

Aufgabe 17: (8 Punkte)

- (a) Wir betrachten das DSA-Signaturverfahren. Angenommen die Angreiferin Eve erhält zwei verschiedene Nachrichten M, M' und die jeweils zugehörigen Unterschriften (r, s) bzw. (r', s') , die allesamt von Alice erzeugt worden sind. Alice habe bei beiden Unterschriften dieselbe Zufallszahl z verwendet.

Zeigen Sie, dass Eve dann *entweder* den geheimen Schlüssel x von Alice berechnen (und damit fortan die Unterschrift von Alice fälschen) kann *oder* dass eine Kollision in der verwendeten Hashfunktion SHA-1 gefunden werden kann.

- (b) Die DSA-Signatur (r, s) einer Nachricht M lasse sich durch einen Programmaufruf der Form $(r, s) = \text{DSA}(M, p, q, g, x, z)$ berechnen.

Zeigen oder widerlegen Sie: Mit Hilfe dieses Programms lässt sich der RSA-Algorithmus simulieren, d.h. eine Zahl $m < n$ lässt sich mit RSA-Schlüsseln $(e, n), (d, n)$ korrekt ver- bzw. entschlüsseln.

Programmieraufgabe P5: (14 Punkte)

Informieren Sie sich über das Java-Sicherheitspaket `java.security`.

- (a) Implementieren Sie ein Programm, das eine Inputdatei byteweise einliest und mit Hilfe der Hashalgorithmen SHA bzw. MD5 aus der Klasse `MessageDigest` den zugehörigen Hashwert berechnet und byteweise hexadezimal ausgibt.
- (b) Implementieren Sie Programme zur Generierung und Verifizierung von digitalen Signaturen mit Hilfe des Signaturalgorithmus SHA/DSA aus der Klasse `Signature`.

Zunächst ist ein Programm zu implementieren, das zufällige Schlüsselpaare für den DSA-Algorithmus erzeugt und in Dateien abspeichert. Der private Schlüssel soll mit Hilfe der Klasse `PKCS8EncodedKeySpec`, der öffentliche Verifizierungsschlüssel mit Hilfe der Klasse `X509EncodedKeySpec` gespeichert werden.

Das Generierungsprogramm soll eine Nachricht und einen privaten Schlüssel aus Dateien einlesen und die zugehörige digitale Signatur berechnen. Danach soll die Signatur als `ByteArray` in einer Datei abgespeichert werden.

Das Verifizierungsprogramm soll eine Nachricht, einen Verifizierungsschlüssel und eine digitale Signatur aus Dateien einlesen und überprüfen, ob die Signatur korrekt ist.