

Geschichte

Juli 1985 von Taher ElGamal (* 18. August 1955) veröffentlicht

Schlüsselerzeugung

Primzahl p , Primitivwurzel $g \bmod p$, $a \in \{0, \dots, p-2\}$ (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)

Bsp.: Wähle $p = 23, g = 7, a = 6 \Rightarrow A = g^a \bmod p = 4 \Rightarrow$ Schlüssel $(p = 23, g = 7, A = 4)$

Verschlüsselung

zu verschlüsselnder Klartext $m \in P$ mit Klartextraum $P = \{0, 1, \dots, p-1\}$, öffentlicher Schlüssel (p, g, A) gegeben. **Bob** wählt Zufallszahl $b \in \{1, \dots, p-2\}$:

Bob berechnet $B = g^b \bmod p$ und $c = mA^b \bmod p$

\Rightarrow geheimer Schlüsselanteil b , **Bob** schickt Schlüsseltext (B, c) an **Alice**

Bsp.: Sei $m = 7, b = 3, \Rightarrow B = 21, c = 11 \Rightarrow$ Schlüsseltext $(B, c) = (21, 11)$

Entschlüsselung

Alice erhält (B, c) und kennt ihren geheimen Schlüsselanteil a . Bestimmt $x = p-1-a$

\Rightarrow **Alice** berechnet $B^x c \bmod p = m$

Bsp.: Entschlüsselt wird $B^{p-1-a} c \bmod p = 21^{23-1-6} \cdot 11 \bmod 23 = 7 = m$

Effizienz

Entschlüsselung eine, Verschlüsselung zwei modulare Exponentiationen.

aber: **Bob** kann $A^b \bmod p$ und $B = g^a \bmod p$ vorausberechnen (da unabhängig von m).

Nachteil: *Nachrichtenerpansion:* Schlüsseltext (B, c) doppelt so lang wie Klartext!

ElGamal und Diffie-Hellman

ElGamal genauso schwer zu brechen wie Diffie-Hellman

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!

ElGamal als randomisiertes Verschlüsselungsverfahren

Verschlüsselungsprozeß wird durch zufällige Wahl von b randomisiert, dadurch wird Kryptoanalyse, z.B. durch statistische Tests erschwert.

Verallgemeinerung

Wichtiger Vorteil von ElGamal: nicht nur in primen Restklassengruppen modulo Primzahl, sondern in jeder anderen zyklischen Gruppe anwendbar. Einige geeignete Gruppen:

1. Jakobische Varietät hyperelliptischer Kurven überendlichen Körpern
2. Klassengruppe imaginär-quadratischer Ordnung
3. Punktgruppe einer elliptischen Kurve über endlichem Körper

Allgemeines Verfahren

1. Sei (G, \circ) endliche Gruppe, $g \in G$ und $H = \langle g \rangle$
2. Wähle $a \in \{1, \dots, |H| - 1\}$ 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 $b \in \{1, \dots, |H| - 1\}$ zufällig
 - Berechne $C_1 = g^b$, $C_2 = m \circ A^b$
 - $E_k(m) =_{\text{def}} (C_1, C_2)$

6. Entschlüsselung mit privatem Schlüssel $K = a$: für Chiffrentext $C = (C_1, C_2)$ definiere $D_k(C) =_{\text{def}} C_2 \circ (C_1^a)^{-1}$ 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

ElGamal-Verfahren **nicht** patentiert; Anwendung etwa in PGP 5.0.

Berechnungsdauer (SPARC II, Exponentenlänge 160 Bits, unterschiedliche Modullängen):

| | 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 |