**erweiterter Euklid**

$$x * a + y * b = d \quad d = ggT(a,b) \rightarrow erw.Euklid(1,0,0,1) \quad A'' = A - q * A' \quad | \quad B'' = B - q * B' \tag{1}$$

**Starke Primzahlen zu Basis b** Fermat Test erfuellt?

$$b^{n-1} \equiv 1 \mod n \quad \wedge \quad n - 1 = 2^s * t \quad s \in \mathbb{N} \quad und \quad t \in ungerade \tag{2}$$

$$[b^t \mod n] = 1 \vee [b^t \mod n] = n - 1 \vee [b^{2t} \mod n] = n - 1 \vee .... \vee [b^{2^{s-1}t} \mod n] = n - 1 \tag{3}$$

Wird der Test einmal $1 \rightarrow$ stopp $\rightarrow$ erfllt

**Starke Primzahlen zu Basis b auch Pseudoprimzahl zur Basis b**

$$b^{n-1} = (b^{2^s * t} - 1) = (b^t - 1)(b^t + 1)(b^{2*t} + 1)(b^{2^2 * t} + 1)...(b^{2^{s-1} * t} + 1) \tag{4}$$

**Pseudoprimzahl** Sei n eine zusammengesetzte Zahl n heisst Pseudoprimzahl zur Basis b wenn gilt: $b^{n-1} = 1 \mod n$ Sei n eine Pseudoprimzahl zu $b_1$ und $b_2$ dann ist sie auch Pseudoprim zu den Basen $b_1 * b_2$ und $b_1 * b_2^{-1}$

**Miller Rabin** Gegeben ist eine ungerade Zahl n:

$$n - 1 = 2^s * t \quad s \in \mathbb{N} \quad t = ungerade \quad \text{Wählen} \quad von \quad 1 < b < n - 1 \tag{5}$$

$$Berechne \quad [b^t \mod n] = (-1 \vee 1 \rightarrow (8)) \vee (\neq 1 \wedge \neq -1 \rightarrow (7)) \tag{6}$$

$$[b^{2^1 * t} \mod n], [b^{2^2 * t} \mod n], ...., [b^{2^{s-1} * t} \mod n] = n - 1 \rightarrow (8), sonst \quad n \neq prim \tag{7}$$

Falls die Anzahl der gewhlten Basen $\leq 40$, gehe zu (5) sonst ist n vermutlich prim (8)

**Anzahl Primzahlen zwischen n und m** m groessere Zahl, n kleinere Zahl

$$0.91... \frac{m}{ln(m)} - 2.13... \frac{n}{ln(n)} \tag{9}$$

**Faktorisieren mit Methode von Fermat**

$$n = p * n = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2 = x^2 - y^2 = (x-y)(x+y)$$

$$y^2 = x^2 - n \quad \text{How to:}$$

$$k = \lceil \sqrt{n} \rceil \rightarrow \sqrt{n} = \sqrt{p * q} \rightarrow \text{geometrisches Mittel}; x = k$$

$x^2 - n$ Quadratzahl? endet sie auf $2, 3, 7$ oder $8$, dann sicher keine Quadratzahl, sonst $\sqrt{x^2 - n}$

Es ist eine Quadratzahl $\rightarrow$ wir sind fertig$n = (x-y)(x+y)$ Es ist keine Quadratzahl $\rightarrow k \mathrel{+}= 1$

x ist das letzte $k$, y wird berechnet via k++, danach noch p und q

**Pollards (y-1) Methode** p = Prim, b = Basis mit ggT(b,y) = 1. dann gilt: $b^{y-1} \equiv 1 \mod p$. Einer der beiden Primfaktoren muss in lauter kleine Primfaktoren zerfallen. Sei M eine Zahl mit folgenden Eigentschaften: 1. $p - 1 \mid M$ (p-1 ist ein Teiler von M) 2. $M \nmid p - 1$ (M ist kein Teiler von p-1)

Sei b eine Basis mit $ggT(b,n) = 1$. M waehlen: $k!$ oder $kgv(1,2,3,...,k)$

$$b^M - 1 \rightarrow [b^M - 1 \mod n] = [b^M \mod n] - 1 \rightarrow d := ggT([b^M \mod n] - 1, n) \tag{10}$$

$$d = \begin{cases} 1 & b^M \not\equiv 1 \mod p \wedge b^M \not\equiv 1 \mod q \quad \text{M groesser waehlen} \\ n & b^M \equiv 1 \mod p \wedge b^M \equiv 1 \mod q \quad \text{Basis b wechseln oder M kleiner waehlen} \\ p & b^M \equiv 1 \mod p \wedge b^M \not\equiv 1 \mod q \\ q & b^M \not\equiv 1 \mod p \wedge b^M \equiv 1 \mod q \end{cases} \tag{11}$$

**Ordnung eines Elementes in einer zyklischen Gruppe (G, *)** $\mathbb{Z}_n^*$ Alle Teiler in $\mathbb{N}$ sind mgliche Ordnungen der Elemente. Ein Generator der Gruppe ist ein Element, wenn es dieselbe Ordnung besitzt wie die Gruppe. Mit dem Generator kann die gesamte Gruppe erzeugt werden. $g^{TeilerderGruppen-1}, g^x, ...g^{n-1}$, wobei $g^{n-1} = 1 \mod n$ ist, wenn es ein Generator der Gruppe ist. Kommutativ $\rightarrow$ a, b sind Elemente der Gruppe, g ein Generator: $a*b = g^m * g^m = g^{n+m} = g^{n+m} = g^n * g^m = b*a$. Operation ist assoziativ $(a*b)*c = a*(b*c)$ Es existiert ein Neutralelement $a*e = e*a = a$ Zu jedem Element existiert ein Inverses, sodass: $a*a^{-1} = a^{-1}*a = e$

**Babystep Giantstep Algorithmus** $y = g^x$ gesucht ist $x$, y, g und p (Gruppenordnung) sind gegeben. $Q = \lceil \sqrt{p-1=N} \rceil$ Q ist also die kleinste natrliche Zahl mit $Q^2 \geq N$
$x = k*Q - l$ wobei $1 \geq k \geq Q \quad 0 \geq l \geq Q-1 \quad y = g^{k*Q-l} \rightarrow g^{k*Q} = g^l * y$
Babystep Liste: $\{[y*g^l \mod p] : l = \{0,1,2,...,Q-1\}\}$ ACHTUNG 0
Giantstep Liste: $\{[g^{k*Q} \mod p] : k = \{1,2,3,...,Q\}\}$ ACHTUNG 1
Die Babystep Liste wird sortiert nach Resultat (Resultat, Index).
In Giantstep Liste suchen nach vorkommen eines Babystep Elementes. $k = x \rightarrow g^{x*Q} \mod p =$ (Resultat, Index (Babystep Liste)), dann sind k und l klar. $\rightarrow$ x = k * Q - l

**DH Keyexchange** Public: $g$ und $p$ Alice bestimmt Zufallszahl $a \in \{1,2,3,...,p-1\}$ und publiziert $[A := g^a \mod p]$ Bob tut dasselbe für $[B := g^b \mod p]$
Beide können den geheimen Schlüssel $k$ berechnen mit: $A^b = B^a = g^{a*b} \mod p = k$
Für Elliptische Kurven (gegeben a, b, p): Basispunkt $B = (x_1, y_1)$; Alice nimmt Zufallszahl $k_a$, Bob $k_b$. Alice rechnet $k_a * B = (x_1, y_1) * k_a \rightarrow \alpha \equiv (3x_1^2 + a)(2y_1)^{-1} \quad x_3 \equiv \alpha^2 - 2x_1 \quad y_3 = \alpha(x_1 - x_3) - y_1$ Task von Alice, dasselbe fr Bob, publiziert wird dann jeweils $n*B =$ pk (n* addierter Basispunkt).
Sessionkey $= (n*B)*k_x$ (erneut Punktaddition)

**El Gamal** Public: $g$ und $p$ Schlsselerzeugung: Zufallszahl $a$ in der Menge $[1,2,3,...p-1]$ wählen (sk) $A := g^a \mod p$ ist pk Alice will eine Nachricht m an Bob senden.
B = pk von Bob. Randomanteil: $R = [g^r \mod p] \quad r \in \{1,2,3,...,p-1\}$
$c = m * B^R \mod p$, sie schickt das Tupel $(R, c)$ an Bob. Bob dechiffriert folgendermassen:
$R^b = g^{k*b} \mod p \rightarrow B^k = g^{kb}$ Aus c kann er anhand von $g^{(kb)^{-1}}$ $m$ berechnen. $g^{(kb)^{-1}} * c \mod p = m$
Elliptische Kurven: Alice an Bob, $B = (x, y)$, $PK_b = b*B$ und $p$ sind public. Nachricht $= P_m$
Alice nimmt Zufallszahl k und schickt $(k*B, P_m + k(PK_b))$ Bob seinerseits muss folgendes machen: $P_m + k(PK_b) - b(k*B)$ Subtraktion $b*kB$ was er erhalten hat.

**Elliptische Kurven** $y^2 = x^3 + a*x + b$ Alle Punkte auf dieser Kurve. Hinzu kommt ein Punkt im Unendlichen $\sigma$. 1.) $P = \sigma : -P = \sigma$ 2.) $P = (x,y) \neq \sigma : -P = (x, -y)$
Addition zweier Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ $P_1 \wedge P_2 \neq \sigma \quad x_1 \neq x_2$

$$P_1 + P_2 = P_3(x_3, y_3) \quad \alpha = \frac{y_2 - y_1}{x_2 - x_1} = (y_2 - y_1)(x_2 - x_1)^{-1} \mod p \begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = \alpha(x_1 - x_3) - y_1 \end{cases}$$

$$P_1 + P_2 = \sigma \quad x_1 = x_2 \wedge y_1 \neq y_2 \qquad P_1 = P_2 \wedge y_1 = 0 \rightarrow P_1 + P_2 = \sigma$$

$$P_1 = P_2 \wedge y_1 \neq 0 \begin{cases} x_3 = \alpha^2 - 2x_1 \mod p \\ y_3 = \alpha(x_1 - x_3) - y_1 \mod p \\ \alpha = (3x_1^2 + a)(2y_1)^{-1} \end{cases}$$

**Quadratische Reste** p = Prim und $a \in F_p$; $x^2 \mod p$ ist ein quadratischer Rest wenn $x^2 \equiv a \mod p$
Die hälfte der Elemente des Fields sind quad. Reste resp. quad-nicht-Reste.

$$a^{\frac{p-1}{2}} \begin{cases} 1 \mod p & \text{a quad Rest mod p} \\ -1 \mod p & \text{a quad Nicht-Rest mod p} \end{cases} \tag{12}$$

Ist $a \in F_p$ ein quad. Rest, dann gilt für die Wurzel: $r_1 = a^{\frac{p+1}{4}}$ falls $p \equiv 3 \mod 4$ und $r_2 = p - r_1$