Solution 1 :

1) Pour n = 1

Pr[X=0] = Pr[X=1] = 1/2

Pr[Y=0] = p_1 et Pr[Y=1] = p_2

Selon la table du Xor:

Z=0 ssi: (X=0 et Y=0) ou (X=1 et Y=1),

Donc: Pr[Z=0] = (Pr[X=0] × Pr[Y=0]) + (Pr[X=1] × Pr[Y=1])

= $p_1/2 + p_2/2$

= $(p_1+p_2)/2 = 1/2$

Ainsi: Pr[Z=0] = Pr[Z=1] = 1/2 (Z est donc uniforme) CQFD (1.5 pts)

Concernant le $\vee$ on procède de la même manière :

Pr[X=0] = Pr[X=1] = 1/2

Pr[Y=0] = p_1 et Pr[Y=1] = p_2

Selon la table du $\vee$:

Z=0 ssi: (X=0 et Y=0),

Donc: Pr[Z=0] = (Pr[X=0] × Pr[Y=0])

= $1/2 \times p_1 = p_1/2$

Ainsi: Pr[Z=1] = $1-p_1/2=p_1 + p_2 – p_1/2 = p_2 + p_1/2 > p_1/2$ (Z est donc non uniforme) CQFD (1.5 pts)

2) Considérons un schéma de Feistel à un tour définie par la fonction F :$\{0,1\}^n \rightarrow \{0,1\}^n$. Soit X_0 une entrée du schéma de Feistel. Par définition nous avons toujours $X_0^R = X_1^R$ (1 pt) alors que cette propriété n'est réalisée qu'avec une probabilité de 2^{-n} pour une permutation aléatoire. Donc cette propriété est suffisante pour distinguer le schéma de Feistel d'une permutation aléatoire avec un avantage de $1-2^{-n}$ proche de 1. (2 pts)

Solution 2 :

1) $MAC_k(m) = F_k(m_1) \oplus F_k(m_2) \oplus \ldots \oplus F_k(m_n)$

   a) On peut échanger deux blocs sans changer la valeur du MAC. En effet l'attaquant envoie au challenger le message m_0m_1 et reçoit le MAC t, ensuite il envoie le message m_1m_0 avec le MAC t et reçoit vrai (falsification existentielle). (2 pts)

   b) Pour authentifier n'importe quel message M=$m_1||m_2$. L'attaquant peut demander les MAC de $m_1||R$ et de $m_2||R$ tel que R est un bloc aléatoire, il reçoit $T_1=F_k(m_1) \oplus F_k(R)$ et $T_2=F_k(m_2) \oplus F_k(R)$ alors le MAC de $m_1||m_2$ est $T_1 \oplus T_2$ (2 pts)

2) Lors du déchiffrement m[0] = D(k, c[0]) ⊕ IV = "dest=80…"

   L'objectif de Bob et de modifier la destination de telle sorte quelle devienne 25, pour cela IV' = IV ⊕ (…80…) ⊕ (…25…) (2 pts).

   En effet D(k, c[0]) ⊕ IV'= D(k, c[0]) ⊕ IV⊕ (…80…) ⊕ (…25…)="dest=80…"⊕ (…80…) ⊕ (…25…) en remplaçant les points par des 0 pour ne pas affecter les autres caractères (2 pts).

Solution 3 :

1) Bob peut retrouver le message x en calculant $x = M_3 \oplus b$. Sachant que b est la clé secrète de Bob.

   En effet $M_3 \oplus b = M_2 \oplus a \oplus b = M_1 \oplus b \oplus a \oplus b = x \oplus a \oplus b \oplus a \oplus b = x$ (3 pts) Aussi il peut utiliser la solution d'Ève décrite dans la deuxième question.

2) Ève qui intercepte les M_i peut retrouver x sans connaitre les clés a et b en faisant $M_1 \oplus M_2 \oplus M_3 = x$.

   En effet $M_1 \oplus M_2 \oplus M_3 = M_1 \oplus M_1 \oplus b \oplus M_2 \oplus a = M_1 \oplus M_1 \oplus b \oplus M_1 \oplus b \oplus a = M_1 \oplus a = x$ (3 pts)