– Praktikumsaufgabe 4 –

Thema: *Brute-Force-Angriff auf eine verschlüsselte Datei*

Zielstellung: Kennenlernen des *Tiny Encryption Algorithm*, Implementierung eines Brute-Force-Angriffes, Fälschen einer Nachricht

1. Gegeben ist ein Chiffrat `sehrgeheim.txt`, von dem Sie wissen, dass es mit dem *Tiny Encryption Algorithm* (TEA) verschlüsselt wurde und dass es ein Bild enthält. Durch einen glücklichen Zufall sind Sie außerdem in den Besitz des Passwortes gekommen, leider fehlt Ihnen das letzte Byte. Der bekannte Teil des Passworts lautet: `xdfg19rtbg38:+h`. TEA wurde (der Einfachheit halber) im ECB-Mode eingesetzt.

   Versuchen Sie, per Brute-Force-Angriff das Chiffrat zu entschlüsseln. TEA ist u. a. hier beschrieben: *http://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm*.

   Welches prinzipielle Problem haben Sie, wenn Sie das Format des Klartextes nicht kennen?

   Hinweise: Der Teufel liegt ein wenig im Detail; Sie müssen das Padding beachten, d. h. den letzten Block der Klartextdatei auf die Blockgröße auffüllen. Wir implementieren *according to the book*:

   > „Um den letzten Block zu vervollständigen, wird er mit einem regelmäßigen Muster aufgefüllt [...]. Wenn die Füllwerte nach der Entschlüsselung wieder entfernt werden sollen, fügt man die Anzahl der Füllbytes einfach als letztes Byte des letzten Blockes an. [...] Damit diese Methode funktioniert, muss jede Nachricht aufgefüllt werden. Selbst wenn der Klartext an einer Blockgrenze endet, muss man einen kompletten Block anfügen.“ (Bruce Schneier. *Angewandte Kryptographie*. Pearson, 2006, S. 225)

2. Durch die Ermittlung des Schlüssels sind Sie nun in der Lage, verschlüsselte Nachrichten zu fälschen. Schlüpfen Sie in die Rolle von Mallory, fälschen Sie geeignet die Nachricht `sehrgeheim2.txt` und schicken Sie mir diese per Mail.