Schlüsselerzeugung

Primzahl p, Primitivwurzel $g \bmod p$, $a \in \{0, \ldots, p-2\}$ (zufällig und gleichverteilt):
Alice berechnet $A = g^a \bmod p$
$\Rightarrow$ Öffentlicher Schlüssel (p, g, A), geheimer Schlüssel a.
Schlüsselanteil von **Alice** ein für allemal fest und öffentlich)

Verschlüsselung

zu verschlüsselnder Klartext $m \in P$ mit Klartextraum $P = \{0, 1, \ldots, p-1\}$, öffentlicher Schlüssel gegeben.
Bob wählt Zufallszahl $b \in \{1, \ldots, p-2\}$:
Bob berechnet $B = g^b \bmod p$ und $c = mA^b \bmod p$
$\Rightarrow$ geheimer Schlüsselanteil b von **Bob** und er schickt Schlüsseltext (B, c) an **Alice**

Entschlüsselung

Alice erhält (B, c) und kennt ihren geheimen Schlüsselanteil a.
Bestimmt $x = p - 1 - a$
$\Rightarrow$ **Alice** berechnet $B^x c \bmod p = m$

Effizienz

Bob kann $A^b \bmod p$ und $B = g^a \bmod p$ vorausberechnen (da unabhängig von m).
Nachteil: *Nachrichtenexpansion:* Schlüsseltext (B, c) doppelt so lang wie Klartext!

Parameterwahl

Primzahl p wenigstens 512 Bits, besser 768 oder sogar 1024 Bits lang, am besten p zufällig und gleichverteilt wählen! **Bob** muß bei jeder Verschlüsselung neues b wählen!

Allgemeines Verfahren

1. Sei $(G, \circ)$ endliche Gruppe, $g \in G$ und $H =< g >$
2. Wähle $a \in \{1, \ldots, |H| - 1\}$ zufällig, berechne $A = g^a$ (Rechnen in $(G, \circ)$!)
3. Klartextraum $P = G$, Chiffrentextraum $C = G \times G$
4. Öffentlicher Schlüssel $K = ((G, \circ), g, A)$, geheimer Schlüssel a
5. Verschlüsselung mit öffentlichem Schlüssel K:
   - Klartext m in Gruppe G darstellen
   - Wähle $b \in \{1, \ldots, |H| - 1\}$ zufällig
   - Berechne $C_1 = g^b$, $C_2 = m \circ A^b$
   - $E_k(m) =_{def} (C_1, C_2)$
6. Entschlüsselung mit privatem Schlüssel $K = a$: für Chiffrentext $C = (C_1, C_2)$ definiere $D_k(C) =_{def} C_2 \circ (C_1^a)^{-1}$ und es gilt:

$$D_k(E_k(m)) = D_k(g^b, m \circ A^b) = (m \circ A^b) \circ ((g^b)^a)^{-1} = m \circ (g^a)^b \circ ((g^b)^a)^{-1} = m$$

Sonstiges

	512 bits	**768 bits**	**1024 bits**
Verschlüsselung	0,33 sec	0,80 sec	1,09 sec
Entschlüsselung	0,24 sec	0,58 sec	0,77 sec

(SPARC II, Exponentenlänge 160 Bits, unterschiedliche Modullängen)