Chiffrierung nach ELGAMAL

CryptoCon13

14. April 2013

sublab

Agenda

Allgemeines

- ElGamal-Verfahren ist ein asymmetrisches Chiffrierverfahren, d.h., Chiffrierschlüssel $\neq$ Dechiffrierschlüssel
- asymmetrische Chiffrierverfahren mit großer Rechenintensität verbunden $\rightarrow$ oft nur in Kombination mit symmetrischen Verfahren eingesetzt
- Beschreibung des ElGamal-Verfahren u. a. im „Handbook of Applied Cryptography“ (online verfügbar)

Erzeugung des Schlüsselpaares

1. Bestimme große, sichere Primzahl $p = 2q + 1$, so daß auch q eine Primzahl ist
2. Bestimme primitives Element α[1] bzgl. $\mathbf{Z}_p^*$
3. Wähle ein beliebiges a mit $1 \leq a \leq p - 2$.
4. Berechne $\beta := \alpha^a \bmod p$.

- Öffentlicher Schlüssel $\mathcal{K}_{\text{pub}} := (p, \alpha, \beta)$
- Privater Schlüssel $\mathcal{K}_{\text{prv}} := (p, a)$

[1] $\mathbf{Z}_p^* = \{\alpha^i \bmod p \mid 0 \leq i \leq p-2\}$

Verschlüsselung mit öffentlichem Schlüssel

- Sei $x \in \mathscr{P}$ mit $0 \leq x \leq p-1$ beliebiger Klartextblock
- Wähle für jeden Klartextblock ein zufälliges λ mit $1 \leq \lambda \leq p-2$
- $y_1 := \alpha^{\lambda} \mod p$
- $y_2 := x \cdot \beta^{\lambda} \mod p$
- $\mathscr{E}_{\mathscr{K}_{\text{pub}}}(x) := (y_1, y_2)$

- Geheimtext doppelt so lang wie der Klartext
- Menge möglicher Geheimtexte größer als Menge der Klartexte $\rightarrow$ probabilistische Verschlüsselung

Entschlüsselung mit privatem Schlüssel

$$\begin{aligned}
\mathscr{D}_{\mathscr{K}_{\text{prv}}}(y_1, y_2) &:= y_2 \cdot y_1^{-a} \bmod p \\
&:= x \cdot \beta^{\lambda} \cdot \alpha^{-a\lambda} \bmod p \\
&:= x \cdot \alpha^{a\lambda} \cdot \alpha^{-a\lambda} \bmod p \\
&= x
\end{aligned}$$

Verringerung des Rechenaufwandes durch Anwendung des Kleinen Satzes von Fermat:

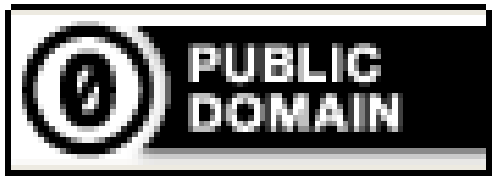
$$\mathscr{D}_{\mathscr{K}_{\text{prv}}}(y_1, y_2) := (y_2 \bmod p) \cdot (y_1^{p-1-a} \bmod p)$$

Sicherheit

- Brechen der ElGamal-Chiffrierung bei bekanntem öffentlichen Schlüssel und Geheimtext $\rightarrow$ Diffie-Hellman-Problem
- Bis zum heutigen Zeitpunkt: Lösen des Diffie-Hellman-Problems nur über Berechnung diskreter Logarithmen
- Angriff: privaten Schlüsselteil a aus dem öffentlichen Schlüssel (p, α, β) berechnen: $\beta \equiv \alpha^a \bmod p$
- Berechnen von a (sog. diskreter Logarithums) schwer im Vergleich zur Berechnung von $\beta \rightarrow$ Einwegfunktion

Weiterhin ist es wichtig, λ immer zufällig zu wählen und dafür einen gute Zufallsquelle zu verwenden.

Lizenz



To the extent possible under law, the person who associated CC0 with this work has waived all copyright and related or neighboring rights to this work.
`http://creativecommons.org/publicdomain/zero/1.0/deed.de`