Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security

SoSe 24
LV 4120, 7240

Übungsblatt 8

Aufgabe 8.1 (Message-Authentication-Codes):

a) Erläutern Sie den Unterschied zwischen einer Authentifizierung mit einem Message-Authentication-Code und einer Signatur.

b) Erläutern Sie den Unterschied zwischen einem Prüfsummenverfahren zur Überprüfung der Integrität und einem Authentizitätsverfahren zum Prüfen der Authentizität anhand einer Hash-Konstruktion.

c) Konstruieren Sie einen HMAC. Nutzen als Basis für den HMAC einen AES-128 Verschlüsselungsalgorithmus und eine Miyaguchi-Prenell Konstruktion. Schreiben Sie hierfür einen Pseudocode. Gehen Sie davon aus, dass es eine Basisoperationen $AES-128E_K(P)$ gibt, um den einen Plaintext P mit dem Schlüssel K zu verschlüsseln. Gehen Sie weiterhin davon aus, dass die Nachricht m, für welche die MAC generiert werden soll, nur 128-Bit lang ist.

d) Herr Seky möchte zur Absicherung der Kommunikation zwischen App und B2DS einen AES-128 im Galios Countermode nutzen. Der gemeinsame geheime Schlüssel zur Verschlüsselung und Authentifizierung der Kommunikation soll mit dem zuvor besprochenen Transportschlüssel aus dem DHKE Protokoll genutzt werden. Erfüllt Herr Seky damit seine Sicherheitsziele, die Kommunikation authentisch und vertrauenswürdig zu gestalten? (Gehen Sie davon aus, dass Herr Seky das DHKE-Protokoll korrekt umgesetzt hat und einen guten Zufallszahlengenrator für die ephemeral Schlüssel nutzt).

e) Warum ist es besser, eine Software für einen sicheren Softwareupdateprozess mit einer Signatur zu signieren und verifizieren zu lassen, als mit einer MAC?

Aufgabe 8.2 (Digitales Signaturverfahren DSA):

a) Schreiben Sie die drei Operationen (Schlüsselgenerierung, Signieren und Verifizieren) für das DSA-Verfahren als Pseudo-Code auf.

Algorithm 1 Schlüsselgenerierung (K_{pb}, K_{pr})

Require: Parameter (p, q, g)
Ensure: K_{pb}, K_{pr}

Algorithm 2 Generiere Signatur (r, s)

Require: Privater Schlüssel K_{pr}, Nachricht m
Ensure: Signatur (r, s)

Algorithm 3 Verifkation der Signatur (r, s)

Require: Öffentlicher Schlüssel K_{pb}, Nachricht m, Signatur (r, s)
Ensure: Signatur valide oder nicht

b) Kann man generell sagen, dass die Signaturgenerierung der Entschlüsselung gleicht und die Signaturverifikation der Verschlüsselung?

c) Zeigen Sie, dass es beim DSA Signaturverfahren wichtig ist, immer einen zufälligen Maskenwert (Ephemeral Schlüssel) k pro Siganturgenerierung zu nutzen.
Tipp: Zeigen Sie dass Sie den privaten Schlüssel mit Hilfe einer Differenzenbetrachtung/ Differenzengeleichnung von zwei Signaturen $s_1 - s_2$ rekonstruieren können. Versuchen den Ausdruck für die Differenzengeleichnung unter der Annahme $k = k_1 = k_2$ zu vereinfachen.

Aufgabe 8.3 (ECDSA - PS3 Hack):

a) Schreiben Sie einen Pseudocode für die Operationsvorschrift zum Signieren für eine gegebene Kurve $E := (p, a, b, q, A)$. Nutzen Sie dafür folgendes Format:

Algorithm 4 Generiere Signatur (r, s)

Require: Kurve $E := (p, a, b, q, A)$, Privater Schlüssel d, Nachricht m
Ensure: Signatur (r, s)

---

b) Zeigen Sie, dass der private Schlüssel d rekonstruiert werden kann, wenn Sie zwei Signaturen $((r_1, s_1), (r_2, s_2))$ mit demselben emphermeral Schlüssel k_E berechnen.