1. Using an affine cipher (mod 26), we do a chosen plaintext attack using "hahaha". The ciphertext is "NONONO". Determine the encryption function. Note the 26 letters correspond to the integers {0,1,...,25}. (4 points)

> We know 7 maps to 13, and 0 maps to 14. Assume the function is $y = ax + b$.
>
> $$\begin{aligned} 13 &= 7x + b \bmod 26 \\ b &= 14 \bmod 26 \end{aligned} \tag{1}$$
>
> Then $13 = 7x + 14$, we have $7x = -1 = 25 \bmod 26$, which has the unique solution $a = 17$
>
> Hence, the solution is a = 17, b = 14.

2. The ciphertext *CRWWZ* was encrypted by an affine function mod 26. The plaintext starts *ha*. Decrypt the message. (6 points)

> We know 7 maps to 2, and 0 maps to 17. Assume the function is $y = ax + b$.
>
> $$\begin{aligned} 2 &= 7x + b \bmod 26 \\ b &= 17 \bmod 26 \end{aligned} \tag{2}$$
>
> Then $2 = 7x + 17$, we have $7x = -15 = 11 \bmod 26$, which has the unique solution $a = 9$
>
> Hence, the solution is a = 9, b = 17.