

Programmieraufgabe P6: (12 Punkte)

Der Weihnachtsmann bittet um Mithilfe. Da er im letzten Jahr zahlreiche gefälschte Wunschzettel erhalten hat, nimmt er dieses Jahr nur signierte Wunschzettel entgegen. Dazu möchte er mit dem Java-Hilfsprogramm `keytool` eine Schlüsseldatenbank aufbauen, in der Schlüsselpaare für DSA-Signaturschlüssel gespeichert werden.

- (a) Lesen Sie die Java-Dokumentation zu `keytool`. Generieren Sie zwei verschiedene Schlüsselpaare (`keytool -genkey`) für zwei verschiedene Personen und speichern Sie die Schlüssel in der Datenbank. Exportieren Sie die zugehörigen Zertifikate der Schlüssel (`keytool -export`) in Dateien.
- (b) Schreiben Sie eine kurze Dokumentation für den Weihnachtsmann, in der die wichtigsten Funktionen und Parameter von `keytool` verständlich erklärt sind. Erläutern Sie an einem Beispiel, welche Schritte der Weihnachtsmann bei seinem Vorhaben konkret durchführen muss.
- (c) Modifizieren Sie Ihre Signaturprogramme aus Programmieraufgabe P5(b) so, dass sie nicht mehr Schlüssel aus Dateien sondern diese mit Hilfe der Klasse `KeyStore` aus der Schlüsseldatenbank einlesen. Erstellen Sie zwei signierte Wunschzettel und verifizieren Sie deren Signatur.

Aufgabe 18: (6 Punkte)

Verschaffen Sie sich einen Überblick über die bisher in dieser Vorlesung behandelten Themen und erstellen Sie eine mögliche *Klausuraufgabe* zu einem von Ihnen gewählten Bereich aus den Kapiteln 1–5 des Skripts.

Formulieren Sie die von Ihnen gewählte Aufgabe möglichst verständlich und geben Sie anschließend einen Lösungsvorschlag dazu an.

Aufgabe 19: (3 Punkte)

Entschlüsseln Sie folgende Chiffretexte:

- (a) `iurkh zhlkqdfkwhq`
- (b) `oixex geton budsmh`
- (c) `0988 | 1137 | 0581 | 0565 | 0955 | 0992 | 0992 | 0062 | 1324 |
0565 | 0877 | 0988 | 0493 | 0062 | 0565 | 0102 | 0988 | 0062 |
0998 | 0565 | 0700 | 1153 | 1153 | 0289 | 0670 (n = 1339, e = 277)`