Theoretische Grundlagen der Informatik II
Blatt 11

Markus Vieth Marvin Becker

28. Januar 2016

Aufgabe 1

Nach dem Theorem aus der Vorlesung (Foliensatz 8, Folie 13), gilt:

$((Gen, Enc, Dec)$ ist perfekt sicher $\Rightarrow |K| \geq |M|) \Leftrightarrow (|K| < |M| \Rightarrow (Gen, Enc, Dec)$ ist nicht perfekt sicher$)$

Laut Vorlesung gilt für das normale One-Time-Pad $K = M \Rightarrow |K| = |M|$.
Nach der Aufgabenstellung gilt $|K| = |M| > |K| - 1 = |K'|$, wobei K' die geänderte Schlüsselmenge aus der Aufgabenstellung meint (ohne 0^ℓ).
$\Rightarrow$ Das in der Aufgabenstellung beschriebene Verfahren kann nicht perfekt sicher sein.

Aufgabe 2

a)

E_1 kann nicht sicher sein, da wir für 2^n Nachrichten nur 1 Schlüssel verwenden. Da Nachrichten mindestens die Länge 1 besitzen gilt $2^n > 1$. Somit ist das Verfahren laut dem Theorem aus der Vorlesung nicht sicher.

b)

Da die 0 keinerlei Aussage über die Verschlüsselung oder die Nachricht selbst liefert, bleibt das Verfahren durch die Verwendung von Π sicher.

c)

Da wir davon ausgehen, dass der Angreifer Enc aus Π kennt, braucht dieser lediglich den Key von der Nachricht zu trennen, um letztere entschlüsseln zu können.

d)

In dem man das Bit m_n seiner Testnachtrichten einmal 0 und einmal 1 wählt, kann der Angreifer diese später mit einer Wahrscheinlichkeit von 100% unterscheiden, da dieser nur das erste Bit des Geheimtextes mit dem letzten Bit seiner Nachricht vergleichen muss.

e)

Dieses Verfahren muss sicher sein. Wäre es nicht sicher, so wäre Π nicht sicher, da man das Verfahren zur Unterscheidung bei E_5 bei Π anwenden könnte, in dem man die durch Π verschlüsselte Nachricht einfach nochmal an dessen Ende kopiert und dann jenes Verfahren anwendet. Da aber Π sicher ist, muss auch E_5 sicher sein.

Markus Vieth, Marvin Becker

Aufgabe 3

Beweis gilt unter der Annahme, das Eve weiß, dass in der Nachricht „To: Bob“ steht.
Es gelte die ASCII Kodierung mit 8-Bit Erweiterung (sollte dies nicht gewünscht sein, so ist lediglich die 0 in Klammern am Anfang eines jeden Byteblocks zu entfernen).
Es sei m die unverschlüsselte Originalnachricht und n die von Eve gewünschte Nachricht. Weiter sei u die Zahl der Bits, welche vor der Passage „To: Bob“ in der Nachricht stehen und v die Zahl der Bits nach der Passage. Des Weiteren soll gelten:

$$m^* := 0^u||(0)1010100\ (0)1101111\ (0)0111010\ (0)0100000\ (0)1000010\ (0)1101111\ (0)1100010||0^v$$

$$n^* := 0^u||(0)1010100\ (0)1101111\ (0)0111010\ (0)0100000\ (0)1000101\ (0)1110110\ (0)1100101||0^v$$

Somit entspricht m^* der Passage „To: Bob“ an der entsprechenden Stelle, ohne den Rest der Nachricht und n^* das selbe für „To: Eve“
Wählt Eve nun als „p“:

$$p := m^* \oplus n^* = 0^u||(0)0000000\ (0)0000000\ (0)0000000\ (0)0000000\ (0)0000111\ (0)0011001\ (0)0000111||0^v$$

So gilt:

$$m \oplus p = n$$

Das heißt für den Angriff:

$$((m \oplus k) \oplus p) \oplus k =^{1} m \oplus k \oplus p \oplus k = k \oplus k \oplus m \oplus p = 0 \oplus n = n$$

$\Rightarrow$ Mit p lässt sich die Nachricht auf die gewünschte Art manipulieren, trotz perfekt sicherer Verschlüsselung.

q.e.d.

[1] Aus der technischen Informatik ist bekannt, dass XOR assoziativ und kommutativ ist.