Rechnersicherheit - Übung 03

Dennis Hägler und Martin Görick

6. Mai 2015

1 Aufgabe 1

2 Aufgabe 2

a) Es ist IND-CPA sicher, da bei jedem Verschlüsseln eine neue Zufallszahl generiert wird, weshalb zwei Verschlüsselungen des selben Textes verschiedene Geheimtexte erzeugen. Damit liegt die Wahrscheinlich bei zwei verschiedenen Texten, wenn einer zufällig gewählt wird nur bei $\frac{1}{2}$ den richtigen Text zu erkennen.

b) Wenn die selbe Zufallszahl mehrfach genommen wird, dann wird aus dem selben Klartext jedes mal beim Verschlüsseln der selbe Geheimtext erzeugt, damit wäre das Verfahren unsicher, da ähnliche Texte gleich verschlüsselt werden.

3 Aufgabe 3

4 Aufgabe 4

Da alle Geburtstage von einander abhängig sind, steht immer nur 1 von 365 zur Wahl. Diese werden durch die Abhängigkeit multipliziert.

$$P(n) = \frac{1}{365}^{n}$$

$$P(20) = 5,68 * 10^{-52}\%$$