Hochschule Darmstadt
Department of Computer Science
Bachelor of Computer Science
Christian Rathgeb, Ulrich Scherhag, Jannis Priesnitz

SS 2020
27. Mai 2020

IT-Sicherheit, Praktikum 3

Hinweis: Geben Sie bitte alle von Ihnen in Rahmen des Praktikums erstellten Dateien in einer .zip-Datei mit ab.

Aufgabe 1 (RSA)

In dieser Aufgabe sollen Sie sich mit der Sicherheit des RSA-Verfahrens, sowie mit der RSA-Funktionalität von `openssl` auseinander setzen.

(a) Worauf beruht die Sicherheit des RSA-Verfahrens? Gegeben sei der öffentlicher Schlüssel $(n, e) = (437, 7)$. Brechen Sie das Verfahren, indem Sie den dazugehörigen privaten Schlüssel d berechnen. Erläutern Sie Ihre Vorgehensweise.

(b) Verschlüsseln Sie mit Hilfe von (a) die Nachricht 123.

(c) Entschlüsseln Sie mit Hilfe von (a) das Ergebnis von (b).

(d) Erzeugen Sie mit Hilfe von `openssl` ein RSA-Schlüsselpaar mit Moduluslänge 4096 Bit und speichern Sie den Schlüssel im PEM-Format in der Datei „`rsaprivkey.pem`“ ab. Das Schlüsselpaar soll bei der Erstellung mit einer 256 Bit AES Verschlüsselung geschützt werden.

(e) Extrahieren Sie den öffentlichen RSA-Schlüssel aus „`rsaprivkey.pem`“ und speichern Sie den Schlüssel im PEM-Format in der Datei „`rsapubkey.pem`“ ab.

(f) Erzeugen Sie sich eine Textdatei „`plain.txt`“ mit Ihrem Namen und Studienfach und verschlüsseln Sie diese mittels RSA zur Datei „`cipher.bin`“. Entschlüsseln Sie anschließend die Datei und vergleichen Sie den Klartext mit der ursprünglichen Textdatei.

(g) Erzeugen Sie sich ein weiteres RSA-Schlüsselpaar, mit dem Sie Ihre Textdatei signieren und verifizieren.

Warum ist es sinnvoll, für Verschlüsselung und Signatur zwei unterschiedliche RSA-Schlüsselpaare zu verwenden?

Aufgabe 2 (Zertifikate in openssl)

In dieser Aufgabe sollen Sie das X.509-Zertifikat der Seite `https://www.h-da.de` untersuchen.

(a) Lassen Sie sich das Zertifikat der Seite „`https://www.h-da.de`“ mittels eines geeigneten `openssl`-Befehls anzeigen und speichern Sie dann das Zertifikat im PEM-Format in der Datei „`hda_cert.pem`“ ab.

Hinweis: Im Moment gibt die h-da Website nach dem Zertifikat ein `HTTP/1.1 400 Bad Request` zurück, welchen Sie ignorieren können.

(b) Geben Sie die Zertifikatskette an. Was ist die Root Certification Authority (Root-CA)?

(c) Wandeln Sie das Zertifikat der Datei „`hda_cert.pem`“ in das DER-Format um und speichern Sie es in der Datei „`hda_cert.der`“.

(d) Geben Sie jeweils für die Datei „`hda_cert.pem`“ sowie „`hda_cert.der`“ die SHA1- und MD5-Hashwerte an. Sind diese im Zertifikat gespeichert? Sind die jeweiligen Werte für die beiden Kodierungen PEM und DER gleich?

(e) Geben Sie das Zertifikat, das Sie in der Datei `hda_cert.pem` gespeichert haben, im lesbaren Textformat auf dem Bildschirm aus. Welcher Algorithmus zur Signaturerstellung wurde verwendet? Wie lang ist der Modulus n des im Zertifikat enthaltenen öffentlichen Schlüssels? Wie lautet der Exponent e des öffentlichen Schlüssels?