Netzsicherheit I, WS 2011
Übung 6

Prof. Dr. Jörg Schwenk

Betreuer: Florian Feldmann, Florian Giesen

Abgabe: Montag, 28. November 2011, 11:00h

In der Übung, am Kasten vor ID 2/467, oder per Mail an Florian.Giesen AT rub.de
Gruppenarbeit bis max. 3 Studenten pro Gruppe ist erlaubt und erwünscht.

1 ECB vs. CBC

Betrachten Sie die verschiedenen Modi, in denen Blockchiffren operieren können, speziell den *Electronic Codebook Modus (ECB)* und den *Cipher Block Chaining Modus (CBC)*.

Warum bevorzugt Bruce Schneier die Verwendung von CBC gegenüber ECB? Begründen Sie! Welche Nachteile muss er dafür in Kauf nehmen?

2 MAC vs. Signatur

Message Authentication Codes (MAC) und *Digitale Signaturen*, wie z.B. das ElGamal-Signaturschema, dienen (unter anderem) beide dem Schutz der Integrität einer Nachricht. Worin unterscheiden sich MAC und Signaturen, insbesondere in Bezug auf die verwendeten Schlüssel, und welche Implikationen für den Einsatz entsprechender Verfahren ergeben sich daraus?

3 Zertifikate

- Was ist die Grundaufgabe eines *Zertifikats* im Zusammenhang mit PKI?
- Welche Bedeutung kommt einem *Root-Zertifikat* in einer PKI zu?