1. An example for which $Pr[Enc_K(m)=c] \neq Pr[Enc_K(m')=c]$ could be:

Let $m = aaa$, $m' = abc$

$c = zzz$

Then $Pr[Enc_K(m)=c] > 0$ and

$Pr[Enc_K(m')=c] = 0$, since a, b, c can't be mapped to z at the same time by mono-alphabetic substitution cipher

Thus, mono-alphabetic substitution cipher is not perfectly secret

2. Since the ciphertext has 17 characters, and two days are in order, the plaintext can only be WEDNESDAYTHURSDAY or WEDNESDAYSATURDAY, which have exactly 17 characters

m	W	E	D	N	E	S	D	A	Y
	22	4	3	13	4	18	3	0	24
c	Y	U	B	C	X	G	J	R	Y
	24	21	1	2	23	6	9	17	24
k	C	R	Y	P	T	O	G	R	A
	2	17	24	15	19	14	6	17	0

By doing the math with first 9 characters of the ciphertext and WEDNESDAY, we get the first 9 characters of the key to be CRYPTOGRA

Thus, it is reasonable to guess the key starts with CRYPTOGRAPHY.

c	H	H	R
	7	7	17
k	P	H	Y
	15	7	24
m	S	A	T
	18	0	19

Using PHY to decipher HHR, we get SAT.
Therefore, the plaintext must be WEDNESDAYSATURDAY.
By comparing SATURDAY with HHRCJIUL, we know the next part of the key is ISFUN, so the key is CRYPTOGRAPHYISFUN

3. a

pqrs	15 16 17 18
mnop	12 13 14 15
svux	18 21 20 23
jmlo	9 12 11 14

Both pqrs and mnop have a form of k, k+1, k+2, k+3 and both svux and jmlo have a form of k, k+3, k+2, k+5. Since the shift cipher shifts all characters by an equal amount, it is possible to tell whether the plaintext has a form of k, k+1, k+2, k+3 or k, k+3, k+2, k+5. However, it is impossible to tell pqrs from mnop and tell svux from jmlo. For example, pqrs with a key 1 and mnop with a key 4 both gives qrst. Thus, it's impossible to determine the users password.

3. b. Period 2: In this case, the first and third characters will be shifted by the same amount. So do the second and fourth ones.

	3rd - 1st	4th - 2nd
mnop	2	2
jmlo	2	2

However, the differences are all 2. Thus, it's impossible.

Period 3: In this case, the first and fourth characters will be shifted by the same amount

	4th - 1st
mnop	3
jmlo	5

The differences are different, So for the ciphertext, if this difference is 3, the plaintext is mnop, if this difference is 5 the plaintext is jmlo

Period 4: For some ciphertext c, there exist keys K and K' such that $Enc_K(mnop) = Enc_K(jmlo) = c$. Thus, it's impossible.

4.a. $Pr[Enc_K(0)=0] = \frac{2}{5}$ (when $k \in \{0,5\}$)

$Pr[Enc_K(1)=0] = \frac{1}{5}$ (when $k=4$)

$Pr[Enc_K(0)=0] \neq Pr[Enc_K(1)=0]$

Thus, it's not perfectly secret

4.b. $|\mathcal{M}| = |\{0,1\}^{2n}| = 2^{2n}$, $|K| = |\{0,1\}^{n}| = 2^{n}$

$|K| < |\mathcal{M}|$

According to Theorem 2.10, if $|K| < |\mathcal{M}|$, then the encryption scheme is not perfectly secret.