FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2024/25
08.01.2025

12. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Alice erzeugt sich einen ElGamal-Schlüssel zu $p = 37$ und $g = 5$. Als geheimen Schlüssel wählt sie $\alpha = 23$.

a) Wie lautet ihr öffentlicher Schlüssel?

b) Bob will die Nachricht $m = 15$ an Alice senden. Zum Verschlüsseln verwendet er $\beta = 7$. Wie lautet der Geheimtext?

c) Führen Sie die Entschlüsselung des Geheimtextes aus b) durch.

Übung 2

Zeigen Sie: Ist α der private ElGamal-Schlüssel zu p und g, so kann man einen Geheimtext (B, c) auch entschlüsseln durch

$$m = B^x \cdot c \bmod p \quad \text{mit} \quad x = p - 1 - \alpha.$$

Übung 3

Alice möchte mit ihrem Schlüssel aus Übung 1 die Nachricht $m = 20$ signieren und wählt dazu $k = 13$.

a) Wie lautet die Signatur?

b) Verifizieren Sie die Signatur.

Übung 4

Zeigen Sie: Nutzt man die ElGamal-Signatur zweimal mit gleichem k und unterschiedlichen Nachrichten m_1 und m_2, so lässt sich ggf. aus den Signaturen und den Nachrichten das geheime α berechnen.

Übung 5

a) Sei (p, g, A) ein öffentlicher ElGamal-Schlüssel.

Zeigen Sie: Wählt man u, v mit $\gcd(v, p-1) = 1$ und setzt man

$$r = g^u A^v \bmod p, \qquad s = -rv^{-1} \bmod (p-1), \qquad m = s \cdot u \bmod (p-1),$$

so ist (r, s) eine gültige Signatur zu m (*existenzielle Fälschung*).

b) Geben Sie ein Beispiel einer solchen „Fälschung“ zu $(p, g, A) = (37, 5, 20)$ an.