Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 4

Aufgabe 1. (Perfekte Sicherheit)
Aus der Vorlesung wissen Sie, dass für ein perfekt sicheres Kryptosystem mit $P(Y = y) > 0$ für alle $y \in \mathcal{C}$ gilt:

$$|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{M}|.$$

Zeigen Sie, dass die Umkehrung i.A. nicht gilt. Konstruieren Sie also ein Kryptosystem mit $P(Y = y) > 0$ für alle $y \in \mathcal{C}$ und $|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{M}|$, welches nicht perfekt sicher ist.

Aufgabe 2. (One-Time-Pad für Bitfolgen der Länge n)
Wir wollen das folgende perfekt sichere Kryptosystem betrachten, welches auch als **One-Time-Pad** bekannt ist. Klartexte, Geheimtexte und Schlüssel (zufällig gewählt) seien Bitfolgen der Länge n, d.h.:

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n.$$

Zur Ver- und Entschlüsselung wird jedes Klartextbit mit dem entsprechenden Schlüsselbit per **XOR** (von **exclusive or**) verknüpft. Die Verknüpfung ist definiert als:

$\oplus$	0	1
0	0	1
1	1	0

Es ist also $E_K(m) = m \oplus K$ bzw. $D_K(c) = c \oplus K$.

- Sie betrachten dieses Kryptosystem für Bitfolgen der Länge 16. Sie wollen die Nachricht $m = 0100\ 0010\ 0100\ 1001$ verschlüsseln und dafür den Schlüssel $K = 0100\ 0101\ 0101\ 0010$ verwenden. Berechnen Sie $E_K(m)$.
- Machen Sie sich klar, warum allgemein tatsächlich $D_K(E_K(m)) = m$ gilt.
- Sie stellen fest, dass bei Verschlüsselung mit der Bitfolge, die nur aus Nullen besteht, Klartext und Geheimtext übereinstimmen. Daher verbieten Sie diese Bitfolge als Schlüssel. Ist Ihr Kryptosystem noch perfekt sicher? Sie fangen als Chiffretext die Bitfolge, die nur aus Nullen besteht, ab. Wie hängen in diesem Fall Schlüssel und Klartext zusammen?
- Jemand hat den Begriff One-Time-Pad nicht verstanden und verwendet für zwei Nachrichten m_1, m_2 den gleichen Schlüssel. Sie fangen die Nachrichten c_1 und c_2 ab. Können Sie Rückschlüsse auf die Klartexte ziehen, wenn Sie wissen, dass der gleiche Schlüssel verwendet wurde? Was können Sie tun, wenn Sie ein Stück Klartext (aber nicht seine Position) für eine der beiden Nachrichten kennen?
- Zur Veranschaulichung finden Sie auf der Rückseite zwei mit dem selben Schlüssel verschlüsselte Binärbilder und die XOR-Verknüpfung der verschlüsselten Varianten.

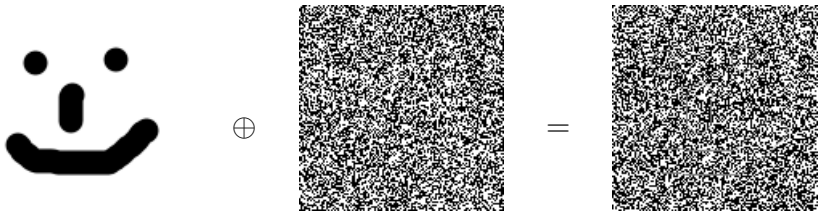

Abbildung 1: Smiley $\oplus$ Schlüssel K

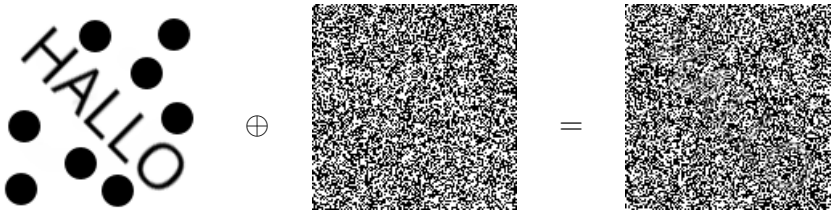

Abbildung 2: Hallo $\oplus$ Schlüssel K

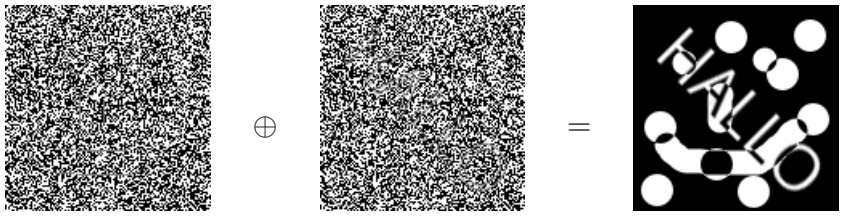

Abbildung 3: Verschlüsselter Smiley $\oplus$ Verschlüsseltes Hallo