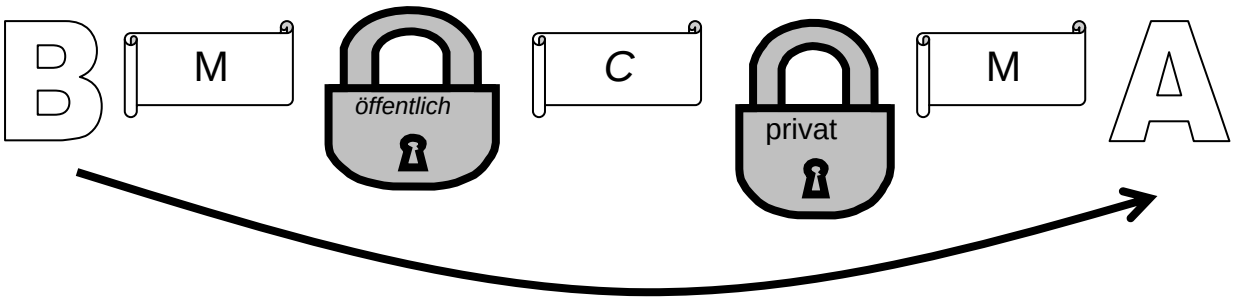
V-AB 4.3 Arbeitsblatt zu Modul V4 für die Beobachtungsgruppe

Gruppe Siegfried

Aufgabenstellung:
Gruppe *Sandra* (und Gruppe *Siegfried*) schicken an Gruppe *Ernst* eine verschlüsselte Nachricht.
Eure Aufgabe ist es sämtliche Kommunikation zwischen den Gruppen abzufangen, damit ihr die Nachricht entschlüsseln könnt.



Vorgehen:

Beobachtet das Geschehen zwischen den gegenseitig Nachrichten austauschenden Gruppen:

a. Wie allen anderen ist euch auch der von *Ernst* publizierte öffentliche Schlüssel bekannt. Ihr habt ihn durch die Kommunikation zwischen *Ernst*, *Sandra* und *Siegfried*) erfahren oder dadurch, dass er sogar von Ernst für alle sichtbar auf die Tafel geschrieben wurde.	N= ___ *e* =___
b. Weiters schicke *Sandra* an *Ernst* eine verschlüsselte Nachricht C_{Sandra}. Vielleicht konntet ihr sogar eine weitere, von *Siegfried* an *Ernst* übermittelte, verschlüsselte Nachricht $C_{Siegfried}$ abhören.	C_{Sandra} =___ $C_{Siegfried}$ =___
c. Da ihr das RSA-Verfahren kennt, wisst ihr auch, dass folgende Formel für die Verschlüsselung verwendet wird: $C = M^e \pmod N$	
d. Ihr könnt also die bekannten Werte in die Funktion einsetzen.	M=???

Welches M würde sich aus den abgehörten Botschaften ergeben? Ist es überhaupt möglich, M zu berechnen?	

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