J'ai (Maxime) posé une question au prof sur la taille des messages après ECB, CTS etc. Voici dans son intégralité sa réponse :

Ci après des extraits du corrigé du contrôle de 2010

Chiffrement par bloc avec chaînage.

Rappels de cours : On rappelle les divers modes de chaînage et/ou d'utilisation des algorithmes par bloc

ECB (Electronic Code Book)

CBC (Cipher Block Chaining)

CTS (Cipher Text Stealing = Vol de texte chiffré)

CTR (CounTeR = CompTeuR)

OFB (Output Feedback)

1. On veut chiffrer un message de 50 octets (sans compression) en utilisant DES en mode ECB. De combien de bits se composera le message chiffré ?

~~(A) 400~~ ~~(B) 428~~ **(C) 448** ~~(D) 512~~ ~~(E) autre valeur~~

50 octets = 400 bits, mais avec DES en mode ECB on a forcément un nombre entier de blocs de 64 bits, donc ici 7 blocs = 448 octets

2. On veut chiffrer un message de 50 octets (sans compression) en utilisant AES en mode ECB. De combien de bits se composera le message chiffré ?

~~(A) 400~~ ~~(B) 428~~ ~~(C) 448~~ **(D) 512** ~~(E) autre valeur~~

50 octets = 400 bits, mais avec AES en mode ECB on a forcément un nombre entier de blocs de 128 bits, donc ici 512

3. On veut chiffrer un message de 50 octets (sans compression) en utilisant DES en mode CTS. De combien de bits se composera le message chiffré ?

(A) 400 ~~(B) 428~~ ~~(C) 448~~ ~~(D) 512~~ ~~(E) autre valeur~~

Le mode CTS permet d'avoir un texte chiffré de même longueur que le clair dès que cette longueur est supérieure ou égale à un bloc

4. On veut chiffrer un message de 50 octets (sans compression) en utilisant AES en mode CTR. De combien de bits se composera le message chiffré ?

~~(A) 512~~ ~~(B) 528~~ ~~(C) 576~~ ~~(D) 640~~
(E) autre valeur

Le mode Compteur utilise l'AES pour générer un masque XOR. On prend ensuite dans le masque uniquement le nombre de bits nécessaires pour « XORer ». On aura donc, dans tous les cas, un texte chiffré de même longueur que le clair, donc ici 400 bits

5. On veut chiffrer un message de 56 bits (sans compression) en utilisant AES en mode CTS. De combien de bits se composera le message chiffré ?

~~(A) 56~~ ~~(B) 64~~ ~~(C) 96~~ **(D) 128** ~~(E) autre valeur~~

Le mode CTS permet d'avoir un texte chiffré de même longueur que le clair dès que cette longueur est supérieure ou égale à un bloc. Si la longueur est inférieure, on est obligé de chiffrer au moins un bloc, soit 128 bits

---

Il faut comprendre qu'un algorithme par blocs chiffre toujours un nombre entier de blocs.

- Si le message est plus petit qu'un bloc, il faut compléter à un bloc (par exemple en rajoutant des bits à zéro) et on transmet minimum un bloc.

- Si le message est plus grand qu'un bloc, le mode CTS est une astuce consistant à ne pas transmettre entièrement l'avant dernier bloc, de façon que le texte chiffré ait la même longueur que le texte clair. Mais il faut bien sûr que le message soit plus long qu'un bloc.

- Exception : le mode CTR : l'algo de chiffrement sert à créer un masque XOR, et le texte chiffré a alors toujours la même longueur que le texte en clair.

Relire le support de cours.

Une fois ces points compris, la réponse auxdites questions est évidente

Bien cordialement

JLS