Verschlüsselung

Division mit Rest

Bsp. $17 = 3 \cdot 5 + 2$

ggT

$(a, b) = d$ d teilt a 2 b

euklidischer Algorithmus

1. a und b $(a > b)$

   $a = q_1 \cdot b + r_1$

2. $b = q_2 \cdot r_1 + r_2$

3. $r_1 = q_3 \cdot r_2 + r_3$

... bis $+ 0$

Bsp.

$a = 3182$ $b = 711$

$3182 = 4 \cdot 711 + 338$

$711 = 2 \cdot 338 + 35$

$338 = 9 \cdot 35 + 23$

$35 = 1 \cdot 23 + 12$

$23 = 1 \cdot 12 + 11$

$12 = 1 \cdot 11 + 1$

$11 = 11 \cdot 1 + 0$

$(3182, 711) = 1$

Linearkombination

1. euklidischer Algorithmus

2. $(a, b) = x \cdot a + y \cdot b$

Bsp.

1. $220 = 1 \cdot 175 + 45$

   $175 = 3 \cdot 45 + 40$

   $45 = 1 \cdot 40 + 5$

   $40 = 8 \cdot 5 + 0$ ggT: 5

2. $5 = 45 - 40$

   $= 45 - (175 - 3 \cdot 45)$

   $= 4 \cdot 45 - 175$

   $= 4 \cdot (220 - 175) - 175$

   $= 4 \cdot 220 - 5 \cdot 175$

Primzahlen

p $(p > 1)$ ist eine Primzahl, wenn sie nur durch $\pm p$ und durch ± 1 teilbar ist

Rechnen mit Resten

Bsp. Modul $n = 7$

$2 \oplus 3 = 5$

$4 \oplus 5 = 2$ oder $R_7(9) = 2$

Kongruent

Gleichwertig Bsp. $1'000 \equiv 6 \mod 7$

Reste mit grossen Zahlen

$R_n(a \cdot b \cdot c) = R_n(R_n(R_n(a) \cdot R_n(b)) \cdot R_n(c))$

Bsp.

$R_{11}(215 \cdot 718 \cdot 123) = R_{11}(R_{11}(215) \cdot R_{11}(718) \cdot R_{11}(123))$

$= R_{11}(6 \cdot 3 \cdot 2) = 3$

$R_n(m^c)$

Bsp.

$R_{143}(2^{103}) = R_{143}(R_{143}(2) \cdot R_{143}(2^2) \cdot R_{143}(2^4) \cdot R_{143}(2^{32}) \cdot R_{143}(2^{64}))$

$\hookrightarrow 2^{103} = 2^{64} \cdot 2^{32} \cdot 2^4 \cdot 2^2 \cdot 2$

Bsp.

$R_{17}(15^{28}) \rightarrow 28 = 2^4 + 2^3 + 2^2$

$R_{17}(15^2) = 4$

$R_{17}(15^4) = 16$

$R_{17}(15^8) = 1$

$R_{17}(15^{16}) = 1$

Kleiner Satz von Fermat

Wenn p prim, dann $a^{p-1} \equiv 1$ für alle $a \neq 0 \mod p$

Bsp. $p = 7$ $a = 3$ $3^6 \equiv 1 \mod 7$

$\rightarrow$ Euler: $a^{k(p-1)(q-1)+1} \equiv a \mod n$ $n = p \cdot q$

RSA - Verfahren

1. 2 grosse Primzahlen p und q
2. $n = p \cdot q$
3. $\varphi(p \cdot q) = (p-1) \cdot (q-1) = r$
4. c gegeben $\rightarrow (c, r) = 1$ $\Leftarrow$ teilerfremd
5. als Linearkombination schreiben

$$d \cdot c = (c, r) + k \cdot r$$

Verschlüsseln / Entschlüsseln:

öffentlicher Schlüssel: c und n

privater Schlüssel : d und n

Verschlüsseln: $\bar{m} = R_n(m^c) = m^c \bmod n$

Entschlüsseln: $m = R_n(\bar{m}^d) = m^d \bmod n$

Authentizität und Integrität

Authentizität: Stammt die Nachricht wirklich von der Person mit dem privatem Schlüssel ? -> Nur der Besitzer des p. Schlüssels kann korrekte Signatur erstellen

Integrität: Sind die Daten unverändert? -> Mit Hash-Wert und dem öffentlichen Schlüssel kann überprüft werden ob die beiden Werte übereinstimmen.

Assymetrisch und Symmetrische Verschlüsselung

Sym.: ein einziger Schlüssel, der beide Partner kennen müssen

Assym.: zwei untersch. Schlüssel