Disclaimer

Die Übungen die hier gezeigt werden stammen aus der Vorlesung *Kryptographie*! Für die Korrektheit der Lösungen wird keine Gewähr gegeben.

1. Possibilistisch sichere Kryptosysteme

   Bestimmen Sie alle possibilistisch sicheren Kryptosysteme $S = (X, K, Y, e, d)$ mit $X = \{a, b\}$ und $K = \{1, 2\}$ (bis auf das Umbenennen von Chiffretexten).

   Solution:

2. Possibilistische Sicherheit: Eine alternative Definition? Beweisen oder widerlegen Sie: Ein Kryptosystem $S = (X, K, Y, e, d)$ ist possibilistisch sicher genau dann, wenn Folgendes gilt: $\forall x \in X \forall y \in Y \exists k \in K : d(y, k) = x$.

   Solution:

   Bemerkung: Im Gegensatz zur Definition der possibilistischen Sicherheit wird hier eine Aussage über die Entschlüsselungsfunktion gemacht.

3. Possibilistische Sicherheit bei komponentenweiser Verschlüsselung

   Gegeben seien ein Kryptosystem $S = (X, K, Y, e, d)$ und $l \in \mathbb{N}^+$. Wir können S benutzen, um längere Klartexte (Elemente aus X^l) zu verschlüsseln.

   Das Kryptosystem $S' = (X^l, K, Y^l, e', d')$ mit $e'((x_1, ..., x^l), k) = (e(x_1, k), ..., e(x_l, k))$ verschlüsselt komponentenweise unter Verwendung eines einzigen Schlüssels k.

   (a) Definieren Sie d' so, dass S' tatsächlich ein Kryptosystem ist.

   Solution:

   (b) Zeigen Sie, dass S' für $|X|, l \geq 2$ nicht possibilistisch sicher ist. (Dies gilt auch dann, wenn S selber possibilistisch sicher ist!)

   Solution:

   Das Kryptosystem $S^* = (X^l, K^l, Y^l, e^*, d^*)$ mit $e^*((x_1, ..., x_l), (k_1, ..., k_l)) = (e(x_1, k_1), ..., e(x_l, k_l))$ verschlüsselt komponentenweise unter Verwendung mehrerer Schlüssel $k_1, ..., k_l$.

   (a) Definieren Sie d^* so, dass S^* tatsächlich ein Kryptosystem ist.

   Solution:

   (b) Zeigen Sie, dass S^* genau dann possibilistisch sicher ist, wenn S possibilistisch sicher ist.

Solution:

Notation: Für eine natürliche Zahl $n \geq 2$ sei Z_n die Menge der Zahlen $\{0, 1, ..., n-1\}$. Die Addition $+_n$ und Multiplikation $*_n$ auf Z_n sind wie folgt definiert: $a +_n b = (a + b)\ mod\ n$ und $a *_n b = (a * b)\ mod\ n$, wobei $x\ mod\ n$ der Rest von x bei Division durch n ist.

4. Verschiebe- und affines Kryptosystem

Für $n \in N^+$ betrachten wir zwei Kryptosysteme, um Elemente aus Z_n zu verschlüsseln. Das Verschiebekryptosystem (Cäsar-Chiffre) mit Parameter n ist gegeben durch $C_n = (Z_n, Z_n, Z_n, e_n, d_n)$ mit $e_n(x, k) = x +_n k$.

(a) Wie muss d_n definiert werden, damit C_n tatsächlich ein Kryptosystem ist?

Solution:

(b) Zeigen Sie, dass C_n possibilistisch sicher ist.

Solution:

Das affine Kryptosystem mit Parameter $n \geq 2$ ist gegeben durch $A_n = (Z_n, A_n \times Z_n, Z_n, e'_n, d'_n)$ mit $A_n = \{a \in Z_n | ggT(a, n) = 1\}$ und $e'_n(x, (a, b) = a *_n x +_n b$. Hinweis: Falls $ggT(a, n) = 1$, d.h., a und n teilerfremd sind, dann gilt: Es existert genau ein $b \in A_n \subseteq Z_n \backslash \{0\}$, so dass $a *_n b = b *_n a = 1$. Dieses Element b heißt „multiplikatives Inverses von a modulo n".

(a) Definieren Sie d'_n so, dass A_n tatsächlich ein Kryptosystem ist.

Solution:

(b) Zeigen Sie, dass A_n possibilistisch sicher ist.

Solution: