



V-AB 4.2b Arbeitsblatt zu Modul V4:

Verwenden eines öffentlichen Schlüssels

Gruppe Siegfried

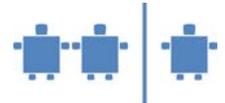


Aufgabenstellung:

Ihr möchtet der Gruppe *Ernst* eine Nachricht schicken. Dafür könnt ihr ihren öffentlichen Schlüssel verwenden und die Nachricht damit verschlüsseln.

Vorgehen:

<p>a. Ihr möchtet symbolisch den Buchstaben A an Gruppe A schicken (etwa als erster Buchstaben von ADAM). Damit X verschlüsselt werden kann, muss es vorher als Zahl dargestellt werden. Schlagt in der beigelegten ASCII-Tabelle nach, welcher binäre Wert X entspricht und welcher dezimale Wert sich daraus ergibt, somit erhalten wir unser M (<i>Message</i>).</p>	<p>M = ____</p>
<p>b. Nun benötigen wir den öffentlichen Schlüssel von Gruppe <i>Ernst</i>. Vorerst muss die Gruppe diesen einmal berechnen. Die Empfängergruppe <i>Ernst</i> wird diesen auf der Tafel anschreiben oder in anderer Form publizieren. Sonst fragt die Gruppe <i>Ernst</i> nach deren öffentlichen Schlüssel und berechnet die verschlüsselte Nachricht (C) mit der Formel $C=M^e \pmod N$.</p>	<p>N= ____ e= ____ C= ____</p>
<p>Berechnungshilfe: Wenn man keinen Computer zu Hand hat, kommt man zu diesem Ergebnis indem man die Potenzen aufteilt, da die meisten Taschenrechner so große Zahlen nicht darstellen: $65^{23} \pmod{187} = [65^1 \pmod{187} * 65^2 \pmod{187} * 65^4 \pmod{187} * 65^{16} \pmod{187}] \pmod{187}$ $65^1 = 65 \pmod{187}$ $65^2 = 4.225 \sim 111 \pmod{187}$ $65^4 = 17.859.625 \sim 166 \pmod{187}$ $65^{16} \sim 65^4 * 65^4 * 65^4 * 65^4 \pmod{187} = 1$ $65^{23} \pmod{187} = 65 * 111 * 166 * 1 \pmod{187} = 142$ <p>Daher ist die verschlüsselte Nachricht C = 142</p> </p>	
<p>c. Diese geheime Botschaft C wird also an Gruppe <i>Ernst</i> geschickt. Gruppe <i>Siegfried</i> selbst kann diese Nachricht nicht mehr</p>	



entschlüsseln, da es sich um eine Einwegfunktion handelt.	
d. Gruppe <i>Ernst</i> sollte nun mit ihrem privaten Schlüssel in der Lage sein, den Anfangsbuchstaben unserer Gesamtbotschaft ADAM zu entschlüsseln.	

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