technische universität dortmund

Prof. Dr. Jan Jürjens, Thomas Ruhroth
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
SFL – Abgabe: 19.11.2014

Sicherheit: Fragen und Lösungsansätze – Übung 3

AUFGABE 1 (RSA) (4LP):

Berechnen Sie zunächst für $p = 13$, $q = 17$ und $e = 5$ die Zahl d gemäß des RSA-Algorithmus und wenden Sie dann dieses Verfahren auf den Klartext $m = 5$ an. (Hinweis: Das Ergebnis ist 31, der Rechenweg ist wichtig.)

AUFGABE 2 (RSA-Java) (3 BP + 3LP):

Für viele moderne Programmiersprachen gibt es fertige Krypto-Pakete. Für Java findet man ein solches z.B. mitgeliefert im Package javax.crypto.

1. Welche Klassen werden für die Nutzung einer RSA-Verschlüsselung benötigt? Welche Klassen für eine DES-Verschlüsselung? Geben Sie bitte für jede Klasse kurz an welche Aufgabe die Klasse hat.
2. Algorithmen für die Verschlüsselung können nach dem Schema "algorithm/mode/-padding" ausgewählt werden, geben Sie die Bedeutung und Zweck für die einzelnen Bestandteile des Schemas an.
3. Schreiben Sie ein kleines Java-Programm (Ausgabe auf der Kommandozeile), welches
   - ein RSA-Schlüsselpaar erzeugt,
   - die Keys ausgibt,
   - den String "Sicherheit: Fragen und Lösungsansätze" verschlüsselt (RSA) ausgibt,
   - und diesen wieder entschlüsselt ausgibt.

   Bitte geben Sie sowohl den Code als auch die Ausgabe einer Ausführung des Programms als Ausdruck ab.