Aufgaben zum Diffie-Hellmann-Verfahren

1. Alice und Bob wollen dem multiplikativen Verfahren

$$V(x) = k \cdot x \ \ mod \ \ 127$$

Nachrichten austauschen. Dazu wird jeder Buchstabe zunächst in seinen ASCII-Code x umgewandelt und dann mit $V(x)$ codiert.
Dazu tauschen sie zuerst mit dem Diffie-Hellman-Verfahren den Schlüssel k aus.
Berechnen Sie mit den Daten $p = 37$, $g = 22$, $a = 13$ und $b = 11$ die Tausch-Zahlen α, β und den Schlüssel k.
Wie lautet die Codierung des Wortes "Bob" ?

2. Alice und Bob schicken sich den geheimen Schlüssel k mit dem Diffie-Hellman-Verfahren zu.
Dabei wird die Botschaft mittels der multiplikativen Verschlüsselung

$$V(x) = k \cdot x \ \ mod \ \ 26$$

verschlüsselt.
Ein Man in the Middle (MiM) fängt die Botschaft von Alice ab.
Sie lautet: FKXSQBQZACKFAHRSCAN
Außerdem gelangt er an die Zahlen $p = 23$, $g = 15$, $\alpha = 5$ und $\beta = 14$.
Bestimmen Sie die decodierte Nachricht von Alice an Bob und berechnen Sie die fehlenden Daten des Diffie-Hellman-Verfahrens a und b.