G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 7

Aufgabe 1 *Kollision I*
Sei X eine Menge mit n Elementen. Es werde k mal aus X mit zurücklegen gezogen.

1. Wie groß ist die Wahrscheinlichkeit, das mindestens zweimal das selbe Element gezogen wird?

2. Wie groß muss k gewählt werden, damit die Wahrscheinlichkeit größer als $1/2$ ist?

Hinweis: Nutzen Sie für Aufgaben Teil 2 die Abschätzung $1 + x \leq e^x$, die für alle reellen Zahlen x erfüllt ist.

Aufgabe 2 *Geburtstags Paradoxon*

1. Wie groß ist die Wahrscheinlichkeit, dass hier im Raum zwei Personen am gleichen Tag Geburtstag haben?

2. Wie groß ist die Wahrscheinlichkeit, dass hier im Raum jemand am gleichen Tag Geburtstag hat wie man selbst?

Aufgabe 3 *Zufällige Abbildungen*
Sei $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ eine zufällige Abbildung. Wie groß ist die Wahrscheinlichkeit, das es mindestens zwei Elemente $x, y \in \mathbb{F}_2^k$ gibt, so dass $f(x) = f(y)$ gilt.

Hausaufgabe 1 *Diskreter Logarithmus und Kollisions-Attacken*
Sei G eine Gruppe der Ordnung n in der das DL-Problem schwer ist.

1. Finde einen Algorithmus für das Berechnen von diskreten Logarithmen in G mit ungefährer Laufzeit $O(\sqrt{n})$. Benutze hierfür die Ergebnisse von Aufgabe 1.

2. Warum nennt man solche Angriffe generisch?

Hausaufgabe 2 *Square Attacke*
Implentieren Sie die Attacke auf den COMP-128.