Christian Schindelhauer

Freiburg, den 22. Juli 2009
Besprechung am 30. Juli 2009

Übungen zur Vorlesung

Algorithmen für drahtlose Netzwerke

Sommer 2009

Blatt 12

AUFGABE 1: *(Aufzeichnungsblock 12-A)*

1. Zwei Studenten haben in einem Universitätsnetzwerk mittels einer Wörterbuchattacke eine Reihe von Passwörtern von Mitarbeitern und Professoren ermitteln können. Klassifizieren Sie diese Bedrohung. Welche Sicherheitsziele werden verletzt?
2. Konstruieren Sie mittels (mehrerer Runden) der Feistel-Chiffre Ihre (noch nie da gewesene) Verschlüsselungsmethode. Kodieren und Dekodieren Sie testweise eine Nachricht.

AUFGABE 2: *(Aufzeichnungsblock 12-B)*

1. Führen Sie den RSA-Algorithmus für die Primzahlen $p = 23$, $q = 17$ und $e = 5$ aus. Die Nachricht sei $m = 2$.
2. Diskutieren Sie den Fall, dass alle Byzantinische Generäle immer die Nachrichten mithören können (aber nicht unbedingt den Sender identifizieren können). Kann das Problem der byzantinische Generäle dann auch ohne Kryptographie gelöst werden?
3. Welcher Nachrichtenaufwand ist notwendig, wenn 10 Byzantinische Generäle versuchen (mit Hilfe von Kryptographie) die Betrüger zu entlarven.

AUFGABE 3: *(Aufzeichnungsblock 12-C)*

1. Angenommen in einer Challenge-Response-Authentifizierung wird immer die selbe Zufallszahl verwendet. Welche Nachteile ergeben sich dadurch?
2. Recherchieren Sie die Funktionsweise von RC-4.