# 1 Primitivwurzel

Eine Zahl $g$ ist eine Primitivwurzel von $p$, wenn gilt:

$$g^i \mod p \;:\; \{0,1,2,\ldots,p-2\} \longleftrightarrow \{1,2,\ldots,p-1\} \tag{1}$$

Die beiden Mengen $\{1,2,\ldots,p-1\}$ und $\{0,1,2,\ldots,p-2\}$ sind bijektiv, das heißt, dass jedes Element der Menge $\{1,2,\ldots,p-1\}$ genau einmal als Ergebnis der Kongruenz $g^i \mod p \quad \forall\, i \in \{0,1,2,\ldots,p-2\}$ auftritt. Nur wenn dies der Fall ist, ist $g$ eine Primitivwurzel von $p$.

Als Beispiel: 3 ist eine Primitivwurzel Modulo 7, denn es gilt:

$$\begin{aligned}
3^0 &\equiv 1 \pmod 7\\
3^1 &\equiv 3 \pmod 7\\
3^2 &\equiv 2 \pmod 7\\
3^3 &\equiv 6 \pmod 7\\
3^4 &\equiv 4 \pmod 7\\
3^5 &\equiv 5 \pmod 7
\end{aligned}$$

# 2 Diffie-Hellman Schlüsselaustausch

Alice und Bob wählen eine ungerade Primzahl $p$ und eine ihrer Primitivwurzeln $g$. Alice und Bob tauschen $p$ und $g$ aus. Hierbei ist es unerheblich, wenn Dritte in den Besitz dieser Informationen kommen.

Alice und Bob wählen nun zufällig jeweils eine Zahl $X_A$ bzw. $X_B$, für die gilt $X_{A/B} < p$, die sie geheim halten. Alice berechnet nun $Y_A \equiv g^{X_A} \mod p$, Bob verfährt analog mit seiner Zahl $X_B$: $Y_B \equiv g^{X_B} \mod p$.

Die Zahlen $Y_A$ bzw. $Y_B$ werden nun ausgetauscht. Auch hierbei spielt es keine Rolle, wenn Dritte in den Besitz der Zahlen gelangen (→ Diskreter Logarithmus).

Alice berechnet nun $S_A \equiv (Y_B)^{X_A} \mod p$, Bob $S_B \equiv (Y_A)^{X_B} \mod p$. Sie beide kommen zu dem gleichen Ergebnis (für ein Beispiel siehe [3]), das sie nun als gemeinsamen Schlüssel, der niemand anderem bekannt ist, verwenden können, denn es gilt:

$$\begin{aligned}
S_A &= S_B\\
(Y_B)^{X_A} &\equiv (Y_A)^{X_B} \pmod p\\
(g^{X_B})^{X_A} &\equiv (g^{X_A})^{X_B} \pmod p\\
g^{X_B X_A} &\equiv g^{X_A X_B} \pmod p
\end{aligned}$$

Obwohl potentielle Dritte die Informationen $g$, $p$ und $Y_{A/B}$ mitbekommen können ist es für genügend große Zahlen unmöglich, auf die geheimen Zahlen $X_{A/B}$ zu schließen, mit Hilfe derer der geheime Schlüssel $S$ aus einem abgefangenen $Y_{A/B}$ berechnet werden könnte. Dieses Problem wird auch als *Diskreter Logarithmus* bezeichnet. Auf ihm basieren viele moderne Kryptosysteme, unter anderem auch RSA.

Es ist leicht, bei bekanntem $x$ das Ergebnis $m \equiv b^x \mod n$ zu berechnen, nicht jedoch aus der Basis $b$, der Modulo-Zahl $n$ und dem Ergebnis der Kongruenz $m$ auf den Exponenten $x$ zu schließen. Der Diskrete Logarithmus wird daher auch als Einweg- oder Trapdoor-Funktion bezeichnet.

# 3 ElGamal

Das ElGamal-Kryptosystem (gesprochen: *Al-Dschamal*) funktioniert – ähnlich wie der Diffie-Hellman-Schlüsselaustausch – auch mit Primitivwurzeln und Primzahlen und ist ein verbreitetes Public-Key-Verfahren.

## 3.1 Die Schlüsselerzeugung

Der öffentliche ElGamal-Schlüssel besteht aus den drei Elementen,

1. $p$, einer großen, zufällig erzeugten Primzahl,
2. $g$, einer Primitivwurzel von $p$ und
3. $g^a \mod p$, wobei $a$ eine zufällig erzeugte, geheime Zahl $1 \leq a \leq p-2$ darstellt.

$$\text{Public Key} = (p, g, (g^a \mod p)) \tag{2}$$

Der geheime Schlüssel ist lediglich die Zahl $a$, wenngleich $p$ bei der Entschlüsselung auch benötigt wird.

## 3.2 Der Verschlüsselungsprozess

Für die zu verschlüsselnde Nachricht $m$ muss gelten: $m \leq p-1$. (Ist $m \geq p$, dann muss $m$, genau wie beim RSA-Verfahren, in mehrere Blöcke, die jeweils kleiner als $p$ sind, aufgeteilt werden.)

Der verschlüsselte Text besteht aus zwei Bestandteilen $\gamma$ und $\delta$, die wie folgt zu berechnen sind, wobei $k$ für eine zufällige Zahl $1 \leq k \leq p-2$ steht:

$$\gamma \equiv g^k \mod p \tag{3}$$
$$\delta \equiv m \cdot (g^a)^k \mod p \tag{4}$$

Dem Empfänger wird der verschlüsselter Text $c = (\gamma, \delta)$ gesandt.

## 3.3 Der Entschlüsselungsprozess

Das Entschlüsseln ist wesentlich einfacher, der Klartext $m$ lässt sich wie folgt errechnen:

$$(\gamma^{p-1-a}) \cdot \delta \equiv (\gamma^{-a}) \cdot \delta \equiv \frac{\delta}{\gamma^a} \equiv m \pmod p \tag{5}$$

Der Bruch $\frac{\delta}{\gamma^a}$ steht hier nicht für eine Division, wie sie bei reellen Zahlen durchgeführt wird, sondern für die Multiplikation mit dem Inversen Element von $\gamma^a$. Das Inverse Element $x$ zu $\gamma^a$ ist in der Mudolaren Arithmetik so definiert, dass $x \cdot \gamma^a \mod p \equiv 1$. Für den Prozess des Entschlüsselns sollte also $\gamma^{p-1-a}$ verwendet werden, da dies immer eine positive Ganzzahl ist.

## 3.4 Beweis der Richtigkeit des Verfahrens

$$m \equiv \frac{\delta}{\gamma^a} \equiv \frac{m \cdot (g^a)^k}{(g^k)^a} \equiv m \cdot \frac{g^{ak}}{g^{ak}} \pmod p \tag{6}$$

## 3.5 Beispiel

Erzeugung eines Keys: $p$ und $a$ werden zufällig erzeugt, $g$ ist eine zu $p$ passende Primitivwurzel.

$$\begin{aligned} p &= 2357 \\ g &= 2 \\ a &= 1751 \\ g^a &\equiv 2^{1751} \equiv 1185 \pmod{2357} \end{aligned}$$

Der Öffentliche Schlüssel ist nun $P = (p \leftarrow 2357, g \leftarrow 2, g^a \leftarrow 1185)$, der geheime Schlüssel ist $a$. Die Verschlüsselung einer Nachricht $m = 2035$ läuft wie folgt ab ($k$ wird zufällig gewählt):

$$\begin{aligned} k &= 1520 \\ \gamma &\equiv 2^{1520} \equiv 1430 \pmod{2357} \\ \delta &\equiv 2035 \cdot 1185^{1520} \equiv 697 \pmod{2357} \\ c &= (\gamma \leftarrow 1430, \delta \leftarrow 697) \end{aligned}$$

Der Schlüsseltext wird nun an den Empfänger versandt. Dieser berechnet wiederum $m$, um die Nachricht zu lesen:

$$m \equiv 1430^{2357-1-1751} \cdot 697 \equiv 872 \cdot 697 \equiv 2035 \pmod{2357}$$

## 3.6 Vor- und Nachteile

- **Geschwindigkeit:** Für die Verschlüsselung von beliebig vielen Klartexten $m_1, \ldots, m_n$ sind lediglich $1+n$ Modulare Exponentiationen nötig ($g^a \mod p$ und $(g^a)^{k_n} \mod p$), außerdem $n$ Multiplikationen ($m_n \cdot (g^a)^{k_n}$). Die beiden Modularen Exponentiationen können allerdings schon im Vorraus berechnet werden, da sie von $m_n$ nicht beeinflusst werden.

- **Sicherheit:** ElGamal hat den Vorteil, dass die Zahl $k$ für jede Verschlüsselungsprozedur zufällig generiert wird. Wird also ein Klartext $m$ einmal mit $k_1$ und einmal mit $k_2$, $k_1 \neq k_2$ verschlüsselt, entstehen bei beiden Verschlüsselungen verschiedene Schlüsseltexte. Dadurch sind statistische Angriffe und das Identifizieren gleicher Klartext-Nachrichten anhand des verschlüsselten Textes nicht möglich, da sie verschieden sind. Allerdings hat diese Zufallskomponente den Nachteil, dass der Schlüsseltext sich im Vergleich zum Klartext verlängert, und maximal $\leq 2 \cdot (p-1)$ wird, da aus einer Zahl $m$ zwei Zahlen $\gamma$ und $\delta$ werden.

  Wird bei der Verschlüsselung von zwei Werten $m_1$ und $m_2$ das gleiche $k$ verwendet, so lässt sich bei Kenntnis von $m_1$ auf $m_2$ schließen, denn es gilt:

$$\frac{\delta_1}{\delta_2} \equiv \frac{m_1 \cdot g^{ak}}{m_2 \cdot g^{ak}} \equiv \frac{m_1}{m_2} \pmod{p} \tag{7}$$

  Wird die Nachricht $c = (\gamma, \delta)$ abgefangen, bevor sie den Empfänger erreicht, kann die Nachricht manipuliert werden, zum Beispiel indem $\delta$ verdoppelt wird, was einer Verdoppelung von $m$ entspricht: $c = (\gamma, 2 \cdot \delta) = (\gamma, 2m \cdot (g^k)^a)$.

## 3.7 Eine Aufgabe zum selbst berechnen

Es seien $p = 4271$ und die Primitivwurzel $g = 7$ mit $a = 505$.
Verschlüssele mit dem daraus erstellten öffentlichen Schlüssel die Nachricht $m = 2342$.

# 4 Quellen

[1] A. Menezes, P. van Oorschot und S. Vanstone: *Handbook of Applied Cryptography*, Kapitel 8.4

[2] Wikipedia-Artikel zu den Themen *ElGamal*, *Inverses Element*, *Modulare Exponentiation*, *Primitive Root* und *Multiplicative Group of Integers Modulo n*

[3] http://www.xml-dev.com/xml/images/DiffieHellman.png