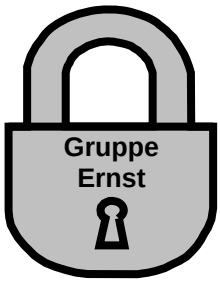
V-AB 4.1 Arbeitsblatt zu Modul V4: Erstellen eines öffentlichen Schlüssels

Gruppe Ernst



Aufgabenstellung:
Ihr wollt vertrauliche Nachrichten von unterschiedlichen Sendern empfangen.
Damit ihr nicht mit jedem einzelnen Sender ein senderspezifisches Paar von Ver- und Entschlüsselungsfunktionen vereinbaren müsst, entwickelt ihr einen *öffentlichen* Schlüssel, mit dem alle senden können und einen *privaten* Schlüssel, mit dem ihr die gesendete Information entschlüsseln könnt.
Der öffentliche Schlüssel muss allen zugänglich sein, die euch verschlüsselte Nachrichten schicken möchten. Allerdings reicht die Kenntnis dieses Schlüssels nicht aus, damit verschlüsselte Nachrichten zu entschlüsseln. Das könnt nur ihr mit eurem geheim zu haltenden privaten Schlüssel.

Vorgehen:

a. Wählt zwei Primzahlen p und q (normalerweise wären es riesige Zahlen, der Einfachheit halber verwenden wir kleine Zahlen). p = 17, q = 11 Diese Zahlen werden geheim gehalten. Aus ihnen berechnet ihr in der Folge den öffentlichen Schlüssel.	p = 17 q =11
b. Die beiden Primzahlen werden miteinander multipliziert, und somit wird eine weitere Zahl N erhalten.	N = p*q = ____
c. Es wird eine weitere Zahl *d* gewählt (Achtung d und (p-1)*(q-1) müssen teilerfremd sein, d.h. sie dürfen keinen gemeinsamen Teiler haben!). Die Zahl *d* werdet ihr später als euren privaten Schlüssel zur Entschlüsselung (*decryption*) verwenden.	*d* = 7
d. Aus den beiden Werten p und q könnt ihr jetzt den für die Verschlüsselung (*encryption*) zu verwendenden öffentlichen Schlüssel berechnen. Die Formel dafür lautet: e * d = 1 (mod (p-1) * (q-1)) Die beiden Zahlen N und *e* ergeben den öffentlichen Schlüssel.	*e* = ___
Lösung: e * d = 1 (mod (p-1) * (q-1)) e * 7 = 1 (mod 16*10) e * 7 = 1 (mod 160) e = 23 (euklidischer Algorithmus) *euklidischer Algorithmus:* p=17, q=11, d=7, N=187 e*d = 1(mod (p-1)*(q-1) 160 = 7*22 + 6 //7 und 6 (der Rest) werden verschoben	

7 = 6*1 + 1 //6 und 1 (der Rest) werden verschoben 6 = 1*6 + 0 *bitte umblättern*	
Umformen: 6 = 160 -7*22 1 = 7 – 6*1 Ausdruck für 6 einsetzen und Klammern auflösen: 1 = 7 – 1* (160 – 7*22) 1 = 7 – 160 + 7*22 1 = 23*7 – 160, somit: e = 23	
e. Jetzt könnt ihr die Zahlen *e* und N als euren öffentlichen Schlüssel veröffentlichen, etwa in einem für alle zugänglichen Verzeichnis abstellen oder auf die Tafel schreiben.	N: 187 *e:* 23
f. Wartet nun bis ihr von einer anderen Gruppe eine verschlüsselte Nachricht erhält.	
g. Die erhaltene verschlüsselte Nachricht C muss nun entschlüsselt werden. Da ihr den privaten Schlüssel d habt, ist das nur euch möglich. Um nun die Mitteilung zu entschlüsseln benutzt ihr folgende Formel: $M = C^d \pmod{187}$	
Lösung für privaten Schlüssel 7 und empfangene Botschaft 11 $M = C^d \pmod{187}$ $M = 11^7 \pmod{187}$ $M = [\ 11^1 \pmod{187} * 11^2 \pmod{187} * 11^4 \pmod{187}\ ] \pmod{187}$ $M = [\ 11 * 121 * 55\ ] \pmod{187}$ M = 88, laut der beigeschlossenen ASCII-Tabelle ergibt dies den Buchstaben X Lösung für privaten Schlüssel 7 und empfangene Botschaft 142 $M = C^d \pmod{187}$ $M = 142^7 \pmod{187}$ $M = [\ 142^1 \pmod{187} * 142^2 \pmod{187} * 142^4 \pmod{187}\ ] \pmod{187}$ $M = [\ 142^3 \pmod{187} * 142^4 \pmod{187}\ ] \pmod{187}$ $M = [\ 131 * 89\ ] \pmod{187}$ M = 65, laut der beigeschlossenen ASCII-Tabelle ergibt dies den Buchstaben A	

ASCII-Tabelle für Großbuchstaben:

	Binär	Dezimal		Binär	Dezimal
A	1000001	65	N	1001110	78
B	1000010	66	O	1001111	79
C	1000011	67	P	1010000	80
D	1000100	68	Q	1010001	81
E	1000101	69	R	1010010	82
F	1000110	70	S	1010011	83
G	1000111	71	T	1010100	84
H	1001000	72	U	1010101	85
I	1001001	73	V	1010110	86
J	1001010	74	W	1010111	87
K	1001011	75	X	1011000	88
L	1001100	76	Y	1011001	89
M	1001101	77	Z	1011010	90