20191028

Montag, 28. Oktober 2019 11:52

BBS I Mainz Informationsverarbeitung
Lernabschnitt: Datenschutz und Datensicherheit
Verschlüsselung

bbs.eins.mainz
Berufsbildende Schule Technik

1. Recherchieren Sie das Verschlüsselungsverfahren von Rivest, Shamir und Adleman (**RSA**).
   Legen Sie bei der Recherche besonderen Wert auf folgende Aspekte:
   + Schlüsselpaare
   + Erzeugung des Schlüsselpaares (öffentlich und privat)
   + Verschlüsseln von Nachrichten
   + Entschlüsseln von Nachrichten
   + weitere Anwendungsbereiche
2. Visualisieren Sie das Verfahren mit einem Partner anhand eines von ihnen gewählten Beispiels.
   Beschränken Sie sich bei dem Beispiel zunächst auf eine Zahl. Im Anschluss können Sie auch ein Wort oder einen ganzen Text verschlüsseln.

+ Schlüsselpaare:
  Chiffrierschlüssel (verschlüsseln) ≙ öffentliche Schlüssel
  Dechiffrierschlüssel (entschlüsseln) ≙ private Schlüssel

+ Wie werden die Schlüsselpaare generiert?
  1. zwei Primzahlen $p \neq q$
  2. $N = p \cdot q$
  3. $\varphi(N) = \varphi(p \cdot q) = (p-1) \cdot (q-1) = m$
  4. Suche $1 < e < m$ für die gilt $ggT(e, m) = 1$
     (im optimalfall ist e Prim)
  5. (e, N) = öffentlicher Schlüssel
     Für den privaten Schlüssel d suchen wir das multiplikative Inverse zu e mod m
  6. (d, N) = privater Schlüssel

Wie bestimmt man das multiplikative Inverse:

1. $p = 5 \quad q = 13 \quad \Rightarrow N = 65$
2. $\varphi(N) = 4 \cdot 12 = 48$
3. $e = 5 \quad ggT(5, 48) = 1$

$48 = 9 \cdot 5 + 3 \rightarrow 3 = \boxed{48 - 9 \cdot 5}$
$5 = 1 \cdot 3 + 2 \rightarrow 2 = \boxed{5 - 1 \cdot 3}$
$3 = 1 \cdot 2 + 1 \rightarrow 1 = 3 - 1 \cdot 2$
$2 = 2 \cdot 1$

Setze nun Sukzessive die umgestellte Gleichung in die vorherige Gleichung ein.

$1 = 3 - 1 \cdot (5 - 1 \cdot 3)$

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3)$$
$$= 3 - 1 \cdot 5 + 1 \cdot 3$$
$$= 2 \cdot 3 - 1 \cdot 5$$

$$1 = 2 \cdot (48 - 9 \cdot 5) - 1 \cdot 5$$
$$= 2 \cdot 48 - 18 \cdot 5 - 1 \cdot 5$$
$$= 2 \cdot 48 - 19 \cdot 5 \mod 48$$

$$\Rightarrow 1 \equiv -19 \cdot 5 \mod 48$$

Unsere Bedingung für d ist $1 < d < m$

Daher müssen wir noch

$48 - 19 = \boxed{29}$

rechnen und erhalten für $d = 29$ und damit das multiplikative Inverse von $e = 5$

Probe: $5 \cdot 29 = 145$
$= 3 \cdot 48 + 1$
$\equiv 1 \mod 48$

$\Rightarrow$ öffentlicher Schlüssel $(5, 65)$
private Schlüssel $(29, 65)$

---

zu übermittelnde Nachricht: $a = 15$

Geheimtext $c = 15^5 \mod 65$
$c \equiv 45$
$\Downarrow$ wird übermittelt

Klartext $a = c^{29} = 45^{29} \mod 65$
$a \equiv 15 \mod 65$