Elgamal-Verschlüsselung

Aufgabe 2

Julia wählt $p = 23$ und die Primitivwurzel $[5]$ in $\mathbb{Z}_{23}$. Weiter wählt sie den Entschlüsselungsexponent $e = 14$ und berechnet

$$[A] = [5]^{14} = [25]^7 = [25 - 23]^7 = [2]^7 = [128] = [128 - 115] = [13] \text{ in } \mathbb{Z}_{23}.$$

Julia veröffentlicht auf ihrer Homepage $(p, g, A) = (23, 5, 13)$.

a) Thomas möchte die Nachricht $n = 11$ an Julia senden. Dazu wählt er den Verschlüsselungsexponent $v = 3$ und berechnet in $\mathbb{Z}_{23}$

$[B] = [g]^v = [5]^3 =$ in $\mathbb{Z}_{23}$,

$[A]^v = [13]^3 =$ in $\mathbb{Z}_{23}$,

$[N] = [A]^v \cdot [n] = [12] \cdot [11] =$ in $\mathbb{Z}_{23}$.

Thomas schickt also $(B = \quad , N = \quad)$ an Julia.
Julia berechnet als erstes $[B]^{-14} = [B]^{22-14} = [B]^8 = [B^2]^4 = [B^2 - 92]^4 =$

in $\mathbb{Z}_{23}$.

Hinweis: $[18] = [-5]$ kann hilfreich sein.
Dann erhält sie die Nachricht n durch Multiplikation:

$[n] = [B]^{-14} \cdot [N] =$ in $\mathbb{Z}_{23}$.

b) Marc schickt an Julia $(B, N) = (3, 21)$. Welche Nachricht n hat er an Julia geschickt?

$[B]^{-14} =$ in $\mathbb{Z}_{23}$,

$[n] =$ in $\mathbb{Z}_{23}$.

c) Zusatzaufgabe: Erstelle die Potenztabelle für $[5]^k$ um herauszufinden, welchen Verschlüsselungsexponent Marc gewählt hat.
Kennzeichne Marcs Verschlüsselungsexponent durch Umkringeln.

$k =$	1	2	3	4	5	6	7	8	9	10	11
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

$k =$	12	13	14	15	16	17	18	19	20	21	22
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]