

Hilfsblatt zur Kryptographie

Alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

κ -Werte.

Deutsch: $\kappa_D = 0,0762$, Englisch: $\kappa_E = 0,0669$, Französisch: $\kappa_F = 0,0746$.

RSA.

Public key: $(n, e) \in \mathbb{N} \times \mathbb{Z}_{\varphi(n)}^*$,
 $n = pq$, $p \neq q$ prim,
Private key: $d = e^{-1} \pmod{\varphi(n)}$,
Nachricht: $m \in \{1, \dots, n-1\}$,
Verschlüsselung: $c = m^e \pmod{n}$,
Entschlüsselung: $m = c^d \pmod{n}$.

Rabin.

Public key: $n = pq$ für Primzahlen $p \neq q$,
 $p, q \equiv 3 \pmod{4}$,
Private key: (p, q) ,
Nachricht: $m \in \{1, \dots, n-1\}$,
Verschlüsselung: $c = m^2 \pmod{n}$,
Entschlüsselung: bestimme Quadratwurzeln
modulo n .

ElGamal.

Systemparameter: Primzahl p ,
Primitivwurzel a modulo p ,
Private key: $x \in \{2, \dots, p-2\}$,
Public key: $y = a^x \pmod{p}$,
Nachricht: $m \in \{1, \dots, p-1\}$,
Verschlüsselung: wähle zuf. $k \in \{2, \dots, p-2\}$,
 $K = y^k \pmod{p}$,
 $c_1 = a^k \pmod{p}$,
 $c_2 = Km \pmod{p}$,
 $c = (c_1, c_2)$,
Entschlüsselung: $K = c_1^x \pmod{p}$,
 $K^{-1} = c_1^{p-1-x} \pmod{p}$,
 $m = K^{-1}c_2 \pmod{p}$.

Goldwasser-Micali.

Public key: $n = pq$ für $p \neq q$ prim,
 $y \in \mathbb{Z}_n$ Pseudoquadrat modulo n ,
Private key: (p, q) ,
Nachricht: $m = (m_1, \dots, m_t) \in \{0, 1\}^t$,
Verschlüsselung: wähle stoch. unabh. Zufallszahlen
 $x_1, \dots, x_t \in \mathbb{Z}_n^*$,
 $c_i = \begin{cases} yx_i^2 \pmod{n}, & \text{falls } m_i = 1, \\ x_i^2 \pmod{n}, & \text{falls } m_i = 0, \end{cases}$
 $i = 1, \dots, t$.
 $C = (c_1, \dots, c_t)$,

Entschlüsselung:

$$m_i = \begin{cases} 0, & \text{falls } \left(\frac{c_i}{p}\right) = 1, \\ 1, & \text{sonst,} \end{cases}$$
$$i = 1, \dots, t,$$
$$m = (m_1, \dots, m_t).$$

Blum-Goldwasser.

Public key: $n = pq$ für Primzahlen $p \neq q$,
 $p, q \equiv 3 \pmod{4}$,
Private key: (p, q, a, b) mit $ap + bq = 1$,
Nachricht: $m = (m_1, \dots, m_t) \in \{0, 1\}^{ht}$
mit $h \leq \log_2 \lfloor \log_2 n \rfloor$,
Verschlüsselung: wähle zuf. QR x_0 modulo n ,
 $x_i = x_{i-1}^2 \pmod{n}$, $i = 1, \dots, t+1$,
 b_i : letzte h Bits von x_i ,
 $c_i = m_i \oplus b_i$, $i = 1, \dots, t$,
 $C = (c_1, \dots, c_t, x_{t+1})$,
Entschlüsselung: $d_1 = \left(\frac{p+1}{4}\right)^{t+1} \pmod{p-1}$,
 $d_2 = \left(\frac{q+1}{4}\right)^{t+1} \pmod{q-1}$,
 $u = x_{t+1}^{d_1} \pmod{p}$, $v = x_{t+1}^{d_2} \pmod{q}$,
 $x_0 = vap + ubq \pmod{n}$,
 $x_i = x_{i-1}^2 \pmod{n}$, $i = 1, \dots, t+1$,
 b_i : letzte h Bits von x_i ,
 $m_i = c_i \oplus b_i$, $i = 1, \dots, t$,
 $m = (m_1, \dots, m_t)$.

ElGamal-Signaturen.

Systemparameter: Primzahl p ,
Primitivwurzel a modulo p ,
Private key: $x \in \{2, \dots, p-2\}$,
Public key: $y = a^x \pmod p$,
Hashfunktion: $h : \{0, 1\}^* \rightarrow \{1, \dots, p-1\}$,
Dokument: $m \in \{0, 1\}^*$,
Signatur: wähle zuf. $k \in \{2, \dots, p-2\}$,
 $\text{ggT}(k, p-1) = 1$,
berechne $r = a^k \pmod p$,
 $k^{-1} \pmod{p-1}$, $h(m)$,
 $s = k^{-1}(h(m) - xr) \pmod{p-1}$
die Signatur von m ist (r, s) ,
Verifizierung: prüfe $1 \leq r \leq p-1$,
 $v_1 = y^r r^s \pmod p$,
 $v_2 = a^{h(m)} \pmod p$,
akzeptiere, falls $v_1 = v_2$.

DSA.

Systemparameter: Primzahlen p, q mit $q \mid p-1$,
 $a \in \mathbb{Z}_p^*$ Element der Ordnung q ,
Private key: $x \in \{2, \dots, q-1\}$,
Public key: $y = a^x \pmod p$,
Hashfunktion: $h : \{0, 1\}^* \rightarrow \{1, \dots, q\}$,
Dokument: $m \in \{0, 1\}^*$,
Signatur: wähle zuf. $k \in \{2, \dots, q-1\}$,
berechne $r = (a^k \pmod p) \pmod q$,
 $k^{-1} \pmod q$, $h(m)$
 $s = k^{-1}(h(m) + xr) \pmod q$
die Signatur von m ist (r, s) ,
Verifizierung: prüfe $0 < r < q$ und $0 < s < q$,
berechne $w = s^{-1} \pmod q$ und $h(m)$,
 $u_1 = wh(m) \pmod q$, $u_2 = rw \pmod q$,
 $v = (a^{u_1} y^{u_2} \pmod p) \pmod q$,
akzeptiere, falls $v = r$.

Feige-Fiat-Shamir-Identifikation.

Systemparameter: Primzahlen $p \neq q$, $p, q \equiv 3 \pmod 4$,
TA publiziert $n = pq$,
jeder Benutzer wählt $s_1, \dots, s_k \in \{1, \dots, n-1\}$,
 $\text{ggT}(s_i, n) = 1$,
und publiziert $v_i = (s_i^2)^{-1} \pmod n$, $i = 1, \dots, k$,
Protokoll: A wählt Zufallszahl r ,
berechnet $x = r^2 \pmod n$,
 $A \rightarrow B: x$,
 B wählt Zufallsbits $b_1, \dots, b_k \in \{0, 1\}$,
 $A \leftarrow B: (b_1, \dots, b_k)$,
 A berechnet $y = r \prod_{j=1}^k s_j^{b_j} \pmod n$,
 $A \rightarrow B: y$,
 B berechnet $z = y^2 \prod_{j=1}^k v_j^{b_j} \pmod n$,
akzeptiert, falls $z = x$.

Additionsformeln für elliptische Kurven.

Es seien $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2) \in E(L)$ für $L \supseteq K$.

(i) Falls $P_1 \neq \pm P_2$, dann gilt $P_1 + P_2 = (x_3, y_3)$ mit

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2,$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1,$$

(ii) falls $P_1 \neq -P_1$, dann gilt $2P_1 = P_1 + P_1 = (x_3, y_3)$ mit

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1,$$

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3) - y_1.$$