1. For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

a.The message space is M = {0,...,4}. Algorithm Gen chooses a uniform key from the key space {0,...,5}. $Enc_k(m)$ **returns [k+m mod 5], and** $Dec_k(c)$ **returns [c-k mod 5].**

> Not perfectly secret. When found c=0, it is more likely to be m=0, and c=1 is more likely to be m=1, and c=2 is more likely to be m=2

M	K	C
0	0	0
0	1	1
0	2	2
0	3	3
0	4	4
0	5	0
1	0	1
1	1	2
1	2	3
1	3	4
1	4	0
1	5	1
2	0	2
2	1	3
2	2	4
2	3	0
2	4	1
2	5	2

b. The message space is M = { m ∈ {0,1}l | the last bit of m is 0}. Gen chooses a uniform key from {0,1}l-1. $Enc_k(m)$ **returns cipher-text m ⊕ (k || 0), and** $Dec_k(c)$ **returns c ⊕ (k || 0).**

> As k is from $\{0,1\}^{l-1}$ and $||$ is logical OR operator, which means 0||1 is 1, 0||0 is 0, so there is nothing effect on the k. Therefore, $Enc_k(m)$ is actually m $\oplus$ k and $Dec_k(c)$ is c $\oplus$ k, which is the binary cipher.
>
> The binary cipher is perfectly secret, so this is perfectly secret.

2. Present two methods to generate pseudo-random numbers using hardware.

> Yarrow algorithm
>
> Clock drift