Übersicht RSA-Verschlüsslung:

von Alexander Ziebolz

Verschlüsslung (engl. cypher):
M^e mod N =C

Entschlüsslung (engl. decypher):
C^d mod N = M

Variable:	Bedeutung:	Bekanntheit:
M (engl. Message)	= Die Nachricht im Klartext	dem Sender und nach dem entschlüsseln auch dem Empfänger bekannt
C (engl. Cypher)	= Die Verschlüsselte Nachricht	allen bekannt
N	= Öffentliches Schloss (Teil des *public keys*)	allen bekannt
e	= (halb) öffentlicher Schlüssel zum codieren (encrypt)	allen bekannt
p, q	= zwei sehr große Primzahlen bilden durch ihr Produkt N	*NUR* dem Empfänger bekannt, da er N und e zur Verfügung stellt, um N zu errechnen sind sie nötig
d	= privater Schlüssel (*private key*)	nur dem Empfänger bekannt, da er auch als Einziger p und q kennt, aus denen sich d errechnet, siehe unten.

Einige notwendige Eigenschaften von e:

Damit das ganze funktioniert, müssen einige Bedingungen erfüllt sein:

a) e muss eine Primzahl sein
b) 1<e<N
c) p # e; q # e
d) z ist nicht durch e Teilbar, wobei z = (p-1)(q-1) ist

Errechnen von d inklusive Beispiel:

d errechnet sich aus der Folgenden Formel:

e*d mod (q-1)(p-1) = 1

Diese lässt sich auf ed mod z = 1 vereinfachen.
Da p und q bekannt sind, ist auch z bekannt (z = (q-1)(p-1), e ist jedem bekannt. Allerdings kann man damit noch nicht d errechnen, allerdings kann diese Formel später zur Probe dienlich sein, um d zu errechnen braucht man eine andere Formel:

$\frac{k*z+1}{e} = d$ wobei k eine grade Zahl der Wahl ist.

Um nun d zu errechnen setzt man beliebige Zahlen für k ein und das erste Ergebnis, bei dem bei der Rechnung X mod e = 0 wobei X das Ergebnis von k*z+1 ist, ist auch d.

Beispielaufgabe zur Errechnung von d:

p sei 3
q sei 5
e sei 7

7*d mod (3-1)(5-1) = 1
7d mod 8 = 1

k: z: X: x mod e = 0? (x mod 7 = 0)

2 * 8 + 1 = 17 falsch
3 * 8 + 1 = 25 falsch
4 * 8 + 1 = 33 falsch
5 * 8 + 1 = 41 falsch
6 * 8 + 1 = 49 wahr

X: e: d:
49 / 7 = 7
d = 7

zur Probe:

7*7 mod 8 = 1
49 mod 8 = 1 wahr

Das d hier gleich e ist, liegt an der Wahl so kleiner Zahlen und ist keinesfalls immer so

Knacken:

Jetzt wo wir wissen wie man d berechnet möchten wir natürlich auch Nachrichten lesen können, die nicht für uns bestimmt sind, das N und e bekannt sind müssen wir prinzipiell also nur die beiden Primzahlen p und q herausfinden, die geht wie folgt:
Man nimmt die Wurzel von N und teilte diese durch sämtlich Primzahlen, die kleiner sind als die Wurzel (ohne Runden!).

Beispiel:

N sei 143:

$\sqrt{N}$ = 11,958

143 / 2 = 71,5 Nicht Prim
143 / 3 = 47,666666 Nicht Prim
143 / 5 = 28,6 Nicht Prim
143 / 7 = 20,428571 Nicht Prim
143 /11 = 13 Prim p und q gefunden

p ist also 11 und q 13, die Probe belegt, dass der Code geknackt wurde: 11*13 = 143

Komplette Kodierung und Dekodierung als Beispielaufgabe:

p sei 11
q sei 5
e sei 3
M sei Die Russen kommen

Als aller erstes wird der Text per ASCII in Zahlen umgewandelt, an dieser Stelle sei auch noch einmal ein Ausschnitt der ASCII Tabelle eingefügt:

A=65	F=70	K=75	P=80	U=85	Z=90
B=66	G=71	L=76	Q=81	V=86	
C=67	H=72	M=77	R=82	W=87	
D=68	I=73	N=78	S=83	X=88	
E=69	J=74	O=79	T=84	Y=89	

Nun zerlegen wir unsere Botschaft in ASCII-Code

D I E R U S S E N K O M M E N
68 73 69 82 85 83 83 69 78 75 79 77 77 69 78

Nun teilen wir den Code in Dreierblöcke auf:

687 369 828 583 836 978 757 977 776 978

Nun erfolgt das Verschlüsseln mit der Rechnung M^e mod N = C, indem wir für M die Dreierblöcke, für 3 (gewähltes e) und für N 11*5=55 (gewählt p und q ergeben multipliziert N) einsetzen:

687^3 mod 55 = C
32424203 mod 55 = 48

369^3 mod 55 = C
50243409 mod 55 = 29

828^3 mod 55 = C
567663552 mod 55 = 27

583^3 mod 55 =C
198155287 mod 55 = 22

836^3 mod 55 = C
584277056 mod 55 = 37

978^3 mod 55 = C
935441352 mod 55 = 32

757^3 mod 55 = C
433798093 mod 55 = 3

977^3 mod 55 = C
932574833 mod 55 = 3

776^3 mod 35 = C
467288576 mod 55 = 51

978^3 mod 35 = C
935441352 mod 55 = 32

Dies ergibt dann als verschlüsselte Nachricht (C):

48 29 27 22 37 32 3 3 51 32

Nun zum Entschlüsseln, dafür müssen wir zunächst d berechnen (siehe oben):

e*d mod (p-1)(q-1) = 1
3*d mod (11-1)(5-1) = 1
3*d mod 40 = 1 (z=40)

$\frac{k*z+1}{e} = d$ -> X/e = d

k: z: X: X mod e = 0
2*40 + 1 = 81 wahr

81/3 = 27
d = 27

Probe:

3*27 mod 40 = 1
81 mod 40 = 1 wahr

Nun können wir zur Dekodierung schreiten:

C^d mod N = M

wir erinnern uns an C:

48 29 27 22 37 32 3 3 51 32

48^27 mod 55 = 687
29^27 mod 55 = 369
27^27 mod 55 = 828
22^27 mod 55 = 583
37^27 mod 55 = 836
32^27 mod 55 = 978
3^27 mod 55 = 757
3^27 mod 55 = 977
51^27 mod 55 = 776

32^27 mod 55 = 978

Das ergibt als M:

687 369 828 583 836 978 757 977 776 978

In 2er Paketen:

68 73 69 82 85 83 83 69 78 75 79 77 77 69 78 <- ASCII-Code
D I E R U S S E N K O M M E N <- Alphabet

Die Russen kommen