Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

12. Aufgabenblatt

Im folgenden Aufgabenblatt setzen wir uns mit der Realisierung, der Anwendung und der Analyse des RSA-Verfahrens auseinander. Mit dem RSA-Algorithmus steht das mit Abstand populärste Public-Key-Verfahren zur Verfügung. Der Algorithmus besteht im Wesentlichen aus zwei Teilen. Neben dem eigentlichen Chiffrieralgorithmus ist die Schlüsselerzeugung von großer Wichtigkeit für die Sicherheit des Verfahrens. Diese basiert auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen. Des Weiteren bewerkstelligen wir mit dem Diffie-Hellman-Verfahren den Schlüsselaustausch innerhalb einer ungesicherten Infrastruktur. Schließlich widmen wir uns noch dem Miller-Rabin-Primzahlentest.

Aufgabe 12.1

Als Public-Key-Verfahren stützt sich der RSA-Algorithmus auf einen öffentlichen Schlüssel (P_K, n) und einen privaten Schlüssel (S_K, n), wobei mit n der Modulus (öffentlich) bezeichnet wird. Dieser sei durch das Produkt zweier Primzahlen $n = p \cdot q$ mit p = 23 und q = 59 vorgegeben. Für die Erzeugung des öffentlichen Schlüssels stehen die folgenden ganzen Zahlen zur Auswahl:

(P_K, n) = (11, 1357) ; (14, 1357) ; (15, 1357) ; (18, 1357) oder (33, 1357)

a) Welcher der fünf Schlüsselwerte kommt als öffentlicher RSA-Schlüssel in Betracht?

b) Begründen Sie Ihre Auswahl!

c) Berechnen Sie den zugehörigen privaten RSA-Schlüssel.

Aufgabe 12.2

Für ein benutztes RSA-Verfahren möge der öffentliche Schlüssel Kp = 3 und n = 33 betragen. Versuchen Sie aus dieser Kenntnis heraus

a) den zugehörigen privaten Schlüssel Ks zu ermitteln und

b) den verschlüsselten Nachrichtenblock C mit dem Wert 180630 bei einer internen Blocklänge von 2 Ziffern zu entschlüsseln.

Aufgabe 12.3

Um einen Diffie-Hellman-Schlüsselaustausch durchzuführen einigen sich die beiden Kommunikationspartner A und B auf g = 3 und p = 17. A wählt als privaten Schlüssel x = 7; B legt für seinen privaten Schlüssel y = 4 fest.

a) Ermitteln Sie die öffentlichen Schlüssel von A und B, die jeweils mit der Gegenseite ausgetauscht werden.

b) Welche Berechnung hat A und B bei der Ermittlung des gewünschten gemeinsamen Schlüssels durchzuführen?

c) Wovon hängt die Sicherheit des DH-Verfahrens ab?

d) Welcher bekannte Angriff besteht beim DH-Schlüsselaustauschprotokoll?

Aufgabe 12.4

a) Erläutern Sie kurz die Grundfunktionen des AES.

b) Welche Bedeutung haben die S-Boxen beim DES?

Aufgabe 12.5

a) Schildern Sie eine Runde des Feistel-Verfahrens in pseudo-algorithmischer Notation. Verwenden Sie hierzu ggf. Zuweisungen, logische Operationen, linkszirkuläres Shiften und arithmetische Funktionen. Als Eingaben haben Sie L0, R0 sowie K0. Ausgaben sind L1 und R1.

b) Auf welchem Konstruktionsprinzip beruht die Sicherheit des Feistel-Verfahrens?

Aufgabe 12.6

Ein Message Authentication Code (MAC) dient dazu, Gewissheit über die Originalität oder den Ursprung von Daten oder Nachrichten zu erhalten und die Unversehrtheit der zu schützenden Daten überprüfen zu können. MAC-Algorithmen erfordern dabei zwei Eingabeparameter: neben dem Hashwert der Daten auch noch einen geheimen Schlüssel. Aus beidem wird dann eine Checksumme – der sogenannte Message Authentication Code – ermittelt.

a) Entwickeln und implementieren Sie ein C-Funktion, mit deren Hilfe Sie für einen gegebenen 32 Bit langen Hashwert h(m) einer Nachricht m und einen ebenso langen (geheimen) Schlüssel k durch die Vorschrift

$$MAC(h(m), k) = h(m) \oplus k$$

den Message Authentication Code MAC(h(m), k) herstellen können.

b) Ermitteln Sie für h(m) = AD778EF0 und den Schlüssel k = 12 34 56 78 den entsprechen MAC-Wert.

c) Welche Eigenschaft besitzt ein auf diese Weise erzeugter MAC? Begründen Sie Ihre Antwort.

d) Ist der auf diese Weise ermittelte MAC-Wert fälschungsresistent? Begründen Sie Ihre Antwort.

Aufgabe 12.7

a) Testen Sie anhand des Miller-Rabin-Verfahrens die beiden Zahlen n = 187 sowie n = 191, ob es sich hierbei jeweils um eine Primzahl handelt. Führen Sie den Test an dem Zeugen a = 2 durch.

b) Wie groß ist die jeweilige Trefferwahrscheinlichkeit?

c) Wie viele Zeugen müsste man theoretisch testen, damit die Fehlerwahrscheinlichkeit kleiner 10^{-7} ist?