

Übungen zur Kryptographie (Wintersemester 2009/2010) 4. Hausübung (20.11.2009)

Aufgabe 4.1 (20 Punkte)

Beschreiben Sie einen Angriff mit bekannten Klartexten auf ein SPKS, bei dem die Wortsubstitution weggelassen wird (formal: die Wortsubstitution ist die Identität auf $\{0,1\}^n$, wobei n die Wortlänge ist). Wieviele Klartext-Chiffretext-Paare benötigen Sie höchstens, um den verwendeten Schlüssel eindeutig und vollständig zu bestimmen?

Aufgabe 4.2 (30 Punkte)

Wir betrachten wieder das SPKS aus der Vorlesung (1.2.1. aus dem 4. Teil des Skriptes). Bestimmen Sie die betragsmäßige Ausrichtung für die folgende Gleichung:

$$x(0) \oplus x(1) \oplus x(3) = z(6).$$

Dabei können Sie die Voraussetzungen für Lemma 1.3.6 aus Kapitel 4 des Skriptes als gegeben annehmen.

Aufgabe 4.3 (25 Punkte)

Beschreiben Sie nach dem Muster des Beispiels aus der Vorlesung gute Unterscheider für Verschiebe- und affine sowie Vigenèrechiffren und bestimmen Sie ihren Vorteil.

Aufgabe 4.4 (25 Punkte)

Konstruieren Sie einen generischen Unterscheider auf ein Block-Kryptosystem unter der Annahme, dass ein Algorithmus gegeben ist, der mit Wahrscheinlichkeit $\geq \frac{3}{4}$ zu einer Menge aus 10 Paaren von Klar- und Chiffretexten den verwendeten Schlüssel bestimmen kann. Wie ist der Vorteil Ihres Unterscheiders?