#1 $Z_{10} = \{0, 1 \ldots, 9\}$ $SE = (K, E, D)$

a)

$D_\pi(E_\pi(M)) = M$

```
Alg D_π(C)
    For i = 1, ..., |C| do
        P[i] ← (C[i] − i) mod 10
        M[i] ← π^{-1}(P[i])
    Return M
```

shows that it is not perfectly secure

#1b This is not a substitution cipher because the encoding is not done directly onto the message but to P[i]. Additionally, the scheme is not one-to-one since you can have a message 3210, where the ciphertext output C[1] = C[2] = C[3] = C[4] = 4, so each input of i maps to the same output for C. This tells us that this scheme is not a substitution cipher

#7c $\Pr[\mathcal{E}_a(M_1)=C] \neq \Pr[\mathcal{E}_a(M_2)=C]$

$C = 1010$

$M_1 = 2121$

$M_2 = 3223$ $\Pr[\mathcal{E}_a(M_2)=C] = \Pr[\mathcal{E}_a(3223)=1010]$

$= \boxed{0}$

Since $\mathcal{E}_a(M_2[1])$ connot equal $\mathcal{E}_a(M_2[2])$

$$\Pr[\mathcal{E}_a(M_1)=C] = \Pr[\mathcal{E}_a(2121)=1010]$$

$$\frac{|\{\mathcal{E}_a \in \text{Perm}(\mathbb{Z}_{10}) : \mathcal{E}_a(2)\mathcal{E}_a(1)\mathcal{E}_a(2)\mathcal{E}_a(1) = 1010\}|}{|\text{Perm}(\mathbb{Z}_{10})|}$$

$$= \frac{8!}{10!} = \boxed{\frac{1}{90}}$$

#1c

$$Pr[E_a(M_1) = C] \neq Pr[E_a(M_2) = C]$$

$$\frac{1}{90} \neq 0$$

This proves that this encryption scheme is NOT perfectly secure, given that $M_1, M_2, C \in \mathbb{Z}_{10}$, & that $E_a(M_1) = C = E_a(M_2)$. The probabilities are not the same shows that it is not perfectly secure

(2a) The key length is [7]

The key is [ATURING]

(2b) I recovered the key by writing a python code of the Kasiski examination & Friedman test & frequency analysis. First I used the Kasiski examination & Friedman function to get the key length. After, I made sure the length was the right length by test the decryption of the cipher text on a random key, "ABCDEFG". After I verified that the key length was 7, I used the frequency analysis approach where I placed the cipher text into 7 columns. Within each column I found the highest frequency character. I treated each column as a Caesar cipher and subtracted the most frequent character by "E". After doing so, I got the key "PIUGING", the last 3 letters looked correct to me so I kept them. I subtracted the initial 4 columns by "T" and got "ATFRING". The "F" looked odd as part of the key so I replaced it with "u" from the precious subtraction. Then I got the key "ATURING" and used the decryption function. I was able to successfully get a readable message.