Ex. 2a) i)

$M = 1101101111111011$

$K=0$: $C_1 = 1101101111111011$

ou

$K=1$: $C_2 = 0010010000000100$

pas sûr !

Ex. 2a) ii)

$$\begin{cases} \text{avec prob } \frac{1}{2} & C_i = M_i \\ \text{avec prob } \frac{1}{2} & C_i = M_i \oplus K_i \end{cases}$$

$P(C_i = M_i) = \frac{3}{4}$

pas sûr !

Ex 2a) iii)

$$\begin{cases} C_i = M_i & \text{avec prob } \frac{1}{2} \\ C_i = M_i \oplus 1 & \text{avec prob } \frac{1}{2} \end{cases}$$

sûr à 100% !

Ex 2b)

M = séquence de lettres

i) K = séquence de lettres tirées unif. au hasard

$$C_i = (M_i + K_i) \bmod 26$$

sûr à 100% !

M BONJOUR
K KFDEVWZ
C ...

ii) $C_i = M_i$ avec prob $\frac{1}{2}$

$C_i = (M_i + K_i) \bmod 26$ avec prob $\frac{1}{2}$

pas sûr !

BONJOUR
K DE Z
$=$ LOQNOUP

iii) encore moins sûr !

$\begin{cases} C_i = M_i \\ C_i = (M_i + N) \bmod 26 \end{cases}$ ^{13}