RSA-Verschlüsselung

https://youtu.be/iHSHOiSCpis

Übung Nr. ..... Note: .....

von ..... Klasse .....

p = ...

q = ...

N = p · q = ...

Eulersche phi-Funktion: $\varphi(N) = (p - 1) \cdot (q - 1)$ = ...

Festlegung des Verschlüsselungexponenten e:

Bestimme eine Zahl e so, dass $1 < e < \varphi(N)$ und e so, dass e und $\varphi(N)$ teilerfremd sind, d.h. $ggT(e,\varphi(N)) = 1$. Bestimme auch das multiplikative Inverse des Verschlüsselungexponenten e innerhalb der Restklasse $\varphi(N)$, d.h. e^{-1} mod $\varphi(N)$, mit dem Rechner für modulare Arithmetik (RMA). (Hinweis: Berechne e^{-1} mod $\varphi(N)$ mit dem RMA. Wenn e^{-1} mod $\varphi(N)$ existiert, dann sind e und $\varphi(N)$ teilerfremd. Dies bedeutet, dass man $ggT(e,\varphi(N))$ nicht berechnen muss).

Wir kennen nun die Schlüssel.

Öffentlicher Schlüssel: (Dient der Verschlüsselung. Mit diesem Schlüssel sollen Botschaften an mich verschlüsselt werden)

$(e,N) = ($..... , ...$)$

Privater Schlüssel: (Mit ihm kann ich alle Botschaften entschlüsseln, die mit dem öffentlichen Schlüssel verschlüsselt wurden)

$(e^{-1},N) = ($..... , ...$)$

Verschlüsselung einer Nachricht mit dem öffentlichen Schlüssel:

Verwendeter öffentlicher Schlüssel:

(e,N) = (.................................... , ...)

Buchstabe Nr.	Buchstabe	ASCII-Code (Msg)	Verschlüsselt (Cipher = $(Msg)^e \bmod N$)
1.	B	066	
2.	Y	089	
3.	T	084	
4.	E	069	

Entschlüsselung einer Nachricht mit dem privaten Schlüssel:

Verwendeter privater Schlüssel:

(e^{-1},N) = (.................................... , ...)

Cipher Nr.	Cipher	Entschlüsselt (ASCII-Code) (Msg = $(Cipher)^{(e^{-1})} \bmod N$)	Buchstabe
1.			
2.			
3.			
4.			

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M
ASCII-Code	65	66	67	68	69	70	71	72	73	74	75	76	77

Buchstabe	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ASCII-Code	78	79	80	81	82	83	84	85	86	87	88	89	90

Schlüsselaustausch

Mein Partner: Name: ..... Klasse: .....

Auftrag:
- Wähle einen Partner
- Partner tauschen ihre öffentlichen Schlüssel aus
- Wähle ein Wort mit vier verschiedenen Buchstaben
- Verschlüssle die vier Buchstaben mit dem Schlüssel des Partners
- Sende die verschlüsselten Buchstaben an den Partner
- Dein Partner sendet dir vier verschlüsselte Buchstaben
- Entschlüssle die vier Buchstaben mit deinem privaten Schlüssel

Verschlüsselung einer Nachricht an meinen Partner:

Der öffentliche Schlüssel meines Partners:

$(e_P, N_P) = ($..... , ...$)$

Buch-stabe Nr.	Buch-stabe	ASCII-Code (Msg)	Verschlüsselt (Cipher = $(Msg)^{e_P} \bmod N_P$)
1.			
2.			
3.			
4.			

Entschlüsselung der Nachricht von meinem Partner:

Mein privater Schlüssel:

$(e^{-1}, N) = ($..... , ...$)$

Cipher Nr.	Cipher	Entschlüsselt (ASCII-Code) (Msg = $(Cipher)^{(e^{-1})} \bmod N$)	Buch-stabe
1.			
2.			
3.			
4.			