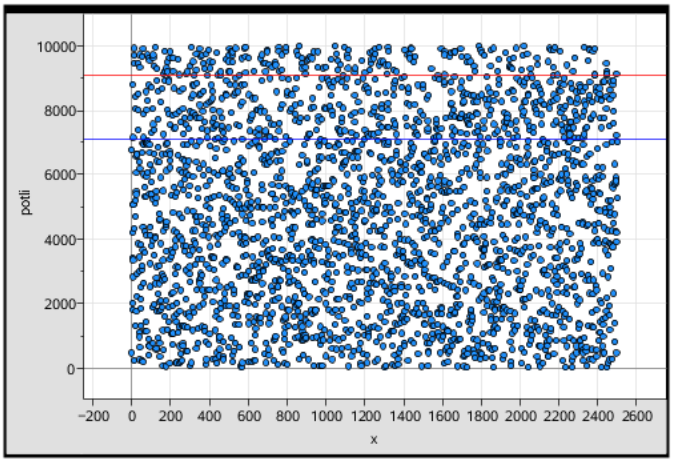
Er braucht nur eine solche Lösung g^{x1}=alpha ▸ 6784^{x1}=9088 oder g^{x2}=alpha ▸ 6784^{x2}=9088
Siehe die Visualisierung dieser Fragestellung mit der gewöhnlichen Exponentialfunktion an.
Die Lösungen kann man in den Ganzen Zahlen nicht gebrauchen.

Die Tabellenseite und Datenpunkte-Seiten zeigen nicht allePotenzen von g modulo p,
denn die Tabellen beim TI haben nur bis 2500 Plätze. Das ist nur etwa ein Viertel der Potenzen.

Als waagerechte Geraden sind y=alpha und y=beta eingetragen. Welcher Punkt wird genau getroffen??????? Mit diese Einschränkung hätte a gerade noch gefunden weren können.

Porbe: potli[2169] ▸ 9088 Man hätte eine Prozedur haben müssen, die die Liste durchforstet.





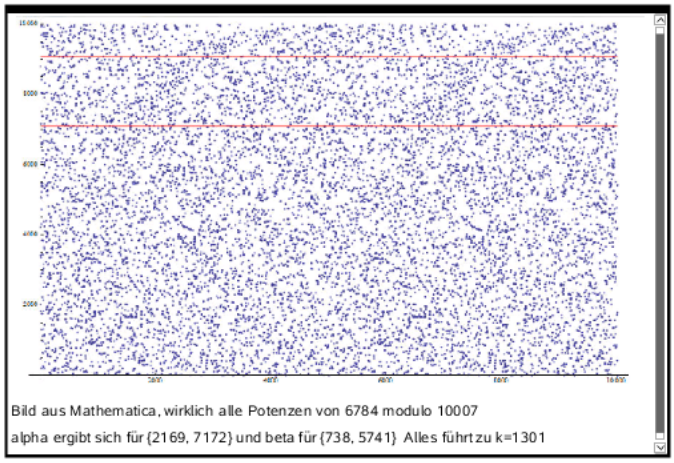


Bild aus Mathematica, wirklich alle Potenzen von 6784 modulo 10007

alpha ergibt sich für {2169, 7172} und beta für {738, 5741} Alles führt zu k=1301

		B potli	C	D	E	F	G
=	eq(i,i,1,'						
1228	1228	4229					
1229	1229	9474					
1230	1230	6662					
1231	1231	3396					
1232	1232	2350					
1233	1233	1249					
1234	1234	7294					
1235	1235	7888					
1236	1236	4763					
1237	1237	9596					
1238	1238	3729					

x:=seq(i,i,1,'p)