Composition de Cryptographie – 2016/2017

Il est recommandé aux élèves de bien choisir l'ordre des questions selon leurs compétences et rapidités.

Si l'élève n'arrive pas à faire une démonstration, il peut considérer que le résultat de la démonstration est admis sur le reste l'exercice.

Le support de cours et les calculatrices sont permis

1. QCM

1. Le PKCS7 est la seule enveloppe de sécurité
    a. Vrai
    b. Faux

2. Le PKCS7-Encrypted permet de chiffrer un document
    a. avec une clé générée aléatoirement
    b. avec une clé fixe chiffrée par la clé publique du destinataire
    c. avec une clé fixe générée aléatoirement et transmise chiffrée par la clé publique du destinataire
    d. avec une clé transmise en dehors du PKCS7-Encrypted

3. Le PKCS7-Enveloped permet de chiffrer un document
    a. avec une clé fixe chiffrée par la clé publique du destinataire
    b. avec une clé fixe générée aléatoirement et transmise chiffrée par la clé publique du destinataire
    c. avec une clé transmise en dehors du PKCS7-Enveloped

4. Dans un PKCS7-Enveloped le mode de padding du chiffrement est transmis comme paramètre dans l'enveloppe :
    a. Vrai
    b. Faux

5. Le PKCS7-Signed and Enveloped est la seule méthode pour transmettre un document signé et chiffré :
    a. Vrai
    b. Faux

6. En cryptographie symétrique par blocs, que représente le "Vecteur IV" ?
    a. Une extension de la clef secrète
    b. Une initialisation du chaînage des blocs en mode CBC (Cipher Block Chaining)
    c. Une initialisation du chaînage des blocs en mode ECB (Electronic Code Book)
    d. La clef de confection du MAC de l'algorithme considéré

7. Une clé USB de stockage peut être utilisée comme Dispositif de sécurité logique
    a. Vrai
    b. Faux

8. Dans une carte à puce la clé privée est exportable
    a. Vrai
    b. Faux
    c. Parfois

9. La Taille minimum d'une clé RSA sûre est de :
    a. 1024 bits
    b. 2048 bits
    c. 512 bits

10. Parmi les fonctions hash suivants quelle est la fonction hash la plus sûre ?
    a. SHA1
    b. MD5

2. Questions Courtes (maximum 4 lignes)

a) Quels sont les avantages et inconvénients des modes de padding ISO et ANSI ?
b) Un message chiffré par AES/CBC a eu n blocs successifs altérés, quel est le nombre de blocs déchiffrés en erreur ?
c) Rappeler rapidement le fonctionnement du mode CTR.
d) Justifier pourquoi dans le cas d'utilisation d'un chiffrement en parallèle d'un texte par plusieurs machines, il faut choisir le mode CTR et non pas le CBC.

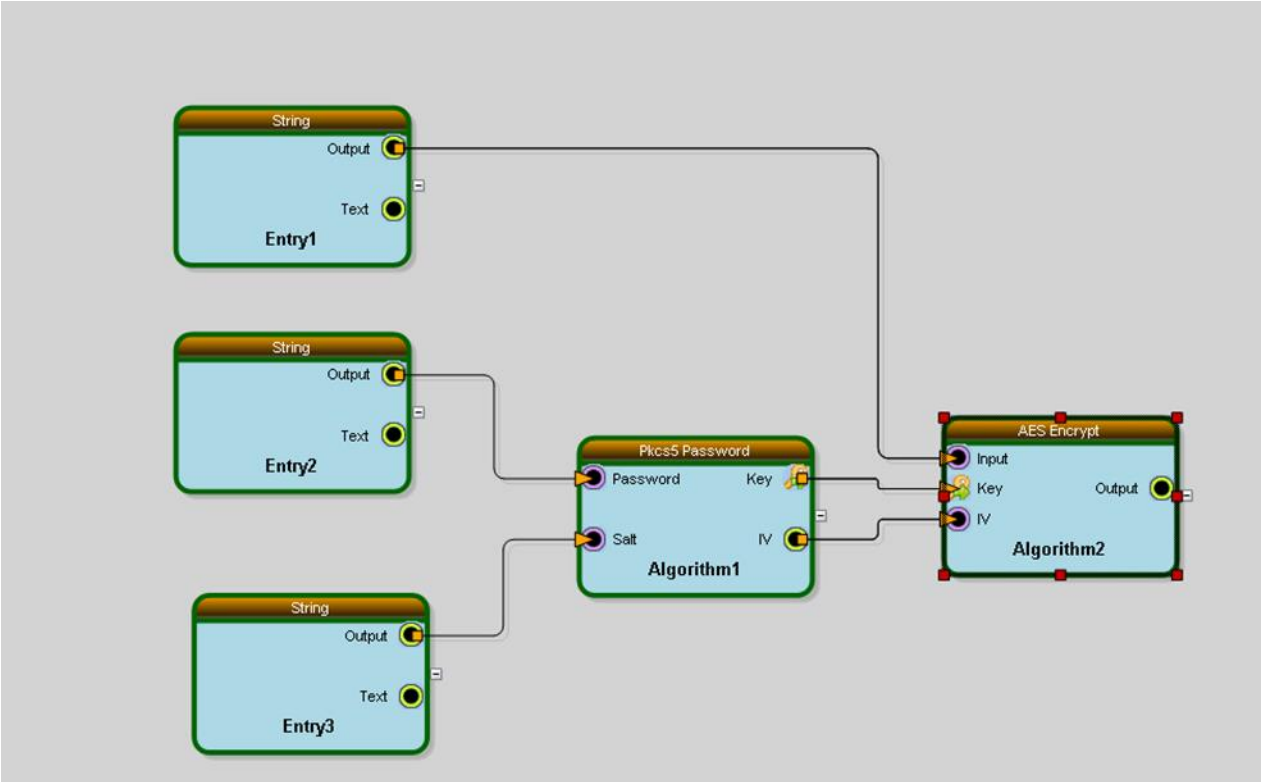
3. Parseur de l'OID

Soit la séquence DER d'un objet Object Identifier (OID) : T/L/V
On supposera L sur un octet.

a) Quelle est la valeur de T primitif ?
b) Quelle est la valeur minimale de L et sa valeur maximale ?
c) Soit V un succession d'octets $V_0V_1…V_n$. Quelle est la valeur de n ?

4. Schéma cryptographique

Soit le schéma suivant :



Les variables des différents blocs sont les suivants :

Entry1:String

Output Values	
Text	alice au pays des merveilles
Output	alice au pays des merveilles

Entry2:String

Output Values	
Text	c'est mon secret
Output	c'est mon secret

Entry3:String

Output Values	
Text	du sel et du poivre
Output	du sel et du poivre

Algorithm1:Pkcs5 Password

Output Values	
Key	09 5E CA 1B 42 A1 E3 21 AC 27 AE 94 2E BC 6E 0D
IV	49 35 80 85 3C B2 9F 96 72 5F 2F EE 7F BF 1E 15

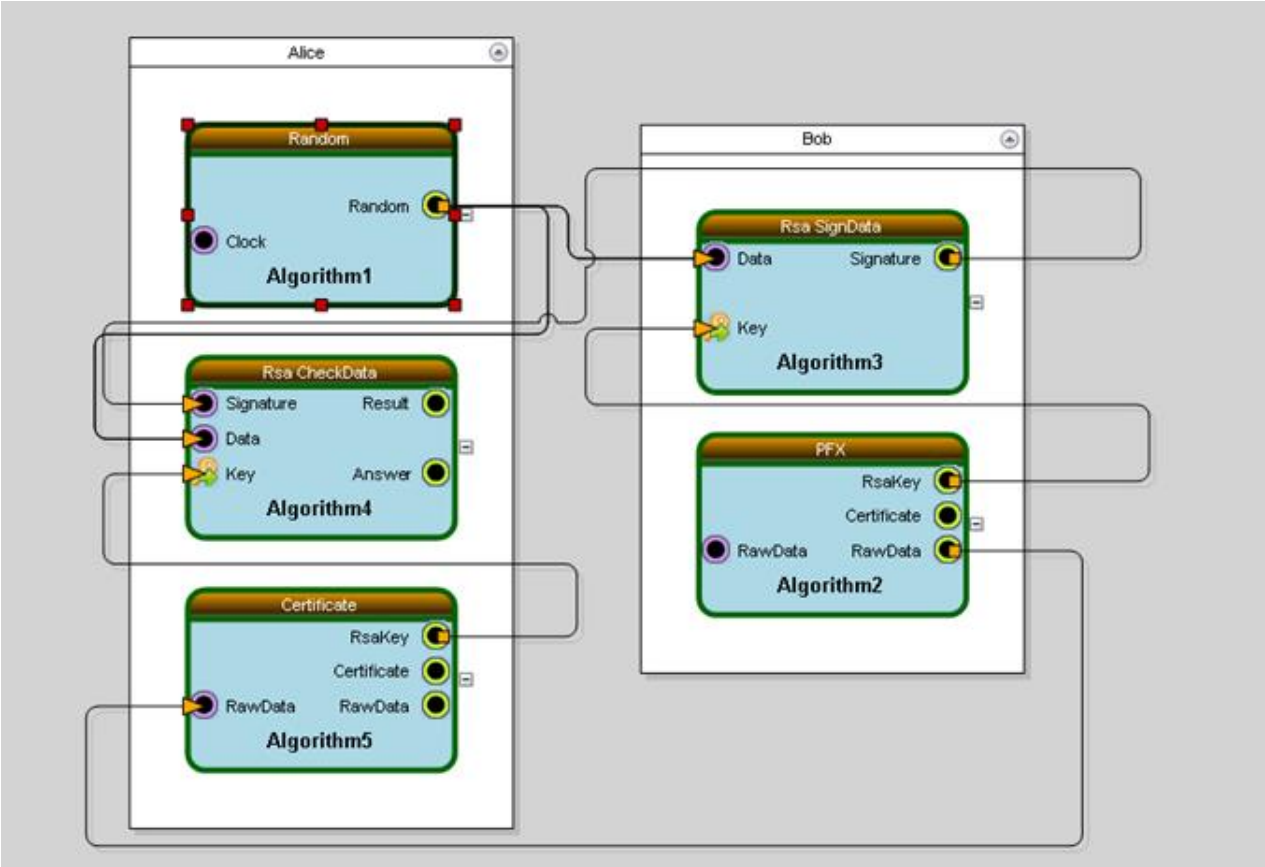
Algorithm2:AES

Input Values	
Input	61 6C 69 63 65 20 61 75 20 70 61 79 73 20 64 65 73 20 6D 65 72 76 65 69 6C 6C 65 73
Key	09 5E CA 1B 42 A1 E3 21 AC 27 AE 94 2E BC 6E 0D
IV	49 35 80 85 3C B2 9F 96 72 5F 2F EE 7F BF 1E 15
Output Values	
Output	15 65 74 F0 17 E8 8E 40 37 D7 68 40 D5 AB ED A2 14 39 07 AB EC 47 B4 23 7E D6 74 BA 34 5B 45 22

a) Interpréter le schéma
b) A quoi sert l'entrée Salt dans le module Algorithm1
c) Cette opération est réalisée côté l'émetteur Alice, compléter le schéma pour implémenter l'opération inverse chez le récepteur Bob.
d) Compléter le schéma dans le cas d'ajout de signature côté Alice et vérification de la signature côté Bob.

5. Schéma cryptographique 2

Soit le schéma suivant :



Les variables des différents blocs sont les suivants :

a) Quel service de sécurité est implémenté par ce schéma ?
b) Quelles sont les techniques utilisées ?
c) Un module demande un mot de passe. Lequel ?
d) Le module Rsa CheckData donne la sortie Answer suivante :

```
00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF 00 30 21 30
09 06 05 2B 0E 03 02 1A 05 00 04 14 36 F3 26 82
C0 23 95 58 18 4D 39 57 FA A3 88 F8 00 A4 51 1D
```

- Sans interpréter la valeur de l’OID quelle fonction hash a été utilisée (Md5, Sha1, Sha256, Sha512) et pourquoi ?