1 Uebungen

Serie 4

Aufgabe 1

$m =$

0011	0101	0110	0000

Padding

1	1	1	1	0	0	0	0

$IV = c_0$ (bekannt)

Aufgabe 4 (Broadcast-attack)

Bem: Sei $n = 100$, $e = 3$, $m \in \{0, 1, 2, 3, 4\}$, $m^e = (m^e \bmod n)$

$\nearrow$ $c_1 := m^3 \bmod n_1$

Annahme: Alice $\rightarrow$ $c_2 := m^3 \bmod n_2$

m $c_3 := m^3 \bmod n_3$

$e = 3$ **für alle Teilnehmer**

$ggT(n_i, n_j) = 1$, wenn $i \neq j$

$m < min(n_1, n_2, n_3)$

Serie 5

Aufgabe 1

(n, e), (n, d) RSA-Schlüssel Oscar

(n, e_A), $(n, ?)$ RSA-Schlüssel Alice

unbekannt p, q $(n = p \cdot q)$ bzw. $\varphi(n)$

Ziel: Finde $\tilde{d_A}$ mit falls $c = m^{m_A} \bmod n$ ist, gilt $m = c^{\tilde{d_A}} \bmod n$

Oscar: $h := e \cdot d - 1$ (Es gilt $ed - k\varphi(n) = 1$, $\varphi(n) \mid h$)

$h := \frac{\overset{k\varphi(n)}{h}}{ggT(\underbrace{ed-1}_{k\varphi(n)}, e_A)}$ $(ggT(e_A, \varphi(n)) = 1$, $\varphi(n) \mid h)$

$d := ggT(h, e_A)$, $h := \frac{h}{d}$ $(\varphi(n) \mid h)$

$e_A \cdot \alpha + h \cdot \beta = 1$

$\boxed{e_A \cdot \tilde{\alpha} + \varphi(n) \cdot \tilde{\beta} = 1}$ löst der Provider

$\tilde{d_A} := \alpha \bmod h$

Behauptung: $m = c^{\tilde{d_A}} \bmod n = (m^{e_A})^{\tilde{d_A}} \bmod n = m^{e_A \cdot \tilde{d_A}} \bmod n = m^{1+h^{\tilde{\beta}}} = m \cdot (m^h)^{\tilde{\beta}} \bmod n$ $((m^h)^{\tilde{\beta}} =$

```
n = 78654787
e = 11
d = 64339331
ea = 17
c = m. power_mod(ea, n)
h = e * d - 1
gcd(h, ea) //1
xgcd(ea, h) //1, alpha, beta
dd = a % h
mm = c. power_mod(dd, n)
m = 1337
```

Serie 7

Aufgabe 1

$exp_{a} : \mathbb{Z}_6 \to \mathbb{Z}_7$
$exp_{a} : x \to a^x \bmod 7$

$(\mathbb{Z}_6, \oplus, 0) : \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
$(\mathbb{Z}_7, \oplus, 1) : \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

a	0	1	2	3	4	5
2	1	2	4	1	2	3
3	1	3	2	6	4	5

a=3 $\Rightarrow$ exp_a beistz eine Umkehrbabbildung: $ind_a : \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$

a) $ind_3(5) = 5$

b) $ind_3(3) = 1$

Aufgabe 2

a)

n=403
$[\sqrt{403}] = 20$

t	$t^2 - n$	$t^2 - n = s^2, s \in \mathbb{N}?$
21	441-403 = 23	nein
22	484 - 403 = 81	$81 = 9^2$: ja

$\Rightarrow t = 22, s = 9 \to a = (t + s) = 31, b = (t - s) = 13$
$\Rightarrow n = 403 = 13 * 31$

b)

$n = 187$ $a = 2$ $k = 10$
Berechne: $ggT(a^k - 1, n) = ggT(1023, 187) = 11$
$p := 11$
$q := \frac{n}{p} = \frac{187}{11} = 17$

Ergänzung: B=10
Gesucht:

$$\left.\begin{array}{l} q \in \mathbb{P} mit q \leq 10 : \{2, 3, 5, 7\} \\ \beta(q, B) : q^{\beta(q,B)} \leq \beta < q^{\beta(q,B)+1} \\ \beta(2, 10) = 3,\ \beta(2, 10) = 2, \beta(5, 10) = \beta(7, 10) = 1 \end{array}\right\} k := \prod q^{\beta(q,B)} = 2^3 * 3^2 * 5 * 7 = 72 * 35 = 2520$$

Sage:
$gcd(\underbrace{2.powermod(k, n) - 1}_{0}, n)$

Aufgabe 3

$factor(n)$
10000993
1000003

Aufgabe 4

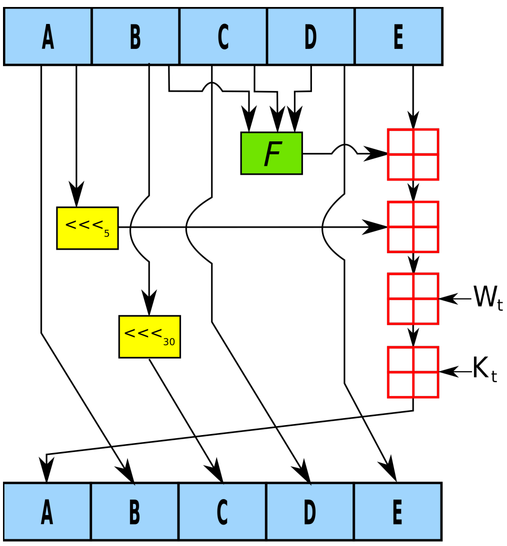
```
factor(n) = p * q
phi = (p-1)(q-1)
d=e.inverse_mod(phi)
(n.nth_root(4)).n() // *.n() = numerisch
```

Wieners Attacke: $0 < d \leq \frac{1}{3} * \sqrt[4]{n}$

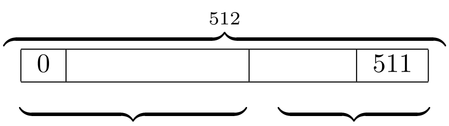
$e = 18439769619$

Serie 8

Aufgabe 1



Aufgabe 2



$\underbrace{0110011011001010}_{m}10\ldots010000,\ |m| = 16 = (10000)_2$

Nr.	Bit
0	0
8	1
13	0
15	0
16	0
17	0
401	0
500	0
510	0
511	0

Aufgabe 3

1. 11
2. Padding-Block
3. c_3 und c_4
4. 53
5.