Der Diffie-Hellmann-Merkle Schlüsseltausch

Eine Primzahl p, eine geeignete Basis $b \in \{0, \dots, p-1\}$ sind öffentlich bekannt.
Aus zwei privaten Schlüsseln werden erst zwei öffentliche und dann ein gemeinsamer privater Schlüssel für die Nachricht erstellt, mit dem kann man dann Symmetrische Verschlüsselungsverfahren verwenden, ohne sich vorher persönlich zum Schlüsseltausch zu treffen.

Aufgaben: Welche Zahl hat welche Rolle? Warum funktioniert das Verfahren und ist sicher?

1. Privater Schlüssel:
$a_1 \in \{0, \dots, p-1\}$
2. Berechne:
$C_1 = b^{a_1} \; mod \; p$
3. Erhalte C_2.
4 Berechne
$K = C_2^{a_1} \; mod \; p$
Es gilt
$K = C_2^{a_1} = b^{a_2 * a_1} \; mod \; p$

1. Privater Schlüssel:
$a_2 \in \{0, \dots, p-1\}$
2. Berechne:
$C_2 = b^{a_2} \; mod \; p$
3. Erhalte C_1.
4 Berechne
$K = C_1^{a_2} \; mod \; p$
Es gilt
$K = C_1^{a_2} = b^{a_2 * a_1} \; mod \; p$

MATHE SH