TD 4 Propriété d'indistinguabilité

Question 1

Montrez que les schémas suivants ne sont pas IND-CPA et donnez l'avantage de l'adversaire :

1. AES-ECB avec un IV aléatoire et uniforme.
2. AES-CBC avec un IV fixe.
3. AES-CBC avec un IV fixé comme étant le dernier bloc du chiffré précédent.
4. AES-GCM avec un IV fixe.
5. AES-GCM avec un IV fixé comme étant le dernier bloc du chiffré précédent.
6. Textbook-RSA.
7. RSA avec le schéma de remplissage suivant :
   $[\ M \ || \ PS \ || \ 0 \cdots 0\ ]$
   où M est le message sur 32 octets, PS une suite pseudo-aléatoire sur 1 octet et le reste un remplissage de zéros.

Question 2

Donnez une recommandation sur la construction 7 de la question précédente pour atteindre une propriété de sécurité IND-CPA.

Question 3

Montrez que AES-CBC avec IV aléatoire et uniforme n'est pas IND-CCA2. Vous pourrez étudier comment se comporte le déchiffrement lorsque l'adversaire inverse un bit du chiffré.

Question 4

Montrez que AES-GCM avec IV aléatoire et uniforme est IND-CCA2. Vous considérerez que AES-CTR avec IV aléatoire et uniforme est IND-CPA.

Question 5

Textbook-RSA avec un mécanisme d'Encapsulation de clé est-il IND-CCA2 ?

Question 6

RSA avec le schéma de remplissage de la question 2, intégré dans un mécanisme d'Encapsulation de clé est-il IND-CCA2 ?