Übungsaufgaben zur Vorlesung Kryptologie

Helmut-Schmidt-Universität — Universität der Bundeswehr Hamburg
Professur für Allgemeine Nachrichtentechnik — Prof. Dr.-Ing. Udo Zölzer
Dr.-Ing. Martin Holters, Raum: H3 - R115, Tel.: 040 / 6541 - 3468

M.Sc. Patrick Nowak, Raum: H3 - R116, Tel.: 040 / 6541 - 3650

Matlab-Übungsaufgaben zu Kap. 10: Stromchiffren

Aufgabe 1 — RC4

Schreiben Sie eine Funktion `rc4(K, N)`, die auf Basis des ggf. wiederholten Schlüssels K die S-Box des RC4-Algorithmus initialisiert und danach N Bytes der Ausgabe erzeugt.

Aufgabe 2 — Angriff gegen WEP

Schreiben Sie eine Funktion `wepattack(IV, K)`, der ein Initialisierungsvektor IV der Länge N und das (vermutete) erste Byte K des Schlüsselstroms übergeben werden. Die Funktion soll die ersten N Runden der RC4-Initialisierung durchführen und dann prüfen, ob $S[1]+S[S[1]]=N$. Ist dies der Fall, soll $K-(j+S[N])$ zurückgegeben werden (mit dem j aus der letzten durchgeführten Initialisierungsrunde); andernfalls -1.

Prüfen Sie Ihre Funktionen mit:

```
for idx=1:2000
   IV = [3, 255, randi(255)];
   res(idx)=wepattack(IV, rc4([IV, 'schluessel'], 1));
end
```

Im Ergebnisvektor `res` sollte der ASCII-Wert des `s`, 115, gehäuft auftreten.