Asymmetrische Kryptographie

Das RSA Kryptosystem nach Rivest, Shamir und Adleman

Funktionsweise des RSA Kryptosystems

1. Wähle zwei sehr grosse Primzahlen **p** und **q** und berechne m = p * q.
2. Bestimme einen zufälligen Wert **e**, der kleiner ist als m und der keine gemeinsamen Teiler mit (p-1) * (q-1) hat.
3. Bestimme das modular Inverse **d** von e. D.h. Finde heraus, welche Zahl **d** die Gleichung

   (e * d) mod ((p-1) * (q-1)) = 1

   erfüllt.
4. Der öffentliche Schlüssel ist das Zahlenpaar **(e, m)**.
5. Der geheime (private) Schlüssel ist das Zahlenpaar **(d, m)**.
6. Zum Verschlüsseln einer Zahl **t** (die kleiner als m sein muss), verwende die Formel $c = t^e \bmod m$.
7. Zum Entschlüsseln einer Zahl **c** verwende die Formel $t = c^d \bmod m$.

Übungen

1. Erstelle ein privates und ein öffentliches Schlüsselpaar mit 2 sehr kleinen Primzahlen p und q (im Bereich 1-20).
2. Gib deinen öffentlichen Schlüssel einem Kollegen.
3. Verschlüssle eine kurze Zahlenfolge, z.B. 4, 15, 12, 9 mit dem öffentlichen Schlüssel eines Kollegen und gib ihm die verschlüsselte Zahlenfolge.
4. Entschlüssle eine verschlüsselte Zahlenfolge mit deinem privaten Schlüssel.
5. Wie könntest du Texte verschlüsseln?
6. Warum sind Nachrichten, welche mit aus sehr kleinen Primzahlen erstellten Schlüsseln verschlüsselt wurden, nicht sicher?
7. Du kannst Zahlen auch mit deinem privaten Schlüssel verschlüsseln. Sie können dann mit dem öffentlichen Schlüssel wieder entschlüsselt werden. Wie könnte man diesen „umgekehrten“ Vorgang sinnvoll nutzen?