Universität Tübingen, WS 13/14

Bernd Borchert

Übungen Kryptologie

Blatt 2.

Aufgabe 1. Die sogenannte *Vignere Chiffre* ist ein Verfahren, das ähnlich zum One-Time Pad Verfahren ist, das aber in einer Nachricht das Geheimnis – immer wieder hintereinander geschrieben - mehrfach verwendet. Meistens ist dabei das Geheimnis nicht zufällig entstanden, sondern ein leicht zu merkender String.

Beispiel (Wikipedia)

Plaintext:	ATTACKATDAWN
Secret:	LEMON
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

Schaffen Sie es, folgende Vignere Chiffre zu entschlüsseln? Der Sender versendet einen deutschen Text und benutzt ein Geheimnis mit 4 Buchstaben. Wie gehen Sie vor? (bruteforce mit 26 hoch 4 Möglichkeiten gilt nicht)

XSEGPRMESRGAFWRNOXRLPOBMLOGIPRIECONUQIA

Aufgabe 2. Sie wollen eine konkrete Triple-DES Inplementierung brechen und haben praktisch beliebige Rechenpower. Sie können jedoch die Implementierung nur per challenge/response kontaktieren, d.h. Sie können einen Klartext in Blockgröße dort hinschicken und bekommen den Ciphertext zurück. Wie oft müssen Sie die Implementierung voraussichtlich mindestens kontaktieren, um den Schlüssel herauszufinden? Wie gehen Sie vor? Können es weniger Kontaktierungen sein, wenn Sie Glück haben? Können es mehr sein, wenn Sie Pech haben?

Welche Anforderung an ein gutes Block-Verschlüsselungs-Verfahren leiten Sie daraus ab?

Aufgabe 3. Warum ist es beim OFB Betriebsmodus dringend empfehlenswert, den Initialisierungsvektor bei jeder neuen Nachricht zu wechseln? Warum stellt das einen praktischen Nachteil des OFB Modus dar? Warum ist ein fester Initialisierungsvektor bei CFB kein so großes Problem?

Aufgabe 4. Zeigen Sie: {10010, 00110, 01010, 11110} ist ein 2-dimensionaler affiner Unterraum von $\mathbf{2}^5$ (ein affiner Unterraum ist eine Menge der Form a + U, wobei U ein Untervektorraum ist).