Prof. Dr. Rüdiger Weis

Sicherheit in Verteilten Systemen

Übungsblatt 3 Public Key Cryptography

Aufgabe 1 (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 2 (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 3 (8 Punkte) RSA Exponent

Gegeben seinen die Primzahlen $p = 41$ und $q = 17$.

- Welche der Zahlen $e_1 = 32$ und $e_2 = 39$ ist als öffentlicher RSA Exponent geeignet?
- Berechnen Sie den privaten Exponenten mit Hilfe des Erweiterten Euklidischen Algorithmus.

Aufgabe 4 (24 P) Schlüsselaustausch Protokoll

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