Vorspann

$24 \,\mathrm{MOD}\, 7 = 3 \qquad \leftarrow \text{Modul } n = 7$
Das ganze nennt man Modulare Arithmetik.
$(3 \cdot 5) \,\mathrm{MOD}\, 7 = 1$
in $\mathbb{Z}_7$ heißt das: $3 \cdot 5 = 1$
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$
$\mathbb{Z}_n$ ist ein Körper, wenn jede Zahl in der Menge mal eine beliebige Zahl aus der Menge 1 ergibt. Voraussetzung: n prim

Empfehlenswerter Link: http://www.infosecurity.org/publications.php

$5^8 = 5^2;\ 4^2;\ 2^2 = 4 \ \Leftrightarrow\ \left(\left(5^2\right)^2\right)^2$

Symmetrische Verschlüsselung:
$E(N) = N \oplus S; E(N) \oplus S = (N \oplus S) \oplus S = N \oplus (S \oplus S) = N \oplus 0 = N$
Public-Key-Verfahren

0 Einleitung

MOD über DIV

$$27 \,\mathrm{DIV}\, 7 = 3 = \left\lfloor \frac{17}{7} \right\rfloor \quad truncate$$
$$= \left\lfloor \frac{27}{7} \right\rfloor$$
$$x \,\mathrm{MOD}\, n = x - (x \,\mathrm{DIV}\, n) \cdot n$$

Wenn $x \,\mathrm{MOD}\, n$ negatives Ergebnis liefert, dann den Modul n draufaddieren.

z.B. $(-27) \,\mathrm{MOD}\, 7 = -6 \underset{+7}{=} 1$

$$(-27) \,\mathrm{MOD}\, 7 = -27 - ((-27) \,\mathrm{DIV}\, 7) \cdot 7 = -27 - \left\lfloor \frac{-27}{7} \right\rfloor \cdot 7 = -27 - \lfloor -3.8\ldots \rfloor \cdot 7 =$$
$$= -27 - (-4 \cdot 7) = 1$$

Definition:

$\forall\, x, y \in \mathbb{Z}$ gilt
$x \,\mathrm{MOD}\, n = y \,\mathrm{MOD}\, n \Leftrightarrow n \mid x - y$
man sagt dazu:

x kongruent y modulo n

i.Z. $x \equiv y \,(mod\, n)$

$x - y = c\,n, x = y + c\,n \quad c \in \mathbb{Z}$ geeignet

andere Schreibweise: $x = y$ in $\mathbb{Z}_n$
$27 = 13$ in $\mathbb{Z}_7$

Satz (o.B.) $n \in \mathbb{Z};\ n \geq 2$ (Modul)

i. $0 \leq x < n \ \Leftrightarrow\ x \operatorname{MOD} n = x$

ii. $\forall\, x \in \mathbb{Z}$ gilt $x \operatorname{MOD} n = 0 \Leftrightarrow n \mid x$

iii. $x > 0 \Rightarrow (-x) \operatorname{MOD} n = n - (x \operatorname{MOD} n)$

iv. $\forall\, x, y \in \mathbb{Z}$ gilt $(x * y) \operatorname{MOD} n = [(x \operatorname{MOD} n) * (y \operatorname{MOD} n)] \operatorname{MOD} n;\quad * \in \{+, -, \cdot\}$

1 Elementare Zahlentheorie

1.1 Teilbarkeit

Definition:

$a, b \in \mathbb{Z};$ a teilt b, i.Z. (im Zeichen) $a \mid b :\Rightarrow \exists\, c \in \mathbb{Z} : a\, c = b$
(b ist ganzzahliges Vielfaches von a, Negation: $a \nmid b$)

Definition:

$p \geq 2$ prim (ist Primzahl)
$:\Leftrightarrow (\forall\, t \in \mathbb{Z} : t \mid p \Rightarrow t = \pm 1 \vee t = \pm p) \underset{\text{o.B.}}{\Leftrightarrow} \forall\, a, b \in \mathbb{Z}\,(p \mid a\, b \Rightarrow p \mid a \vee p \mid b)$

Definition:

t heißt größter gemeinsamer Teiler von a und b
$:\Leftrightarrow t \mid a \wedge t \mid b \wedge \forall\, t'\,(t' \mid a \wedge t' \mid b \Rightarrow t' \mid t)$
$\underset{\text{o.B.}}{\Leftrightarrow} t \mid a \wedge t \mid b \wedge \forall\, t'\,(t' \mid a \wedge t' \mid b \Rightarrow |t'| \leq |t|)$

„Der“ ggT ist bis auf Vorzeichen eindeutig bezeichnet.
Mit $ggT(a, b)$ meint man den nicht negativen ggT von a und b.

Definition:

$x \in \mathbb{R},\ \lfloor x \rfloor :=$ nächste ganze Zahl „links von x“

$\lfloor 1,8 \rfloor = 1,\ \lfloor -1,8 \rfloor = -2$
$\lfloor 1,1 \rfloor = 1,\ \lfloor -1,1 \rfloor = -2$

$a \operatorname{DIV} b := \left\lfloor \frac{a}{b} \right\rfloor (b \neq 0)$

Teilung mit Rest

Zu jedem Paar $a, b \in \mathbb{Z} (b \neq c)$ gibt es genau ein Paar $g, r \in \mathbb{Z}$ mit

1. $a = g\, b + r$
2. $a \leq r < b$

Dabei ist $g = a \operatorname{DIV} b;\ r = a \operatorname{MOD} b\ \ (= a - (a \operatorname{DIV} b \cdot b))$

Vorschau: Euklidischer Algorithmus zur Bestimmung des $ggT(a, b)\quad a \geq 0; b \geq 0$

$a_1 := a;\ a_2 := b$ (o.E. $a > b$ sonst tauschen)

$a_{n+1} := a_{n-1} \text{MOD } a_n$

$a_1 > a_2 > a_3 > \ldots > a_N > a_{N+1} = 0$

letzter nicht verschwundener Rest $a_N = ggT(a,b)$

$a = 217728;\ b = 826875$

$b \bmod a = 173692 = a_3$

$a \bmod a_3 = 44037 = a_4$

$a_3 \bmod a_4 = 41580 = a_5$

$a_4 \bmod a_5 = 2457 = a_6$

$a_5 \bmod a_6 = 2268 = a_7$

$a_6 \bmod a_7 = 189 = a_8$

$a_7 \bmod a_8 = 0$

$ggT(a,b) = 189$

Bemerkung:

Es gibt 2 ganze Zahlen $R, S \in \mathbb{Z}$, so daß

$189 = R \cdot 826875 + S \cdot 217728.$

($ggT(a,b)$ ist eine ganzzahlige Linearkombination von a und b)

Lemma (Hilfssatz)

$\forall a, b, g \in \mathbb{Z}$ gilt

i. $ggT(a,b) = ggT(b,a)$

ii. $ggT(a,b) = ggT(a,-b)$

iii. $ggT(0,a) = a$

iv. $\boxed{ggT(a,b) = ggT(a+gb,b)}$

Beweis von iv.: Es genügt zu zeigen:

$t|a \wedge t|b \Leftrightarrow t|a+gb \wedge t|b$

$\Rightarrow:$

$\exists t_1, t_2 \in \mathbb{Z}:\ t t_1 = a \wedge t t_2 = b$

$\Rightarrow a + g b = t t_1 + g t t_2 = t(t_1 + g t_2) \Rightarrow t|a+gb$

$\Leftarrow:$

$\exists t_3, t_4 : t t_3 = a + g b \wedge t t_4 = b$

$\Rightarrow a = t t_3 - g b = t t_3 - g t t_4 = t \cdot \underbrace{(\ldots)}_{\in \mathbb{Z}}$

Lemma von Bezoit

$\forall a, b \in \mathbb{Z} \exists R, S \in \mathbb{Z}:\quad ggt(a,b) = R a + S b$

Beweis:

Konstruktiv mittels erweiterten Euklidischen Algorithmus (Euklid / Berlekamp)

Euklid:

$a_1 := a;\ a_2 := b$

Fortgesetzte Teilung mit Rest:

$a_1 = g_3 a_2 + a_3$
$a_2 = g_4 a_3 + a_4$
$a_3 = g_5 a_4 + a_5$
$\vdots$
$(*)$
$a_{n-1} = g_{n+1} a_n + a_{n+1}$
$a_n = g_{n+2} a_{n+1} + a_{n+2}$
$\vdots$

dabei ist $g_{n+1} = a_{n-1} \operatorname{DIV} a_n$
$a_{n+1} = a_{n-1} \operatorname{MOD} a_n < a_n$

es gibt eine echt absteigende Kette

$a_3 > a_4 > \ldots > a_{n-1} > a_n > a_{n+1} > \ldots \geq 0$

Deshalb nach endlich vielen Schritten folgende Situation

es gibt ein N mit

$a_{N-1} = g_{N+1} a_N + a_{N+1}; \quad a_{N+1} \neq 0$
$a_N = g_{N+2} a_{N+1}, \quad a_{N+2} = 0$

Der letzte nicht verschwundene Rest a_{N+1} ist der $ggT(a,b)$:

$$ggT(a,b) = ggT(a_1, a_2) \underbrace{=}_{a_3 = a_1 - g_3 a_2} ggT(a_3, a_2) = ggT(a_2, a_3) \underbrace{=}_{a_4 = a_2 g_4 a_3} ggT(a_4, a_3) = ggT(a_3, a_4) = \ldots$$
$$= ggT(a_{N+1}, \underbrace{a_{N+2}}_{=0}) = a_{N+1}$$

<u>Erweiterter Euklidischer Algorithmus</u> (Berlekamp)

<u>Ziel:</u> Zwei Folgen $R_n, S_n \leftarrow \mathbb{Z}$ zu definieren, für die gilt $a_n = R_n a + S_n b$

insbesondere hätte man dann $ggT(a,b) = a_{N+1} = \underbrace{R_{N+1}}_{R} \cdot a + \underbrace{S_{N+1}}_{S} \cdot b$

$a_1 = \underbrace{1}_{R_1} \cdot a + \underbrace{0}_{S_1} \cdot b$
$a_2 = \underbrace{0}_{R_2} \cdot a + \underbrace{1}_{S_2} \cdot b$

angenommen man hat bereits
$a_{n-1} = R_{n-1} a + S_{n-1} b$
$a_n = R_n a + S_n b$
dann gilt

$$a_{n-1} \underbrace{=}_{(*)} a_{n-1} - g_{n+1} a_n = R_{n-1} a + S_{n-1} b - g_{n+1}(R_n a + S_n b) = \underbrace{(R_{n-1} - g_{n+1} R_n)}_{R_{n+1}} a + \underbrace{(S_{n-1} - g_{n+1} S_n)}_{S_{n+1}} b$$

<u>Zusammenfassung</u>

Anfangswerte:

$a_1 := a;\ \ a_2 := b$
g_1, g_2 undefiniert
$R_1 := 1;\ \ R_2 := 0$
$S_1 := 0;\ \ S_2 := 1$

Rekursionsformeln:

$a_{n+1} = a_{n-1} \operatorname{MOD} a_n$
$g_{n+1} := a_{n-1} \operatorname{DIV} a_n$
$R_{n+1} := R_{n-1} - g_{n+1} R_n$
$S_{n+1} := S_{n-1} - g_{n+1} S_n$

Bemerkung:

Zur Ermittlung von R und S genügt es, die R_n allein (oder die S_n allein) zu berechnen, denn $ggT(a,b) = R_a + Sb \Rightarrow S = \frac{ggT(a,b) - R_a}{b}$

$ggT(826875, 217728)$

a_n	g_n	R_n	
826875	-	1	
217728	-	0	
173691	(3)	1	
44037	1	$-1\ (=-g_4)$	
41580	3	4	Rechnen ab hier
2457	1	−5	
2268	16	84	
189	1	−89	
0	~~12~~	~~1152~~	überflüssig

ab R_4: Vorzeichen alternieren!

$189 = -89 \cdot 826875 + 5 \cdot 217728$
$S = 338$

1.2 Restklassenmenge

$n \in \mathbb{N}, n \geq \mathbb{Z}$

$\mathbb{Z}_n := \{0, 1, \ldots n-1\} \left(= \frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{(n)} \right)$

$\underset{\text{in}\mathbb{Z}_n}{x \underset{\smile}{*} y} := \underset{\in\mathbb{Z}}{(x \underset{\smile}{*} y)} \operatorname{MOD} n, \quad * \in \{+, \cdot\}$

z.B. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Satz 1:

$\mathbb{Z}_n$ ist damit ein kommutativer Ring

z.B. $\underbrace{-x}_{\text{additiv Inverses zu } x} := n - x \quad (\text{in } \mathbb{Z})$

Bemerkung:

$\forall x, y \in \mathbb{Z}, * \in \{+, \cdot\}$ ist $(x \underbrace{*}_{\text{in } \mathbb{Z}} y) \text{MOD } n = (x \text{MOD } n) \underbrace{*}_{\text{in } \mathbb{Z}_n} (y \text{MOD } n)$

„Zwischenergebnisse reduzieren MOD n“

Definition:

R kommutativer Ring, $x \in R$ heißt invertierbar $:\Leftrightarrow \exists y : xy = 1$

Bemerkung:

Ein solches y ist dann eindeutig bestimmt:

$y'x = 1 \Rightarrow y = 1 \cdot y = \underbrace{y'x}_{1} y = y' \underbrace{xy}_{1} = y$

Definition:

$\mathbb{R}^* := \{x \in R : x \text{ invertierbar}\}$ heißt Einheitengruppe von R

($\mathbb{Z}_n^* :=$ prime Restklassen modulo n)

Bemerkung 1:

R^* ist eine Gruppe bezüglich „$\cdot$“, d.h. $a, b \in R^* \Rightarrow ab \in R^*, a^{-1} \in R^*$

neutrales Element 1, Assoziativgesetz

Bemerkung 2:

R Körper $\Leftrightarrow R^* = R \setminus \{0\}$

Beispiel:

$\mathbb{Z}_{15}^* = \{1, 2, 8, 4, 7, 13, 11, \underbrace{14}_{14 = -1,\ (-1)\cdot(-1) = 1}\}$

.	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	13	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Die Gruppe $\mathbb{Z}_{15}^*$

Satz 2:

$n \geq 2, \quad x \in \mathbb{Z}_n$, dann sind äquivalent

i. $\text{ggT}(x, n) = 1$, d.h. x und n sind teilerfremd („zueinander prim“)

ii. 1 ist eine GLK (ganzzahlige Linearkombination) von x und n

iii. $x \in \mathbb{Z}_n^*$

Beweis:

(i) ⇒ (ii) erweiterter Euklidischer Algorithmus

(ii) ⇒ (iii) $1 = R \cdot n + S \cdot x \underset{n=0}{\Rightarrow}$ in $\mathbb{Z}_n$ ist $1 = S \cdot x$

...

Folgerung:

$\mathbb{Z}_n$ Körper ⇔ n prim

Beispiele:

7 in $\mathbb{Z}_{15}$ invertieren:

15	-	1
7	-	0
1	2	1

$1 = 1 \cdot 15 + S \cdot 7 \Rightarrow \frac{1-15}{7} = -2 = 13$

9 in $\mathbb{Z}_{100}$ invertieren:

	g_k	R_k	S_k
100	-	1	
9	-	0	
1	11	1	

$1 = 1 \cdot 100 + S \cdot 9 \Rightarrow \frac{-99}{9} = -11 = 89$

77 in $\mathbb{Z}_{100}$ invertieren:

100	-	1	
77	-	0	
23	(1)	1	
8	3	−3	
7	2	7	
1	1	−10	

$1 = -10 \cdot 100 + S \cdot 77$

$\Rightarrow S = \frac{1001}{77} = 13$

in $\mathbb{Z}_{100}$ ist $13 \cdot 77 = 1001 = 1$

1.3 Kleiner Satz von Fermat & Eulersche φ-Funktion

Satz: (Fermat)

(G_i) Gruppe mit m Elementen, $g \in G$ beliebig, dann gilt

$$\boxed{g^m = 1} \qquad g^m = \underbrace{g \cdot g \cdot g \cdots g}_{m\text{-mal}} \qquad 1 = \text{neutrales Element}$$

Beweis: (nur kommutative Gruppen)

Es sei $G = \{g_1, g_2, \ldots, g_m\}$

$z := g_1 \cdot g_2 \cdot g_3 \cdots g_m$; g beliebig $\in G$

$$g^m \cdot z = g \cdot g \cdots g \cdot g_1 \cdot g_2 \cdots g_m \underset{\text{Komm.}}{=} (g g_i)(g g_2) \cdots (g g_m) \underset{\text{Komm.}}{=} g_1 g_2 \cdots g_m = z$$

$$\Rightarrow g^m \cdot z = z \quad | \cdot z^{-1}$$

$$g^m = 1$$

Korollar:

$$g^{m-1} = g^{-1}$$

allgemein

$g^e = g^{e \,\mathrm{MOD}\, m}$ für $m = |R|$

$|G|$ heißt Ordnung von G

$$14^{66} \,\mathrm{MOD}\, 15 = \underbrace{14^{64}}_{=1} \cdot 14^2 \,\mathrm{MOD}\, 15$$

Eulersche φ-Funktion

Euler: $\boxed{\varphi(n) = n \cdot \prod_p | n \left(1 - \frac{1}{p}\right)}$

p prim

$\prod$ = Produkt

z.B. $\varphi(44) \underset{44 = 2^2 \cdot 11}{=} 44 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right) = 20$

speziell: wenn $n = pq$; p, q prim

$\boxed{\varphi(pq) = (p-1)(q-1)}$

z.B. $\varphi(15) = \varphi(35) = 2 \cdot 4 = 8$

Beweis dieses Spezialfalls $n = pq$:

nicht invertierbar sind

1. alle Vielfache von p: $\underbrace{p, 2p, 3p, \ldots, qp = n = 0}_{q \text{ Stück}}$
2. alle Viefachen von q: p Stück

Insgesamt $p + q - 1$ Stück ($pq = 0$ doppelt gezählt)

$\Rightarrow \varphi(n) = n - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$

noch spezieller $\boxed{\varphi(p)=p-1}$, d.h. $|\mathbb{Z}_p^*|=p-1$

Satz von Euler-Fermat

Ist ggT$(x,n)=1$, dann

$\boxed{x^{\varphi(n)} \text{MOD } n=1}$ $\quad x^{\varphi(n)}\equiv 1 \bmod n;\quad x^{\varphi(n)}\equiv 1 \text{ in } \mathbb{Z}_n$

Korollar:

Ist ggT$(x,n)=1$, so gilt in $\mathbb{Z}_n: x^e=x^{e \text{MOD } \varphi(n)} \forall\, e\in\mathbb{Z}$

Beweis:

$e=g\cdot\varphi(n)+r$ (Teilung mit Rest)

$x^e=x^{g\varphi(n)}\cdot x^r=(\underbrace{x^{\varphi(n)}}_{=1})^g\cdot x^r=x^r$

1.4 Schnelles Potenzieren

$N^e \text{MOD } n$ (d.h. $N^e \text{ in } \mathbb{Z}_n$)

Sei $e=a_r a_{r-1}\ldots a_1 a_0$ die Binärdarstellung von e mit $a_r=1$

```
x := N
for i = v – 1 down to 0 do
     x := x^2;
     if a_i = 1 then x := x * N;
print x;
```

Square & multiply-Algorithmus
S&M-Alg.

Beispiel:

$2^{123} \text{MOD} 55$ $\quad (2^{123} \text{ in } \mathbb{Z}_{55})$

1. $\varphi(55)=\varphi(5\cdot 11)=4\cdot 10=40$
   $2^{123}=2^{123 \text{MOD} 40}=2^3=8$
2. $123=1111011$ $\quad N=2,\ e=123$

	x
1	2
1	8
1	18
1	43
0	34
1	2
1	8

Beweis:

$r=0$ o.k.

$r-1 \to r$

$$e=\underbrace{a_r a_{r-1}\ldots a_1}_{=:e'}\, a_0=\begin{cases} 2e' \text{ für } a_0=0 \\ 2e'+1 \text{ für } a_0=1 \end{cases}$$

$$N^e=\begin{cases} N^{2e'}=(N^{e'})^2 \text{ für } a_0=0 \\ N\cdot N^{2e'}=(N^{e'})^2\cdot N;\ \ a_0=1 \end{cases}$$

nach induktivem Vorgehen (?) liefert der Algorithmus für $N^{e'}$ das Richtige.

Bemerkung: „Russische Bauernmultiplikation“

$N \cdot e$: statt Multiplikation → Addition
Quadrieren → Verdoppeln
Potenzieren → Multiplizieren

Beispiel:

1. $97^{89} \text{ MOD } 100$
2. $97 \cdot 89 \text{ MOD } 100$

	1.	2.
1	97	97
0	9	94
1	57	85
1	53	67
0	9	34
0	81	68
1	17	33

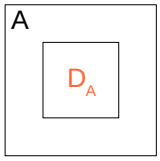
2 Public-Key-Verfahren

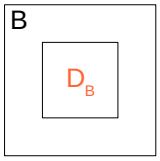
Teilnehmer A, B, C, ..., T, ..., X, ...

öffentliches Directory

A	E_A
B	E_B
⋮	⋮

↳ öffentlicher Schlüssel E_X





geheime Schlüssel D_X, nur dem Teilnehmer X bekannt.

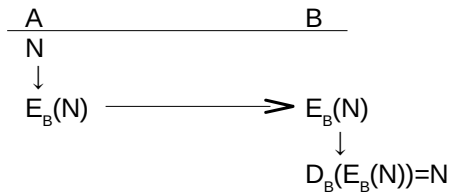
Dabei gilt für jede Nachricht N, jedes X

$$D_X(E_X(N))=N$$
$$E_X(D_X(M))=M$$

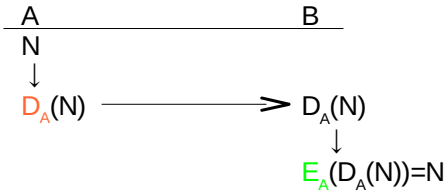
d.h. D_X ist die Umkehrfunktion von E_X.

Bedingung: Es soll „praktisch“ unmöglich sein, D_X aus E_X zu berechnen.

A möchte geheime Nachricht N an B schicken.



elektronische Unterschrift:



2.1 RSA-Verfahren (Rivest, Shamir, Adleman 1978)

1. Wähle 2 große Primzahlen p, q (z.B. 200-stellig)
2. Berechne $n := pq$ und $\varphi(n) := (p-1)(q-1)$
3. Wähle $e < \varphi(n)$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$
4. Berechne $d < \varphi(n)$ mit $ed = 1 \text{ in } \mathbb{Z}^*_{\varphi(n)}$ (d.h. $ed = 1 + s \cdot \varphi(n)$ und mit einer ganzen Zahl s)
   - vergiß $p, q, \varphi(n)$
   - veröffentliche e, n
   - halte d geheim

$N \in \{0, 1, \ldots, n-1\} = \mathbb{Z}_n$ sei die Nachricht (eventuell in Blöcke zerlegen)

$$E(N) := N^e \text{ MOD } n$$
$$D(N) := N^d \text{ MOD } n$$

Behauptung:

$$D(E(N)) = E(D(N)) = N$$

Testbeispiel:

$p = 43, q = 59; n = 2537, \varphi(n) = 2436$

wähle $e = 13$

$d = ? \underset{\text{Euklid}}{\rightarrow} d = 937$

Euklidischer Algorithmus

2436	-	1
1	-	0
5	()	1
3	2	−2
2	1	3
1	1	−5

$1 = -5 \cdot 2436 + d \cdot 13 \Rightarrow d = 937$

z.B. Nachricht sei $N = 95$

$E(N)=95^{13}\,\mathrm{MOD}\,2537 \quad =1950$

1	95
1	2406
0	1939
1	1950

$D(1950)=1950^{937}\,\mathrm{MOD}\,2537 \quad =95=N$

1	1950
1	322
1	122
0	2199
1	1830
0	60
1	121
0	1956
0	140
1	95

Beweis für $D(E(N))=N$

1. In $\mathbb{Z}_p$ gilt $N^{ed}=N$:
   1. $p|N \Rightarrow p|N^{ed} \Rightarrow p|N^{e1}-N \Rightarrow N^{ed}-N=0 \text{ in } \mathbb{Z}_p$
      über $N^{e1}=N$
   2. $p\nmid N$, d.h. $\mathrm{ggT}(p,N)=1$
      $\Rightarrow N^{ed}=N^{1+S\cdot verphi(n)}=N\cdot N^{S\varphi(n)}=N\cdot(N^{\varphi(n)})^S=N\cdot(N^{(p-1)(q-1)})^S=$
      $=N\cdot[(\underbrace{N^{p-1}}_{=1 \text{ in } \mathbb{Z}_p^* \text{(kleiner Fermat)}})^{q-1}]^S=N \text{in } \mathbb{Z}_p$
2. ebenso $N^{ed}=N \text{in } \mathbb{Z}_q$
3. $\left.\begin{array}{l} p|N^{ed}-N \\ q|N^{ed}-N \end{array}\right\} p\neq q$ beide prim
   $\Rightarrow n=pq|N^{ed}-N$
   d.h.
   $N^{ed}=N \text{in } \mathbb{Z}_n$

$\Rightarrow D(E(N))=N^{ed}\,\mathrm{MOD}\,n=N\,\mathrm{MOD}\,n \underset{N<n}{=} N$

Bemerkung:

Es genügt: n quadratfrei (jeder Primfaktor nur einmal)

Auf die quadratfreiheit des Moduls n kann nicht verzichtet werden:
$n=147=7^2\cdot 3;\ e=5;\ d=17$
$(\varphi(n)=147(1-\frac{1}{7})(1-\frac{1}{3})=84)$
$N=7;\ E(N)=7^5\,\mathrm{MOD}\,147=49;\ D(49)=49^{17}\,\mathrm{MOD}\,147=49\neq N$

Sicherheit des RSA-Verfahrens:

Es ist zur Zeit (!) unmöglich, d aus e zu ermitteln, ohne n zu faktorisieren.

Bemerkung: Genauer gesagt benötigt man „nur“ $\varphi(n)$, aber dann hätte man auch die Faktoren p und q von n:

$$\varphi(n)=(p-1)(q-1)=\underbrace{pq}_{n}-p-q+1,\quad q=\frac{n}{p}$$

$$\Rightarrow \varphi(n)=n-p-\frac{n}{p}+1$$

$$p\varphi(n)-np+p^2+n-p=0$$

$$p^2-p\cdot(\underbrace{\varphi(n)-n-1}_{\text{gegeben}})+\underbrace{n}_{\text{gegeben}}=0 \quad \text{quadratische Gleichung in } p$$

Beispiel: $n=2537,\ \varphi(n)=2436$

$$p^2-102p+2537=0$$

$$p_{1,2}=\frac{1}{2}(102\pm\underbrace{\sqrt{102^2-4-2537}}_{16}) \rightarrow p_1=59\ \ p_2=43$$

Angriffe auf das RSA-Verfahren

1) Faktorisierungsalgorithmen

a) „ausprobieren“ bis $\sqrt{n}$. Dazu:
$\Pi(x):=|\{p:p\le x, p\text{ prim}\}|$ Primzahlverteilungsfunktion $z.B.\ \Pi(50)=15$

$\Pi(x)\approx\frac{x}{\ln x}$ für "große" x

z.B. $\frac{50}{\ln 50}=12{,}7$

$\frac{100}{\ln 100}=21{,}7 \quad \Pi(100)=26 \quad (x \text{ noch viel zu klein})$

wieviele Primzahlen, 99- bis 101-stellig, gibt es?

$$\Pi(10^{101})-\Pi(10^{98})=\frac{10^{101}}{\ln(10^{101})}-\frac{10^{98}}{\ln(10^{98})}=10^{98}(\frac{10^3}{101\cdot\ln 10}-\frac{1}{98\cdot\ln 10})=$$

$$=\frac{10^{98}}{\ln 10}\cdot(\frac{10^3}{101}-\frac{1}{98})\approx 10^{98}\cdot 4{,}3$$

b) „Zahlkörpersieb“ (Pollard)

c) quadratisches Sieb

d) elliptische Kurven

e) Pollards Monte-Carlo-Algorithmus

f) Kettenbrüche $\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}$

g) einfaches Beispiel:
Methode der Differenz der Quadrate (Gauß):

Idee: $n=(a+b)(a-b)=a^2-b^2$ (immer möglich $a:=\frac{p+q}{2}$; $b:=\frac{p-q}{2}$)

also: Suche ein a, für das a^2-n eine Quadratzahl ist (b^2)

Start: $a:=\lceil\sqrt{n}\rceil$(nach oben runden): a^n-n Quadratzahl?

wenn nicht: $a:=a+1$

Beispiel: $n=3463373$

$a:=1862$, $a^2-n=3671$ kein Quadrat

$a:=1863$, $a^2-n=7396=86^2$

$n=(1863-86)(1863-86)=1777\cdot1949$

Empfehlung

2) Achtung vor $e=3$ für öffentliche Schlüssel
(früher aus Effizienzgründen gerne verwendet)

Szenario 2.1: 3 Teilnehmer erhalten dieselbe Nachricht N jeweils mit $e=3$.
Angreifer kann aus $E_i(N)=N^3 \operatorname{MOD} n_i \quad i=1,2,3$ N ermitteln (Chinesischer Restsatz)

Szenario 2.2: Verschlüsselung von Sequenznummern N und $N+1$ abgefangen: $C_1=N^3 \operatorname{MOD} n$, $C_2=(N+1)^3 \operatorname{MOD} n$

dann ist $N=\frac{C_2+2C_1-1}{C_2-C_1+2}$ in $\mathbb{Z}_n^+$ (falls C_2-C_1+2 nicht invertierbar in $\mathbb{Z}_n$, dann ist $\operatorname{ggT}(C_2-C_1+2,n)\neq1$, d.h. dann ist sogar n faktorisiert)

Beispiel: $n=17\cdot59=1003$, $R=3$, $N=22$

$C_1=618$, $C_2=131$

$N=\frac{363}{518}=363\cdot304$

$518=-487+2+1003$

1003	-	1
518	-	0
485	1	1
33	1	−1
23	14	15
10	1	−16
3	2	47
1	3	−157

$1=-157\cdot1003+x\cdot518$

$x=304$

Beweis: in $\mathbb{Z}_n$ gilt:

$$\frac{C_2-2C_1-1}{C_2-C_1+2}=\frac{N^3+3N^2+3N+1-2N^3-1}{N^3+3N^2+3N+1-N^3+2}=$$

$$=\frac{3N^3+3N^2+3N}{3N^2+3N+3}=N\cdot\frac{3N^2+3N+3}{3N^2+3N+3}=N$$

3) Keinen gemeinsamen Modul n verwenden!
Szenario 3.1: 2 Benutzer B_1, B_2 mit $n_1=n_2=n$
B möchte beiden die Nachricht N übermitteln.
Angreifer fängt $M_1=N^{e_1} \operatorname{MOD} n$ und $M_2=N^{e_2} \operatorname{MOD} n$ ab.
Ist $\operatorname{ggT}(e_1,e_2)=1$, dann mit Euklid a,b so, daß
$a e_1+b e_2=1$, o.E. sei $a<0$

1) $\operatorname{ggT}(M_1,n)>1 \rightarrow n$ bereits faktorisiert

2) ggT$(M_1, n)=1$

Behauptung: $[(\underbrace{M_1^{-1}}_{M_1 \text{ invertieren in } \mathbb{Z}_n^*})^{-a}\cdot M_2^b] \text{MOD}$

Beweis: in $\mathbb{Z}_n$ gilt $(M_1^{-1})^{-a}\cdot M_2^b = M_1^a\cdot M_2^b = (N^{e_1})^a\cdot(N^{e_2})^b = N^{e_1 a+e_2 b}=N^1=N$

Beispiel: $n=2773$; $e_1=17$; $e_2=3$; $N=920$ gesucht

$\Rightarrow M_1=948$; $M_2=1870$ bekannt

17	-	1
3	-	0
2	5	1
1	1	-1

$1=-1\cdot 17+b\cdot 3$ *newlien* $\Rightarrow b=6$

$a=-1,\ b=6$

M_1 invertieren in $\mathbb{Z}_{2773}$

2773	-	1
948	-	0
877	()	1
71	1	-1
25	12	13
21	2	-27
4	1	40
1	5	-227

$1=-227\cdot 2773+x\cdot 948$

$x=664=M_1^{-1}$

$664^{-a}\cdot 1870^b = 664\cdot 1870^6 \text{ MOD } 2973=920$

Szenario 3.2 diesmal nicht

4) <u>Iterationsattacke</u>

Angreifer hat $M:=E(N)=N^e \text{ MOD } n$

$M_1:=M,\ M_2:=E(M_1),\ M_3:=E(M_2),\ \ldots$

<u>Behauptung</u>:

$\forall h$ mit $M_{h+1}=M_1$ und damit $M_h=N$.

<u>Beweis</u>:

Es gibt endlich viele $0\le M_i<n$

somit irgendwann $M_l=M_{l-h} \underset{E \text{ injektiv}}{\Rightarrow} M_{l-1}=M_{l+h-1}\Rightarrow \ldots M_1=M_{h+1}$

$M_1=E(M_h)=E(N) \qquad M_{h-1}=E(H_h)$

$\underset{E \text{ injektiv}}{\Rightarrow} N=M_h$

Beispiel:

$n=77=7\cdot 11$

$\varphi(n)=60 (=2^2\cdot 3\cdot 5),\ e=7,\ N=2$

$M_1=E(N)=2^7 \text{ MOD } 77=51$ abgefangen

gesucht N

1. Möglichkeit: n faktorisieren

$m=\prod_{i=1}^{l} p_i^{r_i}$

$\varphi(m)=m\cdot\prod_{i=1}^{l}(1-\frac{1}{p_i})=\prod_{i=1}^{l} p_i^{r_i-1}\cdot\prod_{i=1}^{l}(p_i-1)$

$p=2q_1+1;\ q=2q_1+1$

$\varphi(pq)=2p_1\cdot 2q_1=4p_1q_1$

$p_1=2p_2+1;\ q_1=2q_2+1$

$\varphi(\varphi(p\cdot q))=2\cdot(p_1-1)(q_1-1)=2\cdot 2p_2\cdot 2q_2=8p_2q_2$

$m=\varphi(n)=\varphi(pq)=(p-1)(q-1)$

$m=\underset{t\ge 2}{2^t}\cdot q_1^{t_1}q_2^{r_2}\ldots q_c^{r_c}$

30.06.06

$n = 7 \cdot 11$; $\varphi(n) = 6 \cdot 10 = 60$

$e = 7$ in $\mathbb{Z}_{60}$ invertieren:

60	-	1
7	-	0
4	(8)	1
3	1	−1
1	1	2

$1 = 2 \cdot 60 + x \cdot 7$

$x = -17 = \underline{43 = d}$

$N = 51^{43} \text{ MOD } 77 = 2$

43

1	51
0	60
1	32
0	23
1	29
1	2

$M_1 = 51$

$M_2 = E(M_1) = 51^7 \text{ MOD } 77 = 72$

$M_3 = 72^7 \text{ MOD } 77 = 30$

$M_4 = 30^7 \text{ MOD } 77 = 2$

$M_5 = 2^7 \text{ MOD } 77 = 51$

$\Rightarrow N = 2$

Bemerkung:
Zyklenfolge h (hier =4) ist immer ein Teiler von $\varphi(\varphi(n))$, hier:
$\varphi(\varphi(\omega)) = \varphi(60) = 16$

Einschub: Chinesischer Restsatz

Gegeben:

$M = \prod_{i=1}^{k} m_i$ $\quad m_i$ paarweise teilerfremd: $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$

$a_i \in \mathbb{Z}_{m_i}\ i = 1, \ldots, k$

Gesucht:

Ein $x \in \mathbb{Z}_M$ mit $x \text{ MOD } m_i = a_i$ (d.h. $x \equiv a_i (\text{und } m_i) \quad i = 1, \ldots, k$

Behauptung:

Es existiert genau eine goldene Lösung x

Beispiel:

Jede Zahl $x \leftarrow \{0, 1, \ldots 9\}$ ist eindeutig bestimmt durch ihre Reste modulo 2 und modulo 5 ($M := 10,\ m_1 = 2,\ m_2 = 5$: Gegebene Reste: $a_1 = x \text{ MOD } 2,\ a_2 = x \text{ MOD } 5$, daraus eindeutig x zu bestimmen)

Unterbeispiel: $x \text{ MOD } 2 = 0,\ x \text{ MOD } 5 = 3$

$\Rightarrow x = 8$

Konstruktion:

definiere $M_j = \frac{M}{m_j} = \prod_{i=1; i\neq j}^{k} m_i$

wegen $\mathrm{ggT}(m_j, M_j) = 1$ existiert $\boxed{N_j := M_j^{-1} \text{ in } \mathbb{Z}_{m_j}}$

$x := (\sum_{i=0}^{k} a_i N_i M_i) \,\mathrm{MOD}\, M$ leistet das gewünschte ($M_j \text{ in } \mathbb{Z}_{m_j}$ gelesen):

Beweis:

$$(\sum_i a_i N_i M_i) \,\mathrm{MOD}\, m_j = \sum_i (a_i N_i M_i) \,\mathrm{MOD}\, m_j \underset{\text{für alle } i \neq j \text{ ist } M_i \text{ ein Vielfaches von } m_j, \text{ aber MOD } m_i = 0}{=} a_j \overbrace{N_j M_j}^{=1} \,\mathrm{MOD}\, m_j = a_j$$

auf das vorige Beispiel übertragen:
$M = 10;\ m_1 = 2;\ m_2 = 5;\ M_1 = 5;\ M_2 = 2$
$N_1 = 5^{-1} \text{ in } \mathbb{Z}_2$, d.h. $\underline{N_1 = 1}$ $\quad (5 = 1 \text{ in } \mathbb{Z}_2)$
$N_2 = 2^{-1} \text{ in } \mathbb{Z}_5$, d.h. $\underline{N_2 = 3}$
$x = (a_1 N_1 M_1 + a_2 N_2 M_2) \,\mathrm{MOD}\, 10$
$x = (5 a_1 + 6 a_2) \,\mathrm{MOD}\, 10$

x	x MOD 2	x MOD 5
0	0	0
1	1	1
2	0	2
3	1	3
4	0	4
5	1	0
6	0	1
7	1	2
8	0	3
9	1	4

$\mathbb{Z}_{10} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$

Einschub Ende

2.1.1 Message-Concealment Problem

(Wann ist $E(N) = N$?)

Satz (o.B.):

Anzahl der Fixpunkte ($E(N) = N$):
$|\mathrm{Fix}| = (1 + \mathrm{ggT}(e-1, p-1))(1 + \mathrm{ggT}(e-1, q-1))$
$(n = pq,\ E(N) = N^e \,\mathrm{MOD}\, n)$

→ mindestens 9 Fixpunkte

Extrembeispiel: $e=\frac{\varphi(n)}{2}+1$

$\text{ggT}(e-1,p-1)=\text{ggT}(\frac{(p-1)(q-1)}{2},p-1)=p-1$

$\text{ggT}(e-1,q-1)=q-1$

$\Rightarrow|\text{FIX}|=n$ also alles

$e^2=1 \text{ in } \mathbb{Z}_{\varphi(n)}$, d.h. $1=e$

$n=15;\ \varphi(n)=8;\ e=5$

$E(0)=0;\ E(1)=1;\ E(2)=2^5 \text{MOD } 15=2;\ E(3)=3^5 \text{MOD } 15=3;$

$E(4)=4^5 \text{MOD } 15=4;\ \ldots 14^5 \text{MOD } 15=14$

Wieviel Exponenten e sind möglich? (Formel, abhängig von n) $\varphi(\varphi(n))$

2.2 Public-Key-Verfahren, welche auf dem DL (Discret Logarithm)-Problem basieren

2.2.1 DL-Problem

Definition:

Eine endliche Gruppe heißt zyklisch, wenn es darin ein Element $g \in G$ gibt (Generator, primitives Element), so daß $G=\{\underbrace{e}_{\text{neutr. Element}}, g, g^2, g^3, \ldots\}$

Allgemein definiert man für beliebiges $g \in G$:
$<g>:=\{g, g^2, g^3, \ldots g^n=e\}$
$<g>$ ist die von g erzeugte Untergruppe von G.
Immer gilt $r:=\min\{t \geq 1 : g^t=e\}$, dann ist $r=|<g>|$ und $r|m \quad m=|G|$
d.h. G zyklisch $\Leftrightarrow \exists g \in G$ mit $<g>=G$, d.h. $\underbrace{g^m=e}_{\text{gilt sowieso (Fermat)}}$ aber $g^t \neq e \quad 1 \leq t < m \quad m=|G|$

- Folgerung: Ist $|G|$ prim, so ist G zyklisch
- Gauß: Charakterisiert diejenigen n, für die $\mathbb{Z}_n^*$ zyklisch ist
- endliche Körper $\text{GF}(q)$: $\text{GF}(q)^*=\text{GF}(q)\setminus\{0\}$ (multiplikativ) ist immer zyklisch

$n=2, 4, p^r, 2p^r$
p prim, $p \neq 2$
$n=\{2,3,4,5,6,7,9,10,11,13,14,17,18,19,22,23,25,26,27,29,31,\ldots\}$
$\mathbb{Z}_{10}^*=\{1,3,7,9\}$
$<3>=\{3,9,7,1\}$
$<9>=\{9,1\}$
wenn $\mathbb{Z}_n^*$ zykl., dann $\varphi(\varphi(n))$ Generatoren von $\mathbb{Z}_n^*$

Beispiel:

$G=\mathbb{Z}_{31}^{*}=\{1,2,\ldots 30\}$
$|G|=30$
$<2>=\{2,4,8,16,1\}, |<2>|=5$ Teiler von 30
$<3>=\{3,9,27,19,26,16,17,20,29,25,13,8,24,10,30,28,22,4,12,5,15,14,11,2,6,18,23,7,21,1\}\neq 1$
zu 30: $\neq 1$, spätestens hier sieht man $<3>=G$, weil $30=3^{15}\neq 1$, 15 größter echter Teiler von $|G|=30$

zur Basis 3 ist $\log 3=1, \log 9=2$
$\log 27=3,\ldots$
$\log 14=22$

Bemerkung:

Weitere Generatoren: 3^t mit $\text{ggT}(t,30)=1$, also $\underbrace{\varphi(30)}_{=\Sigma}$ (allgemein: $\varphi(|G|)$)

Für „große“ Gruppen ist die Berechnung des DL ähnlich aufwendig wie das Faktorisieren von Zahlen in ähnlicher Größenordnung.

2.2.2 Methoden zur Berechnung des DL

Gegeben:

Endliche zyklische Gruppe G, $|G|=m$, Generator g (also $<g>=G$), $x\in G$

Gesucht:

t mit $g^t=x$

1) Problem: Berechne $g^2, g^3, g^4, \ldots \overset{\text{solange bis}}{\frown}, \quad g^t=x$
2) Baby-Step-Grant-Step-Methode
   Definiere $a:=\lceil\sqrt{m}\rceil$ (nach oben gerundet)

   Baby-Step-Liste: $x\cdot g^{-1}, x\cdot g^{-2}, x\cdot g^{-3}, \ldots, x\cdot g^{-a}$

   Grant-Step-Liste: $\underbrace{e=1}_{g^{0\cdot a}}, g^a, g^{2a}, g^{3a}, \ldots g^{(a-1)\cdot a}$

   Listenvergleich: Ist $x\cdot g^{-r}=g^{sa}$, dann $x=g^{sa+r} \quad \Rightarrow t=\log x=sa+r$

Beispiel:

$g=\mathbb{Z}_{31}^{*}, \quad |G|=\underbrace{30}_{=m}, \quad g=3, x=23$

$a:=\lceil\sqrt{m}\rceil=6$

Baby-Step-Liste:

$x\cdot g^{-1}=\underbrace{23\cdot 21}_{3^{-1}=21:\ \text{Eukl. Alg.}}=18$

$x\cdot g^{-2}=18\cdot 21=6$

$x\cdot g^{-3}=6\cdot 21=2$

alles in $\mathbb{Z}_{31}$ $\qquad x\,g^{-4}=11 \quad x\,g^{-5}=14 \quad x\,g^{-6}=15$

Giant-Step-Liste (unabhängig von x):

$g^a = 3^6 = 16$
$\downarrow \cdot 16$
$g^{2a} = 8$
$\downarrow \cdot 16$
$g^{3a} = 4$
$g^{4a} = 2$
$\rightarrow 6 = 5a + r = 4 \cdot 6 + 3 = 27 = \log 23$

2.2.3 DL-basierte Methoden

2.2.3.1 Diffie-Hellmann Schlüsselaustausch

öffentlich:

- endliche zyklische Gruppe G, $|G| = n$
- Generator g
- Directory

Teilnehmer	öffentlicher Schlüssel
A	$\alpha = g^a$
B	$\beta = g^b$
$\vdots$	

$a < m$ geheim
$\alpha = g^a$ öffentlich

Hintergrund: A und B wollen mittels eines gemeinsamen „Session-Schlüssel“ über ein symmetrisches Kryptoverfahren kommunizieren.

Aufgabe: Erzeugen eines solchen gemeinsamen Schlüssels ohne Kommunikation.

Realisierung:

A: holt β aus dem Telefonbuch (Directory) und bildet β^a

B: holt α aus dem Telefonbuch und bildet α^b

$$\beta^a = (g^b)^a = g^{ab} = (g^a)^b = \alpha^b$$

$\downarrow$

`gemeinsamer Session-Schlüssel` für ein symmetrisches Verfahren

Beispiel:

$G = \mathbb{Z}_{101}^*$, $m = |G| = 100$, $g = 3$
$A: \alpha = 70$
$B: \beta = 50$
Angreifer soll gemeinsamen Sessionschlüssel von A und B finden.

1. Möglichkeit: DL von α

   Baby-Step-Giant-Step ($v := \lceil\sqrt{m}\rceil$ statt $a := \lceil\sqrt{m}\rceil$)
   also hier $v = 10$

   Giant-Step-Liste: $\cdot 65 \quad \cdot 65 \quad 65 \quad \cdot 65 \quad \cdot 65$

   $1,\ g^v = 3^{10} \text{ MOD } 101 = 65,\ g^{2v} = 65^2 = 84,\ 6,\ 87,\ 100,\ 36,\ 17,\ \underbrace{95}_{=g^{8\cdot v}},\ 14$

   (zu 100 auf 36 : $100 = -1,\ (-1)\cdot 65 = -65 \overset{+101}{=} 36$)

   Baby-Step-Liste: $\cdot 34 \quad \cdot 34 \quad \cdot 34 \quad \cdot 34 \quad \cdot 34$

   $g^{-1} = 34,\ xg^{-1} = \alpha \cdot 34 = 70 \cdot 34 = 57,\ 19,\ 40,\ 47,\ 83,\ \underbrace{95}_{\alpha \cdot g^{-6}}$

   $:3$

   $\alpha \cdot g^{-6} = g^{8v} \Rightarrow \alpha = g^{8v+6} = g^{86,} \Rightarrow a = 86$

   Session-Schlüssel $= \beta^a = 50^{86} \text{ MOD } 101 = 22$
   $86 = 1010110_{\text{bin}}$

1	50
0	76
1	41
0	65
1	59
1	27
0	22

2. Möglichkeit:
   DL von $\beta = 50$:

   Baby-Step: $50 \cdot g^{-1} = 50 \cdot 34 = 84$
   $50 \cdot g^{-1} = g^{2v} = g^{20} \Rightarrow 50 = g^{21} \Rightarrow b = 21$

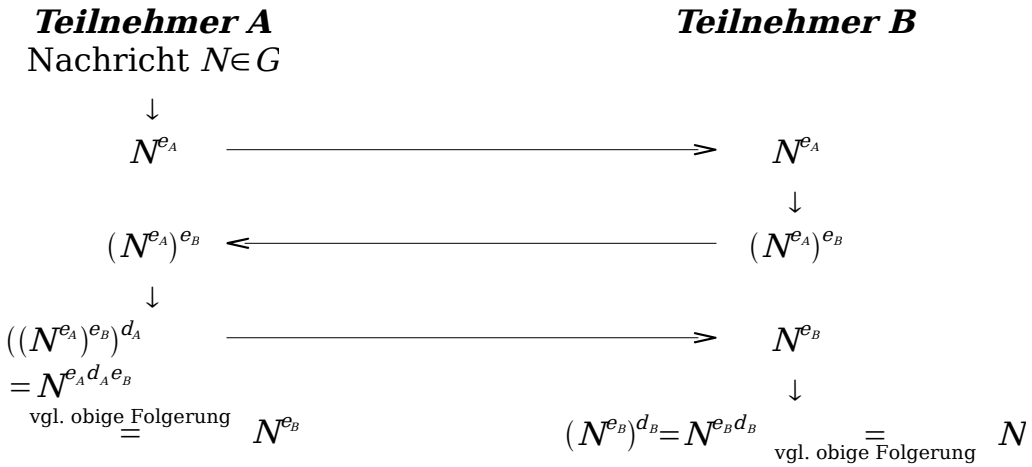
   Sessionschlüssel $= \alpha^b = 70^{21} \text{ MOD } 101 = 22$ (wie oben)

2.2.3.2 Massey-Omura

Alle Teilnehmer kennen eine gemeinsame endliche (zyklische) Gruppe G, $|G| = m$ „groß“.

Jeder Teilnehmer T hat 2 geheime Zahlen $1 < e_T, d_T < m$ mit $e_T \cdot d_T = 1$ in $\mathbb{Z}_m^*$

(Folgerung: $\forall\, x \in G$ ist $x^{e_T \cdot d_T} = x^{1+lm} = x \cdot (\underbrace{x^m}_{=1 \text{ (Fermat)}})^l = x$)



Problem: Authentifizierung

2.2.3.3 Verschlüsselung nach El Gamal

Wie bei Diffie-Hellmann:

G zyklische Gruppe mit Generator $g \in G$, $|G| = m$ (alles öffentlich)

jeder Teilnehmer T hat geheim $t < m$, öffentlich $\tau = g^t \in G$

$(A, a, \alpha), (B, b, \beta)$ usw.

Teilnehmer A	***Teilnehmer B***
(möchte N an B schicken)	
Nachricht $N (\in G)$	
wähle Zufallszahl $z < m$	
(kann auch a sein)	
$k := \beta^z (= g^{bz})$	
$M := f_k(N)$ = verschlüsselte Nachricht	
wobei f_k irgendein symmetrischer Verschlüsselungsalgorithmus mit Parameter k (hier Original-El-Gamal: $f_k(N) = k \cdot N$ in $G = \mathrm{GF}(q)^* \underset{\text{spez. für } q=\text{Primzahl } p}{=} \mathbb{Z}_p^*$)	
bildet (g^z, M)	(g^z, M)
	$(g^z)^b = k$
	$k = \beta^z = (g^b)^z = (g^z)^b$
	$f_k^{-1}(M) = N$
	hier: $f_k^{-1}(M) = k^{-1} \cdot M = k^{-1} k N = N$

<u>Zahlenbeispiel:</u>

$\underbrace{G}_{g=z,\,|G|=100} := \mathbb{Z}_{101}^*$ (Hauptanwendung El Gamal $g = K^*, K$ endlicher Körper wie $\mathbb{Z}_p, p$ prim

A:	**B:**
$N = 77$;	geheim: $b = 5$
wählt $z = 3$ (geheim)	öffentlich: $\beta = 2^5 = 32$

$k := 32^3 \text{ MOD } 101 = 44$
$M := 44 \cdot 77 \text{ MOD } 101 = 55$
$g^z = 2^3 \text{ MOD } 101 = 8$
$(8,55) \longrightarrow (8,55)$
$\downarrow$
$k = 8^b = 8^5 \text{ MOD } 101 = 44$
$N = 44^{-1} \cdot 55 \underset{*}{=} 77 \; (\text{in } \mathbb{Z}_{101})$

101	-	1
44	-	0
13	2	1
*) 5	3	-3
3	2	7
2	1	-10
1	1	17

$1 = 17 \cdot 101 + x \cdot 44$
$x = -39 = 62$
$62 \cdot 55 \text{ MOD } 101 = 77$

2.2.3.4 El-Gamal-Signaturschema

klassisch: $G = \mathbb{Z}_p^* = \{1, \ldots, p-1\}, m = |G| = p-1$
Generator $g \in \mathbb{Z}_p^*$

Teilnehmer T erzeugt eine Unterschrift für eine Nachricht $N \in \mathbb{Z}_{p-1}$:

- → wählt eine Zufallszahl r mit $\text{ggT}(r, p-1) = 1$ (d.h. $r \in \mathbb{Z}_{p-1}^*$)
- → berechnet $k := g^r$
- → berechnet s in $\mathbb{Z}_{p-1}$ so, daß $t \cdot k + r \cdot s = N$ in $\mathbb{Z}_{p-1}$ (realisieren: $s = (N - t \cdot k) \cdot r^{-1}$ in $\mathbb{Z}_{p-1}$)

Digitale Unterschrift zur Nachricht N ist das Paar (k, s).

Empfänger: Hat N und (k, s)

prüft: Ist $g^N \overset{?}{=} \tau^k \cdot k^s$ in $g = \mathbb{Z}_p^*$ (τ öffentlich von T)

Es gilt $\tau^k \cdot k^s = g^{tk} \cdot g^{rs} = g^{tk+rs} \underset{\text{in } \mathbb{Z}_p, \text{ weil } tk+rs = N \text{ in } \mathbb{Z}_{p-1}. (*)}{=} g^N$

Bemerkung 1: Hier in der Praxis statt N ein $\underbrace{H}_{\text{Hash-Funktion}}(N) = N'$

in anderen Gruppen G müßten die Exponenten N und k erst als Zahlen kodiert werden

(*): Begründung: Es gilt $tk + rs = N + l \cdot (p-1)$
in $\mathbb{Z}_p^*$: $g^{tk+rs} = g^N \cdot (\underbrace{g^{p-1}}_{=1 \text{ in } \mathbb{Z}^* \, (Fermat)})^l = g^N$

Bemerkung 2: Unterschrift unabhängig vom Empfänger
Prüfung der Unterschrift: Nur abhängig vom Absender (und von N)

Zahlenbeispiel:

$p = 101; \; g \in 2; \; N = 77; \; t = 5; \; r = 3$

1) $k := g^r = 2^3 = 8$

2) r^{-1} in $\mathbb{Z}_{p-1}$: in $\mathbb{Z}_{100}$ ist $\frac{1}{r} = \frac{1}{3} = \frac{101}{3} = \frac{201}{3} = 67 = r^{-1}$ (oder mit Euklid)

$s := (N - t\,k)\,r^{-1} = (77 - 5\cdot 8)\cdot 67 \,\mathrm{MOD}\, 100 = 79$

Unterschrift $= (8, 79)$

Prüfen der Unterschrift:

a) $g^N = 2^{77} \,\mathrm{MOD}\, 101 = ¿$

b) $\tau = 2^5 \,\mathrm{MOD}\, 101 = 32 \cdot \tau^k \cdot k^s = 32^8 \cdot 8^{79} \,\mathrm{MOD}\, 101 = ¿$

$32^8 \cdot 8 = 79 = 2^{40} \cdot 2^{3\cdot 79} = 2^{277} = (\underbrace{2^{100}}_{=1})^2 \cdot 2^{77}$

$a^{p-1} \,\mathrm{MOD}\, p = 1 \quad 1 \le a < p$ Fermat

3 Elliptische Kurven (EC)

$y^2 = x^3 + a\,x + b$

$4\,a^3 + 27\,b \neq 0$

Körper $\mathrm{GF}(q) = \mathrm{GF}(p^n)$

Hauptanwendungen

$\rightarrow p = 2, n$ groß

$\rightarrow n = 1, p$ groß : $\mathrm{GF}(p) = \mathbb{Z}_p$ (hier)

$p = \mathrm{char}\,\mathrm{GF}(p^n) \neq 2, 3$

$P(x_1, y_1)$

$Q(x_2, y_2)$

$P * Q = (x_3, y_3)$

$(x, y) * (x, -y) := \Omega$ ← neutrales Element

$x_3 = s^2 - x_1 - x_2$

$y_3 = s(x_1 - x_3) - y_1$

$$s_i = \begin{cases} \dfrac{3x_1^2 + a}{2\,y_1} & \text{falls } P = Q \\ \dfrac{y_2 - y_1}{x_2 - x_1} & \text{sonst (aber } x_1 \neq x_2) \end{cases}$$

<u>Beispiel:</u>

$K = \mathrm{GF}(11) = \mathbb{Z}_{11} \quad (\mathrm{char} = 11)$

$y^2 = x^3 + 3 \quad (a = 0, b = 3)$

Prüfen, ob $4\,a^3 + 27\,b \neq 0$; $\quad 0 + 81 \neq 0$

alle Punkte ausrechnen (jenseits aller Realität)

↔

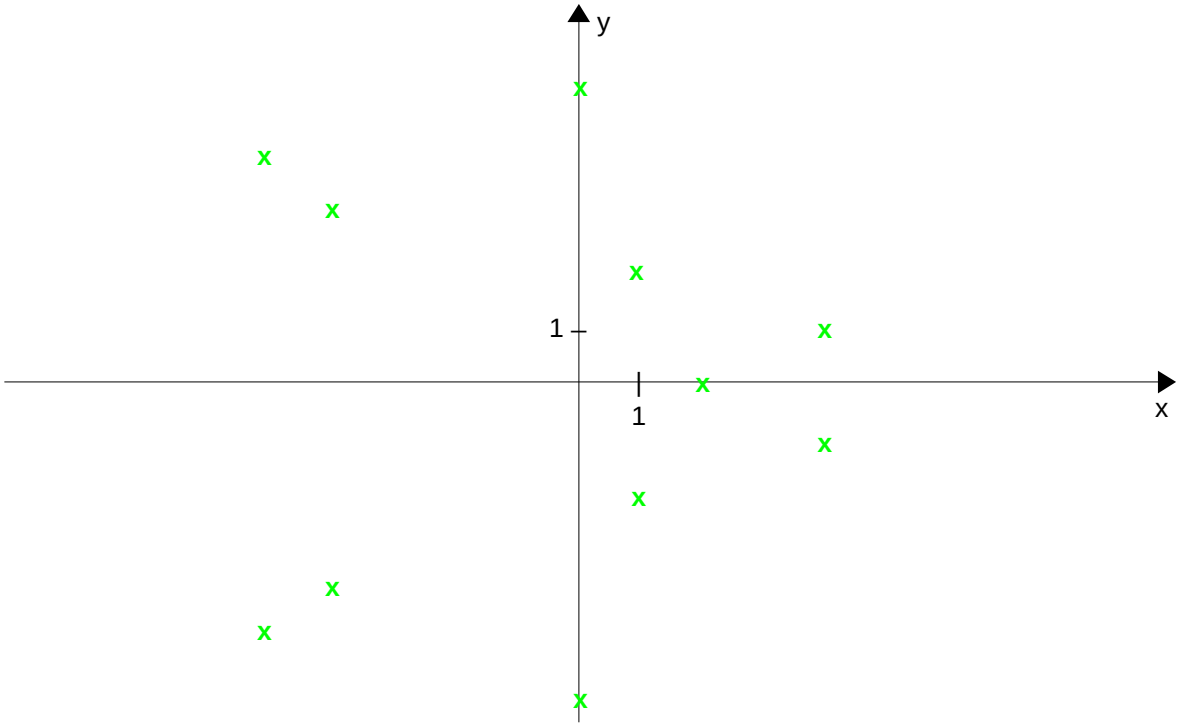
y	0	1	2	3	4	5	6	7	8	9	10
y^2	0	1	4	9	5	3	3	5	9	4	1

y	0	1	2	3	4	5	-5	-4	-3	-2	-1
y^2	0	1	4	-2	5	3	3	5	-2	4	1

x	0	1	2	3	4	5	-5	-4	-3	-2	-1
x^3	0	1	-3	5	-2	4	-4	2	-5	3	-1
$x^3 + 3$	3	4	0	-3	1	-4	-1	5	-2	-5	2

$E=\{(0,5),(0,-5),(1,2),(1,-2),(2,0),(4,1),(4,-1),(-4,4),(-4,4),(-3,3),(-3,-3),\Omega\}$

$(x,y)\in EC \underset{(-y)^2=y^2}{\Leftrightarrow} (x,-y)\in EC$



z.B. $(0,5)*(0,5)=(x_3,y_3)=(0,-5) \quad \Rightarrow (0,5)^3=\Omega$

$s=\frac{3x_1^2+a}{2y_1}=0; \quad x_3=0-0-0=0; \quad y_3=-y_1=-5$

$(0,-5)*(0,-5)=(0,5)^2*(0,5)^2=(0,5)^4=\underbrace{(0,5)^3}_{=\Omega}(0,5)=(0,5)$

Allgemein: $(x,-y)^n=[(x,y)^{-1}]^n=(x,y)^{-n}=[(x,y)^n]^{-1}$

$(1,2)*(1,2)=?$

$s=\frac{3}{4}\underset{4^{-1}=3}{=}3\cdot 3=-2; \quad x_3=4-1-1=2; \quad y_3=-2(1-2)-2=0 \quad \Rightarrow (2,0)$

$(4,1)*(4,1)\underset{\uparrow}{=}(-4,4)$

$s=\frac{4}{2}=2; \quad x_3=4-4-4=-4; \quad y_3=2(4+4)-1=4$

$(-4,4)*(-4,4)\underset{\uparrow}{=}(0,5)$

$s=\frac{4}{8}=\frac{1}{2}=-5; \quad x_3=3+4+4=0; \quad y_3=-5(-4-0)-4=5$

$\Rightarrow$ Ordnung von $P=P(4,1)$ ist $12 (|P|=12$, oder $P^{12}=\Omega$ aber $P^m\neq\Omega \; \forall m \;\; 1\leq m\leq 11)$

$|G|=n$

Gg Generator, dann gilt

g^r Gen. $\Leftrightarrow$ ggT$(r,n)=1$

$\varphi(n)$ Generatoren

$P=(4,1)$ Generator

weitere Generatoren: P^5, P^7, P^{11}

P(4, 1)

n	P^n
1	(4, 1)
2	(-4, 4)
3	(1, ±2)
4	(0, 5)
5	(-3, ±3)
6	(2, 0)
7	(-3, ±3)
8	(0, -5)
9	(1, ±2)
10	(-4, -4)
11	(4, -1)
12	Ω

$(P^6)^2 = \Omega$

$(P^n)^{-1} = P^{-n} = P^{12-n}$

Definition:

Ordnung eines Elements $g \in G$ (endliche Gruppe):

$$\operatorname{ord} g := |g| := |<g>| := \min\{r \in \mathbb{N} : g^r = \underbrace{e}_{\text{neutr. El.}}\}$$

Satz:

$\operatorname{ord} g$ teilt $|G|$.

4 Symmetrische Verfahren

4.1 Blockchiffren / Stromchiffren

4.2 Pseudozufallszahlen

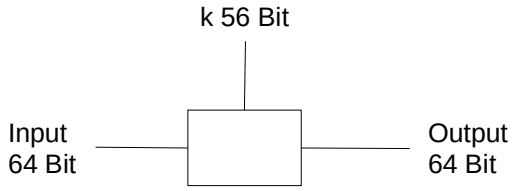
4.2.1 Modulare Pseudozufallsgeneratoren

4.2.2 Linear rückgekoppelte Schieberegister

4.3 DES (Data Encryption Standard)

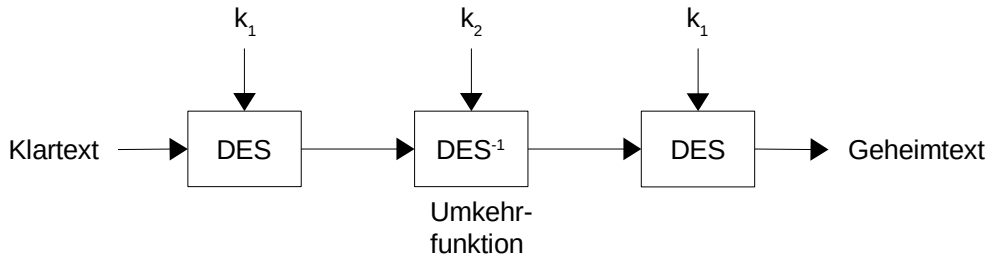
NBS (USA 1977)

Länge des gemeinsamen Schlüssels k: 56 Bit



Blockchiffre

Triple DES



4.4 AES (Advanced Encryption Standard)

NBS

↓

NIST (National Institute of Standards Technology)
Internationaler Wettbewerb 1977

Gewinner 2000 Algorithmus „Rijndael“ (Daemen, Rijmen) (Belgier)

Vorbetrachtung

Der endliche Körper $GF(2^8)=GF(256)=\mathbb{F}_{256}$

Analyse

$\mathbb{Z}$	Polynomring $K[X]$, K Körper
$a,b\in\mathbb{Z}\rightarrow$ dazu $g,r\in\mathbb{Z}$ mit $0\neq r<b$ und $a=\underbrace{g}_{a\,\mathrm{DIV}\,b}\cdot b+\underbrace{r}_{a\,\mathrm{MOD}\,b}$ (Teilung und Rest)	Elemente sind Polygone $a(X)=\Sigma\, a_i X^i$ $a(X),b(X)\in K[X]\rightarrow$ dazu $g(X),r(X)\in K[X]$ mit $\mathrm{grad}\,r(X)<\mathrm{grad}\,b(X)$ $a(X)=\underbrace{g(X)}_{a(X)\,\mathrm{DIV}\,b(X)}\cdot b(X)+\underbrace{r(X)}_{a(X)\,\mathrm{MOD}\,b(X)}$ (Teilung mit Rest)
n fest $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$ $a\cdot b:=(ab)\,\mathrm{MOD}\,n$ $a+b:=(a+b)\,\mathrm{MOD}\,n$	$p(X)\in K[X]$ fest, $\mathrm{grad}\,P(X)=n$ $K[X]_{p(X)}:=\{$alle Polynome$\in K[X]$ mit $\mathrm{grad}<n\}$ Darstellung durch Koeffiziententupel $a_0 a_1 \ldots a_{n-1}$ bzw. durch $\underline{a_{n-1}a_{n-1}\ldots a_0}$ $a(X)\ \dot{\text{in}}_{K[X]_{p(X)}}\ b(X):=[a(X)\ \dot{\text{in}}_{K[X]}\ b(X)]\,\mathrm{MOD}\,p(X)$ Addition wie in $K[X]$
$\mathbb{Z}_n$ Ring $\mathbb{Z}_n$ Körper $\Leftrightarrow n=p=$ prim	$K[X]_{p(X)}$ Ring $K[X]_{p(X)}$ Körper $\Leftrightarrow p(X)=\pi(X)=$ irreduzibel, d.h. $\pi(X)$ läßt sich nicht in Produkt von 2 Polynomen kleineren Grades zerlegen

alle endlichen Körper:
$GF(p^n)=\mathbb{Z}_p[X]_{\pi(X)}$
$\pi(X)$ irreduzibel von Grad n

Hier: $K=\mathbb{Z}_2=\{0,1\}$

·	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	0

XOR

$n=8$; $\pi(X)=X^8+X^4+X^3+X+1\in\mathbb{Z}_2[X]$ im AES festgelegt (inredizibel!)

$\mathbb{F}_{256}=\{a_7a_6\ldots a_0; a_i\in\{0,1\}\}=\{\text{alle Polynome } a_7X^7+a_6X^6+\ldots+a_1X+a_0 \text{ mit } a_i\in\mathbb{Z}_2\}=$
$=\{\text{alle Polynome mit Koeff.}\in\mathbb{Z}_2 \text{ von Grad} <8\}$

Addition = normale Polynomaddition = koeffizientenweise (komponentenweise) XOR
Multiplikation: $a(X)\cdot b(X):=[a(X)\cdot b(X)]\,\text{MOD}\,\pi(X)\rightarrow dazu$
Beispiel:
$A0+C0=10100000+11000000=(X^7+X^5)+(X^7+X^6)=X^6+X^5=01100000=0x60$
$A0\cdot C0$: zuerst in $\mathbb{Z}_2[X]$: $(X^7+X^5)\cdot(X^7+X^6)=X^{14}+X^{13}+X^{12}+X^{11}$
dann: $\text{Rest}\,\text{MOD}\,\pi(X)$:

$$X^{14}+X^{13}+X^{12}+X^{11}=\underbrace{(X^8+X^4+X^3+X+1)\cdot(X^6+X^5+X^4+X^3+X^2)}_{=\text{Produkt}\,\text{DIV}\,\pi(X)}+\underbrace{X^7+X^5+X^2}_{\text{Rest}(=\text{Produkt}\,\text{MOD}\,\pi(X))}$$

$$\begin{array}{l}
\underline{X^{14}+X^{10}+X^9+X^7+X^6} \\
\quad X^{13}+X^{12}+X^{11}+X^{10}+\underline{X^9}+X^7+\underline{X^6} \\
\quad \underline{X^{13}+\underline{X^9}+X^8+\underline{X^6}+X^5} \\
\qquad X^{12}+X^{11}+X^{10}+\underline{X^8}+\underline{X^7}+\underline{X^5} \\
\qquad \underline{X^{12}+\underline{X^8}+\underline{X^7}+\underline{X^5}+X^4} \\
\qquad\quad X^{11}+X^{10}+\underline{X^4} \\
\qquad\quad \underline{X^{11}+X^7+X^6+\underline{X^4}+X^3} \\
\qquad\qquad X^{10}+X^7+\underline{X^6}+\underline{X^3} \\
\qquad\qquad \underline{X^{10}+\underline{X^6}+X^5+\underline{X^3}+X^2} \\
\qquad\qquad\quad X^7+X^5+X^2
\end{array}$$

Rest $=10100100=A4$ also: $A0\cdot C0=A4$

Bemerkung: Alternative statt $\text{Rest}\,\text{MOD}\,\pi(X)$:
Setze $\pi(X)=0$, d.h. $X^8=x^4+X^3+X+1$, damit Grad reduzieren.
Im Beispiel:

$$x^{14}+x^{13}+X^{12}+X^{11}=X^6(\underline{X^8}+X^7+X^6+X^5)=X^6(\underline{X^4+X^3+X+1}+X^7+X^6+X^5)=$$
$$=X^7+X^6+X^3(\underline{X^6}+X^7+\underbrace{X^8}_{1+X+X^3+X^4}+\underbrace{X^9}_{X+X^2+X^4+X^5}+\underbrace{X^{10}}_{X^2+X^3+X^5+X^6})=X^7+X^6+X^3(1+X^7)=$$
$$=X^7+X^6+X^3+X^2\underbrace{X^8}_{1+X+X^3+X^4}=X^7+\underline{X^5}+\underline{X^3}+X^2+\underline{X^3}+X^5+\underline{X^6}=X^7+X^5+X^2$$

$GF(256), \pi(X)=0$?

$\pi(X)=X^8+X^4+X^3+X+1$ festgelegt

$\mathbb{Z},\ \mathbb{Z}_n=\frac{\mathbb{Z}}{n\mathbb{Z}}=\frac{\mathbb{Z}}{(n)} \quad n=0$

$\underbrace{K}_{K=\mathbb{Z}_2}[X],\ \underbrace{K[X]_{\pi(X)}}_{*}=\frac{K[X]}{(\pi)},\quad \pi(X)=0$

*: alle Polynome von Grad $<8; \mathbb{Z}_2[X]_{\pi(X)}=GF(2^8)=GF(256)=\mathbb{F}_{256}$

$\mathbb{F}_{256}=\{\underline{a}=a_7 a_6 \ldots a_1 a_0 \in \mathbb{Z}_2^8=\{0,1\}^8;\ \underline{a}=a(X)=a_7X^7+a_6X^6+\ldots a_1X+a_0\}$

Addition komponentenweise (ohne Überhang)
Multiplikation: Erst wie üblich und dann

Rest MOD $\pi(X)$
$\pi(X)=0$ benutzen $(X^8=X^4+X^3+X+1)$

Beispiel:

$10100101 \cdot 10010001 = ?$

$(X^7+X^5+X^2+1)\cdot(X^7+X^4+X^3+1)=X^{14}+X^{12}+X^{11}+X^{10}+X^8+X^6+X^4+X^3+X^2+1$

1. Möglichkeit: Teilen durch $\pi(X) \rightarrow$ Rest

$$X^{14}+X^{12}+X^{11}+X^{10}+X^8+X^6+X^4+X^3+X^2+1=(X^8+X^4+X^3+X+1)\cdot(X^6+X^4+X^3+X)+\underbrace{X^7+X^6+X+1}_{11000011}$$

$$\begin{array}{l}
X^{14}+X^{10}+X^9+X^7+X^6 \\
\quad X^{12}+X^{11}+X^9+X^8+X^7+X^4+X^3+X^2+1 \\
\quad X^{12}+X^8+X^7+X^5+X^4 \\
\quad\quad X^{11}+X^9+X^5+X^3+X^2+1 \\
\quad\quad X^{11}+X^7+X^6+X^4+X^3 \\
\quad\quad\quad X^9+X^7+X^6+X^5+X^4+X^2+1 \\
\quad\quad\quad X^9+X^5+X^4+X^2+X \\
\quad\quad\quad\quad \underbrace{X^7+X^6+X+1}_{\text{Rest (Grad}<8)}
\end{array}$$

2. Möglichkeit: $\pi(X)=0$, d.h. $X^8=X^4+X^3+X+1$

$$\underbrace{X^{14}}_{=X^6X^8=X^{10}+X^9+X^7+X^6=X^6+X^5+X^3+X^2+X^5+X^4+X^2+X+X^7+X^6} + \underbrace{X^{12}}_{=X^8+X^7+X^5+X^4=X^4+X^3+X+1} + \underbrace{X^{11}}_{=X^7+X^6+X^4+X^3} + \underbrace{X^{10}}_{=X^8+X^5+X^3+X^2} + \underbrace{X^8}_{=X^4+X^3+X+1} + X^6+X^4+X^3+X^2+1=X^7+X^6+X+1$$

Invertieren in $\mathbb{F}_{256}=\mathbb{Z}_2[X]_{\pi(X)}=\frac{\mathbb{Z}_2[X]}{(\pi(X))}=\frac{\mathbb{Z}_2[X]}{(X^8+X^4+X^3+X+1)}$

Erweiterter Euklidischer Algorithmus

zum Invertieren $\mathbb{Z}_n=\frac{\mathbb{Z}}{(n)}$: Invertiere y in $\mathbb{Z}_n$

a_k	g_k	R_k	S_k	
$a_1 = n$	-	1	0	$a_{k+1} := a_{k-1} \operatorname{MOD} a_k$
$a_2 = y$	-	0	1	$a_{k+1} := a_{k-1} \operatorname{DIV} a_k$
	g_3	1	$-g_3$	$R_{k+1} := R_{k-1} - g_{k+1} R_k$
	g_4	$-g_4$		$S_{k+1} := S_{k-1} - g_{k+1} S_k$

$$(1=)\underbrace{\operatorname{ggT}(n,y)}_{\text{letztes } a_k \neq 0} = R_k n + S_k y$$

Invertiere von $b(X) \neq 0 \in \mathbb{F}_{256}$

und weg war die Tafelanschrift....

<u>Beispiel</u>

Invertiere $b(X) = X^5 + X$ in $\mathbb{F}_{256}$:

$a_k(X)$	$g_k(X)$	$R_k(X)$	$S_k(X)$
$X^8+X^4+X^3+X+1$	-	1	0
X^5+X	-	0	1
X^3+X+1	x^3	1	x^3
X^2+1	X^2+1	X^2+1	$1+(X^2+1)\cdot X^3=X^5+X^3+1$
1	X	X^3+X+1	$X^3+X(X^5+X^3+1)=X^6+X^4+X^3+X$

$1=(X^3+X+1)(X^8+X^4+X^3+X+1)+S(X)\cdot(X^5+X)$

$\Rightarrow S(X)=\dfrac{1+(X^3+X+1)(X^8+X^4+X^3+X+1)}{X^5+X}$

(im Polynomenring $\mathbb{Z}_2[X]$, Division muß aufgehen!)

besser: gleich $S_k(X)$-Spalte!

NR:

$X^8+X^4+X^3+X+1=(X^5+X)\cdot\underbrace{(X^3)}_{\text{DIV}}\underbrace{+X^3+X+1}_{\text{MOD}}$

$\underline{X^8+X^4}$

X^3+X+1

$X^5+X=(X^3+X+1)\cdot\underbrace{(X^2+1)}_{\text{DIV}}+\underbrace{X^2+1}_{\text{MOD}}$

$\underline{X^5+X^3+X^2}$

X^3+X^2+X

$\underline{X^3+X+1}$

X^2+1

$X^3+X+1=(X^2+1)\cdot\underbrace{X}_{\text{DIV}}+\underbrace{1}_{\text{MOD}}$

$\underline{X^3+X}$

1

$1+(\ldots)\cdot(\ldots)=$

$=X^{11}+X^9+X^8+X^7+X^6+X^5+X^4+X^2=(X^5+X)(X^6+X^4+X^3+X)$

$\underline{X^{11}+X^7}$

$X^9+X^8+X^6+X^5+X^4+X^2$

$\underline{X^9+X^5}$

$X^8+X^6+X^4+X^2$

$\underline{X^8+X^4}$

X^6+X^2

$\underline{X^6+X^2}$

- -

Fazit: in $\mathbb{F}_{256}$ ist $(00100010)^{-1}=01011010$

Aufbau des AES

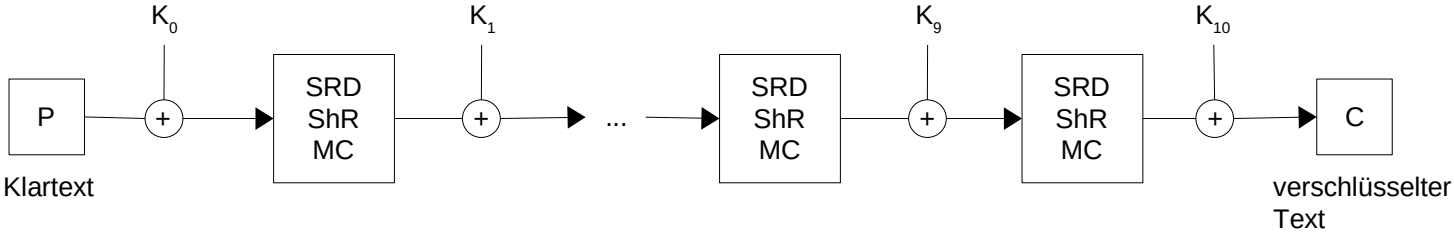
Blockänge: $128=16$ Byte

Schlüssellänge: 128=16 Byte (Varianten mit 192, 256 Bit)

Klartext: Zustandsmatrix $P=\begin{bmatrix} p_0 & p_4 & \vdots & \vdots \\ p_1 & p_5 & \vdots & \vdots \\ p_2 & \vdots & \vdots & \vdots \\ p_3 & \vdots & \vdots & p_{15} \end{bmatrix}$ jedes p_i ist ein Byte

Schlüssel $K=\begin{bmatrix} k_0 & k_4 & \vdots & \vdots \\ k_1 & k_5 & \vdots & \vdots \\ k_2 & \vdots & \vdots & \vdots \\ k_3 & \vdots & \vdots & k_{15} \end{bmatrix}$ =Schlüsselmatrix jedes k_i ist ein Byte

<u>10 Runden</u> (Varianten: 12 Runden, 14 Runden)



i-te Runde:

$E_i(\underline{x})=K_{i\,plus}\mathrm{MC}(\mathrm{ShR}(\mathrm{SRD}(\underline{x})))$

kurz: $e_i=K_i+\mathrm{MC}\circ\mathrm{ShR}\circ\mathrm{SRD}$ $\quad E_i:\{0,1\}^{128}\to\{0,1\}^{128}$

$\underline{x}\in\{0,1\}^{128}$

1) SRD (entspricht den S-Boxen beim DES, nichtlinear)
2) MC linear
3) ShR linear
4) K_i?

1) SRD vgl. Beiblatt „Einzelheiten zu AES“

$$\mathrm{Inv}(\underline{b})=\begin{pmatrix} \underline{b}^{-1} & \text{in } \mathrm{F}_{256} \text{ falls } \underline{b}\neq\underline{0} \\ \underline{0} & \text{falls } \underline{b}=\underline{0} \end{pmatrix}$$

Byteweise:

$$\mathrm{SRD}(\underline{p_i})=\underbrace{\underline{M}}_{\text{konstant}}\cdot\mathrm{Inv}(\underline{p_i})+\underbrace{\underline{a}}_{\text{konstant}}$$

2) MC (Mix column) vgl. Beiblatt (übliche Multiplikation von 4x4-Matrizen mit Einträgen in $\mathbb{F}_{256}$)

Bemerkung zu den Zahlen 1, 2, 3: Bytes interpretiert als Dezimalzahlen ($\sum a_i x^i \leftrightarrow \sum a_i 2^i$)
Eintrag 1 = 0000 0001 = 1 (als Polynom) = $\{01\}_{\mathrm{hex}}$

Eintrag 2 = 0000 0010 = X (als Polynom) = $\{02\}_{hex}$
Eintrag 3 = 0000 0011 = X+1 (als Polynom) = $\{03\}_{hex}$

3) ShR (Shift Round)

i-te Zeile um i - 1 zyklisch verschoben

4) $K_0=[\underset{\uparrow}{w_0}\ \underset{\uparrow}{w_1}\ \underset{\uparrow}{w_2}\ \underset{\uparrow}{w_3}]$

Spalten der Schlüsselmatrix K

$$w_i = \text{Spaltenvektor mit } 4 \text{ Bytes} \begin{pmatrix} \underline{a}_0 \\ \underline{a}_1 \\ \underline{a}_2 \\ \underline{a}_3 \end{pmatrix}$$

$$K_0=[\underset{\downarrow}{w_0}\ \underset{\rightarrow}{w_1}\ \underset{\rightarrow}{w_2}\ \underset{\rightarrow}{w_3}]$$
$$K_1=[\underset{\downarrow}{w_4}\ \underset{\rightarrow}{w_5}\ \underset{\rightarrow}{w_6}\ \underset{\rightarrow}{w_7}]$$
$$K_2=[\underset{\downarrow}{w_8}\ \underset{\rightarrow}{w_9}\ \underset{\rightarrow}{3_{10}}\ \underset{\rightarrow}{w_{11}}]$$
$$\vdots$$
$$K_i=[w_{4i}\ w_{4i+1}\ w_{4i+2}\ w_{4i+3}]$$
$$\vdots$$
$$K_{10}=[w_{40}\ w_{41}\ w_{42}\ w_{43}]$$

1) j kein Vielfaches von 4: $w_j := w_{j-1} + w_{j-4}$

2) $j = 4i: w_j = S(w_{j-1}) + C_i + w_{j-4}$ mit $S\begin{pmatrix} \underline{a}_0 \\ \underline{a}_1 \\ \underline{a}_2 \\ \underline{a}_3 \end{pmatrix} = \begin{pmatrix} \mathrm{SRD}(\underline{a}_1) \\ \mathrm{SRD}(\underline{a}_2) \\ \mathrm{SRD}(\underline{a}_3) \\ \mathrm{SRD}(\underline{a}_0) \end{pmatrix}$

$$C_i := \begin{pmatrix} X^{i-1} \text{ in } \mathrm{F}_{256} \\ \underline{0} \\ \underline{0} \\ \underline{0} \end{pmatrix} = \text{const.}(\text{hängt nur von } i \text{ ab})$$

X^{i-1} in F_{256} ?

$i=1 : X^0 = 1 = 00000001 = \{01\}_{\text{hex}}$

$i=2 : X^1 = X = 00000010 = \{02\}_{\text{hex}}$

$i=3 : X^2 = 00000100 = \{04\}_{\text{hex}}$

$i=4 : X^3 = 00001000 = \{08\}_{\text{hex}}$

$X^4 = \underbrace{0001}_{1_{\text{hex}}}\underbrace{0000}_{0_{\text{hex}}} = \{10\}_{\text{hex}}$

$X^5 = \{20\}_{\text{hex}}$

$X^6 = \{40\}_{\text{hex}}$

$X^7 = \{80\}_{\text{hex}}$

$i=9 : X^8 = X^4 + X^3 + X + 1 = 00011011 = \{1\mathrm{B}\}_{\text{hex}}$

$i=10 : x^9 = X^5 + X^4 + X^2 + X = 00110110 = \{36\}_{\text{hex}}$