11. Verschlüsselungsverfahren

Nachfolgend wird das RSA-Verfahren erklärt:

RSA - Verschlüsselung

symetrisch:

z.B. Passwort ziffern alphabetisch um eine bestimmte Anzahl schieben
→ gut, einfach knackbar mit z.B. der Brute-Force Methode

asymetrisch:

Hat 1 Schlüssel zum chiffrieren und 1 Schlüssel zum entschlüsseln
→ öffentliches Verfahren wie z.B. das RSA-Verfahren, welches 1976 von R. Rivest, A. Shamir und M. Hellmann entwickelt wurde.

RSA-Kurzerklärung:

- Einwegfunktion: $n = p \cdot q$ n wird schwer 'knackbar' nach p und q

$\varphi(n) = (p-1)(q-1)$ ist die Eulerische Funktion

=> aus Satz von Euler: $m^{k \cdot (\varphi(n)+1)}$ ergibt sich m', wobei man dabei 'e' $\in IN$ mit $ggT(e; \varphi(n)) = 1$ wählt und sich dann der private Schlüssel mit 'd' und 'n', als auch der öffentliche Schlüssel mit 'e' und 'n' ergibt. Die Werte von 'p' und 'q' sind dabei geheim.

Daraus ergibt sich: $\cdot c = m^e$ bei Verschlüsselung
$\cdot c^d = m$ bei Entschlüsselung

- Beispiel: Geg: $p = 17$, $q = 3$, $m = 11$

$n = p \cdot q = 17 \cdot 3 = 51$

$\varphi(51) = (p-1)(q-1) = (17-1)(3-1) = 32$

Gegenseitig festgelegter e-Wert: $e = 5$

Verschlüsselter Wert 'd' ergibt sich nun aus:

Vielfaches von $\varphi(n)+1$ => 33, 65, 97, 129, 161, ...

Vielfaches von e => 5, 10, ..., 60, 65

65 ist in beiden Reihen gemeinsam:

=> $e' = 65$ und $d = \frac{e'}{e} = \frac{65}{5} = 13$

Gesendet wird nun d mit Wert 13. und der Wert von n, der hier 51 beträgt. Dies ist nun der öffentliche Schlüssel! Die Werte d = 13 und n = 51 bilden den privaten Schlüssel!

Wenn nun der Charakter m = 11 (Es soll dabei m < n sein!) gesendet werden soll, ergibt sich nach dem RSA-Verfahren folgendes:

c ist verschlüsselter m, das sich ergibt aus:

$c = m^e \bmod n = 11^5 \bmod 51 = 44$

Der Wert c = 44 wird nun gesendet und dann beim Empfänger entschlüsselt mit:

m' ist entschlüsselter m aus: $m' = c^d \bmod n = 44^{13} \bmod$

m' ist entschlüsselter m aus: $m' = c^d \bmod n = 44^{13} \bmod 51 = 11$

entschlüsselter Wert m' stimmt mit dem Wert 'm' überein!!