3.3 Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselungsverfahren (*Public-Key-Verschlüsselung*) arbeiten mit *Schlüsselpaaren*. Ein Schlüssel ist der öffentliche Schlüssel (*Public-Key*), der andere ist der private Schlüssel (*Private-Key*). Dieses Schlüsselpaar hängt über einen mathematischen Algorithmus eng zusammen. Daten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel entschlüsselt werden. Deshalb muss der private Schlüssel vom Besitzer des Schlüsselpaares geheim gehalten werden.

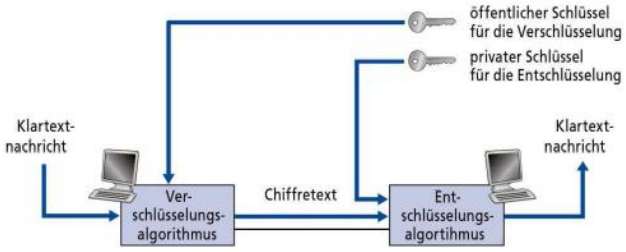

Abbildung 1: Asymmetrische Verschlüsselung

Das bekannteste asymmetrische Verschlüsselungsverfahren ist sicherlich *RSA* (benannt nach *R*ivest-*S*hamir-*A*dleman)[1]. Diese Methode nützt die Tatsache, dass es sehr schwierig ist große Zahlen in ihre Primfaktoren zu zerlegen. So besteht bei diesem Verfahren der öffentliche Schlüssel im Wesentlichen aus dem Produkt zweier großer Primzahlen. Um nun vom *Public-Key* auf den *Private-Key* schließen zu können, müsste eine solche Zerlegung gefunden werden.

RSA

Um den *Public-Key* und den *Private-Key* zu wählen, sind folgende Schritte durchzuführen:

1. Wähle zwei Primzahlen p und q.
2. Berechne $n = p * q$ und $z = (p - 1) * (q - 1)$.
3. Wähle eine Zahl *e*, kleiner als *n*, die keine gemeinsamen Primfaktoren mit *z* hat (ausser *1*). (In diesem Fall bezeichnet man *e* und *z* als relative Primzahlen zueinander). Der Wert wird mit *e* bezeichnet, weil dieser Wert bei der *Verschlüsselung* (*encryption*) verwendet wird.
4. Suche eine Zahl d, sodass $e * d - 1$ ohne Rest durch z teilbar ist. Der Buchstabe d wird benutzt, weil dieser Wert bei der *Entschlüsselung* (***D**ecryption*) verwendet wird. Anders ausgedrückt gesucht wird bei einem gegebenen e ein d, sodass

[1] Siehe: RSA-Kryptosystem – Wikipedia

$$e * d \; mod \; z = 1$$

5. Der öffentliche Schlüssel ist das Zahlenpaar *(n, e)* und sein privater Schlüssel ist das Zahlenpaar *(n, d)*.

Als einfaches Beispiel sei $p = 5$ und $q = 7$. Dann sind $n = 35$ und $z = 24$. Wähle $e = 5$, da *5* und *24* keine gemeinsamen Faktoren haben. $d = 29$, denn $5 * 29 - 1$ (also $e * d - 1$) ist genau durch *24* teilbar. Folglich werden das Zahlenpaar $(n = 35, e = 5)$ als *Public-Key* und $(n = 35, d = 29)$ als *Private-Key* eingereiht. Die Tabelle 1 zeigt die Verschlüsselung eines Klartextes und Tabelle 2 die Entschlüsselung des Chiffretextes auf:

m: Klartext	m^e	c = m^e modulo n: Chiffretext
12	248832	17
9	159049	4
5	3125	10
2	32	32

Tabelle 1: RSA-Verschlüsselung mit und $e = 5$

Chiffre-text	c^d	m = c^d modulo n: Klartext
17	48196857210675091509150914118252230716 97	12
4	288230376151711744	9
10	100000000000000000000000000000	5
32	44601490397061246283071436545296723011960832	2

Tabelle 2: RSA-Entschlüsselung mit $n = 35$ und $d = 29$

