2. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 23.04.2015
Abgabe 30.04.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1 (Cipher Block Chaining (CBC), Wasserzeichen-Angriff)

In der Vorlesung haben wir Blockchiffren und deren Betriebsmodi kennengelernt. Ein Betriebsmodus ist CBC. Für diesen Betriebsmodus existiert der sogenannte Wasserzeichen-Angriff. Machen Sie sich mit diesem Angriff vertraut, indem Sie die gestellten Fragen beantworten.

(a) In welchem Umfeld wird der Wasserzeichenangriff benutzt?

(b) Welche im CBC-Modus verwendeten Elemente müssen vorhersagbar sein, um einen erfolgreichen Angriff durchzuführen?

(c) Warum kann man diese Elemente vorhersagen?

(d) Wie kann man den Angriff verhindern?

Aufgabe 2. (Substitutions-Permutationsnetzwerk, SPN)

Stellen Sie jeweils einen Angriff auf das in der Vorlesung kennen gelernten SPN dar, wenn

(a) Permutationen

(b) Substitutionen

weggelassen werden.

Aufgabe 3. (Advanced Encryption Scheme, AES)

Vergleichen Sie die in der Vorlesung kennen gelernte schematische Darstellung eines SPN mit der Blockchiffre AES. Welche Unterschiede gibt es und warum.

Aufgabe 4. (Betriebsmodi)

(a) Stellen Sie die Entschlüsselung einer Nachricht, die mittels AES im CBC-Mode verschlüsselt wurde, graphisch dar.

(b) Nehmen Sie an, dass ein Geheimtextblock fehlerhaft bertragen wurde. Wie viele Klartextblöcke werden hiervon beeinflusst. Begründen Sie Ihre Antwort.

Aufgabe 5. (RSA)

Zeigen Sie, dass $(\mathbb{Z}_n^*, \cdot)$ eine abelsche Gruppe ist.