RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 10 / 15. Dezember 2010

AUFGABE 1:
Gegeben seien 30 zufällig gewählte Personen. Wir nehmen an die Geburtstage seien über das gesamte Jahr (ohne 29.02.) gleichverteilt.

a) Wie hoch ist die Wahrscheinlichkeit, dass mehrere der 30 Personen heute Geburtstag haben?

b) Wie hoch ist die Wahrscheinlichkeit, dass mindestens 2 der 30 Personen am gleichen Tag Geburtstag haben?

c) Wie hoch ist die Wahrscheinlichkeit aus b) gerade bei Ihnen im Raum?

d) Wie hoch ist die Wahrscheinlichkeit, dass mindestens 3 der 30 Personen am gleichen Tag Geburtstag haben?

AUFGABE 2:
Gegeben sei eine 128-Bit Hashfunktion. Benutzen sie das Geburtstagsparadoxon, um Kollisionen dieser Hashfunktion zu finden. Wieviele Hashwerte müssen Sie bilden, um mit einer Wahrscheinlichkeit von 50% eine Kollision zu finden?

Hinweis: Benutzen Sie die Approximation $e^{-\frac{n(n-1)}{2m}}$ für die Wahrscheinlichkeit, dass in einer Stichprobe der Größe n eines von m möglichen Ereignissen mindestens 2x auftritt.