Q.1 (key length is denoted by n)

$Pr[n=1] = 0.5 = Pr[n=2]$

$Pr[m = aa] = 0.4$

$Pr[m = ab] = 0.6$.

$Pr[m = aa \mid c = bb] = ?$

For $n=1$ $Pr[m=aa \mid c=bb] =$

$$= \frac{Pr[c=bb \mid m=aa] \times Pr[m=aa]}{Pr[c=bb]}$$

$Pr[c=bb \mid m=aa]$: For key length 1: $1/26$

$$\begin{array}{cc} a & a \\ b & b \\ \hline b & b \end{array}$$

26 possibilities)

For keylength 2: $\frac{1}{26} \cdot \times \frac{1}{26}$

$$\begin{pmatrix} a & a \\ b & b \\ \hline b & b \end{pmatrix}$$

$$Pr[C = bb \mid m = aa] = \left[\frac{1}{26} + \frac{1}{26} \times \frac{1}{26} \right] \times 0.4 \times 0.5$$

$$= 0.01597 \times 0.5$$

$Pr[C = bb]$

$$Pr[C = bb] = Pr[C = bb \mid m = aa] + Pr[C = bb \mid m = ab]$$

$Pr[C = bb \mid m = ab]$

For key length 1: no key can produce bb from ab.

For key length 2 :

$$\begin{array}{r} a\ b \\ b\ a \\ \hline b\ b \end{array}$$

one key can produce the required ciphertext

$$= \frac{1}{26} \times \frac{1}{26}$$

$$\therefore Pr[C = bb \mid m = ab] = \left(\frac{1}{26} \times \frac{1}{26}\right)$$

0.6×0.5

$$= 0.000088755 \times 0.5$$

$$Pr[C = bb] = 0.01686383 \times 0.5$$

$$= 0.0084$$

$$\frac{Pr[C = bb \mid m = ab]}{Pr[C = bb]} = 0.9473$$

2. Not true. Consider the OTP so that the encryption appends a bit that is 0 with probability $1/4$ and 1 with probability $3/4$. The scheme is perfectly secret but the ciphertexts ending in 1 are more likely than the ones ending in 1.

3. Not true. For a perfectly secret scheme we have $\Pr[M=m \mid C=c] = \Pr[M=m]$ and $\Pr[M=m' \mid C=c] = \Pr[M=m']$. But the distribution may be such that $\Pr[M=m] \neq \Pr[M=m']$