Prof. Dr. Rüdiger Weis

Betriebssysteme

Übungsblatt 8: Sicherheit

Aufgabe 1 Schlüsselmanagement (9 Punkte)

Eine Gruppe von 10 Teilnehmern soll verschlüsselt kommunizieren.

- Wie viele Schlüssel müssen ausgetauscht werden, falls Public Key Verfahren verwendet werden?
- Wieviele wären es, wenn keine Public Key Verfahren verwendet werden? Nennen Sie zwei mögliche Szenarien.

Bitte begründen Sie kurz Ihre Antworten.

Aufgabe 2 (9 Punkte) Diffie-Hellmann Keyexchange

Berechnen Sie die beiden Public Keys und den mittels DHKE vereinbarten gemeinsamen Schlüssel bei den gemeinsamen Parametern $p = 467$ und $g = 2$ für

- $a = 2, b = 5$
- $a = 400, b = 134$
- $a = 228, b = 57$

Aufgabe 3 (8 Punkte) RSA

- Verschlüsseln Sie die Nachricht $x = 9$ mit den RSA Parametern

$$p = 5, q = 11, e = 3$$

- Berechnen Sie den zugehörigen privaten Schlüssel und entschlüsseln Sie zur Überprüng die verschlüsselte Nachricht.

Aufgabe 4 (24 P) Schlüsselaustausch Protokoll

Programmieren Sie ein `naiveDH.py` Python-Programm, welches einen generischen Diffie-Hellman Schlüsselaustausch über mittels base64 codierter Nachricht realisiert. Weiterhin sollen nach dem Schlüsselaustausch mittesls XTEA im CFB Mode verschlüsselte Nachrichten versendet und diese vom Empfänger entschlüsselt werden.