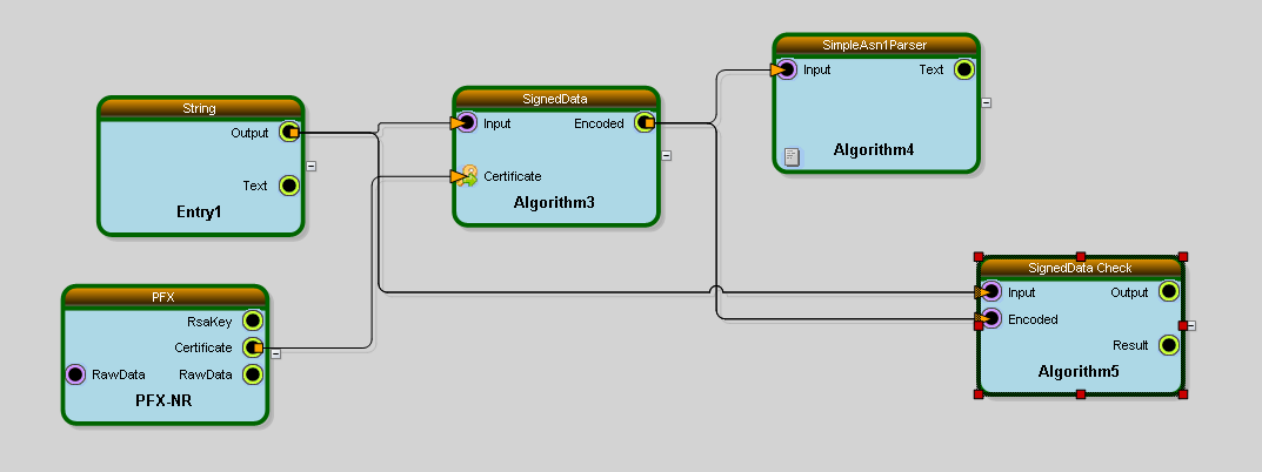
Composition de Crypto

La composition est composée de plusieurs exercices

Le support de cours est permis. La majeure partie des questions font appel au sens pratique.

1. PKCS7 et DER



SignedData désigne la fonctionnalité Signature PKCS7.
SignedData-Check désigne la fonctionnalité de Vérification de Signature PKCS7.
Les entrées/sorties Certificate désignent un handle (ou contexte) d'un certificat avec ou sans clé privée.

Les paramètres des blocs Algorithm3 et Algorithm5 sont les suivants :

Algorithm3:Pkcs7

Variable	Value
Parameters	
AddSignatureDate	False
SignatureHashAlgorithm	Sha256
SignatureLevel	Signature
Detached	True
IncludeOption	EndCertOnly

Algorithm5:Pkcs7

Variable	Value
Parameters	
Function	SignedCheck
Detached	True
CheckOnlySignature	True

Dans le fonctionnement actuel de le début de la sortie de parseur Asn1est la suivante:

```
(0x30,0x000000,0x059B) SEQUENCE
    (0x06,0x000004,0x0009) OBJECT IDENTIFIER : signedData : '1.2.840.113549.1.7.2'
    (0xA0,0x00000F,0x058C) CONTEXT SPECIFIC (0)
        (0x30,0x000013,0x0588) SEQUENCE
            (0x02,0x000017,0x0001) INTEGER : '1'
            (0x31,0x00001A,0x000F) SET
                (0x30,0x00001C,0x000D) SEQUENCE
                    (0x06,0x00001E,0x0009) OBJECT IDENTIFIER : SHA256 : '2.16.840.1.101.3.4.2.1'
                    (0x05,0x000029,0x0000) NULL
            (0x30,0x00002B,0x000B) SEQUENCE
                (0x06,0x00002D,0x0009) OBJECT IDENTIFIER : data : '1.2.840.113549.1.7.1'
            (0xA0,0x000038,0x03A3) CONTEXT SPECIFIC (0)
                (0x30,0x00003C,0x039F) SEQUENCE
                    (0x30,0x000040,0x0287) SEQUENCE
                        (0xA0,0x000044,0x0003) CONTEXT SPECIFIC (0)
```

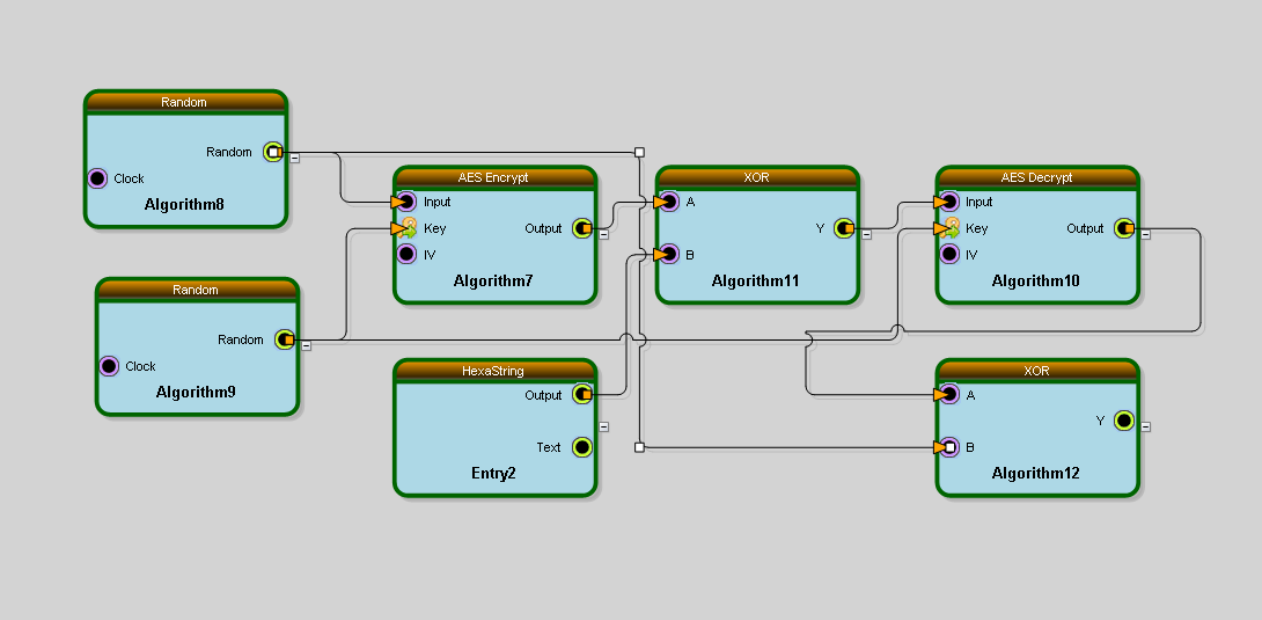
Dans le fonctionnement standard du PKCS7-SignedData, le début de la sortie de parseur Asn1 est la suivante :

```
(0x30,0x000000,0x05BB) SEQUENCE
        (0x06,0x000004,0x0009) OBJECT IDENTIFIER : signedData : '1.2.840.113549.1.7.2'
        (0xA0,0x00000F,0x05AC) CONTEXT SPECIFIC (0)
                (0x30,0x000013,0x05A8) SEQUENCE
                        (0x02,0x000017,0x0001) INTEGER : '1'
                        (0x31,0x00001A,0x000F) SET
                                (0x30,0x00001C,0x000D) SEQUENCE
                                        (0x06,0x00001E,0x0009) OBJECT IDENTIFIER : SHA256 : '2.16.840.1.101.3.4.2.1'
                                        (0x05,0x000029,0x0000) NULL
                        (0x30,0x00002B,0x002B) SEQUENCE
                                (0x06,0x00002D,0x0009) OBJECT IDENTIFIER : data : '1.2.840.113549.1.7.1'
                                (0xA0,0x000038,0x001E) CONTEXT SPECIFIC (0)
                                        (0x04,0x00003A,0x001C) OCTET STRING :
'416C6963652061752050617973206465732046573204D65727665696C6C6573'
                        (0xA0,0x000058,0x03A3) CONTEXT SPECIFIC (0)
                                (0x30,0x00005C,0x039F) SEQUENCE
```

a) Décrire le fonctionnement de ce schéma
b) Quelle est la différence majeure au niveau du schéma par rapport à un fonctionnement classique de l'enveloppe PKCS7-SignedData ?
c) Quel est le type de signature utilisée ?
d) A partir des deux débuts de sorties du parseur comment la vérification de signature peut connaître la différence entre les deux modes de signatures ?
e) Si la liaison entre la sortie Output de Entry1 et l'entrée Input de Algorithm5 est éliminée comment se comporte la vérification de la signature ? Pourquoi ?
f) Si la sortie Output de Entry1 est perturbée avant d'être liée à l'entrée de Input de Algorithm5 comment se comporte la vérification de la signature ?
g) Dans quel cas pratique ce schéma est utilisé ?

2. Altération des données chiffrées en mode CBC

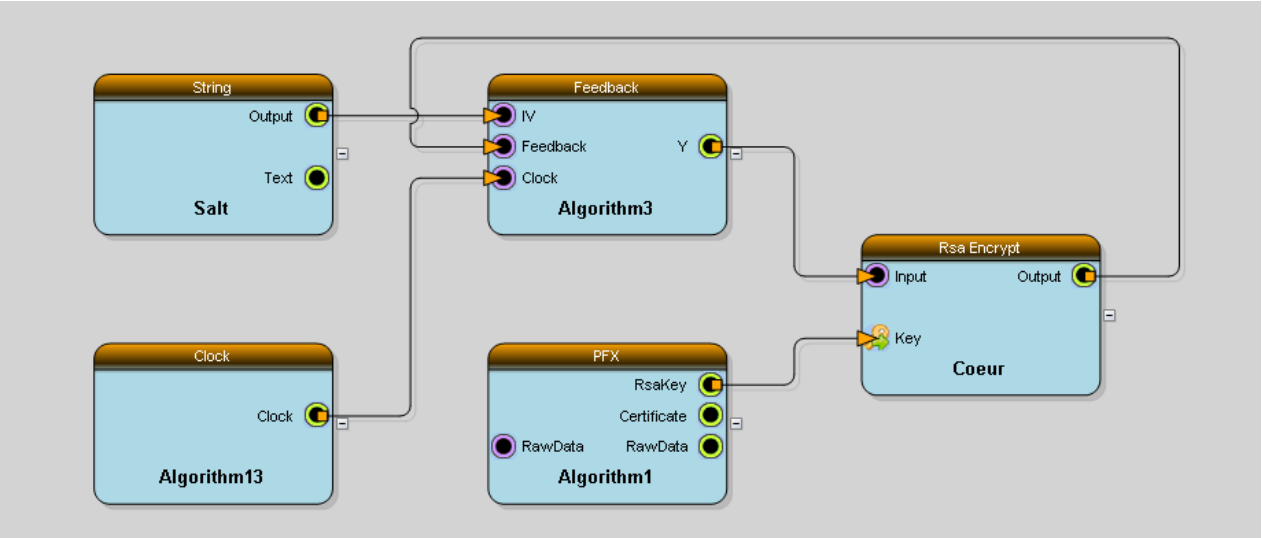
Soit le schéma



a) On suppose que la sortie M' du bloc AES de chiffrement est formé des blocs B'_0, B'_1, B'_2, .., B'_i, … B'_n. On suppose que le bloc B'_0 est perturbé par l'entrée B du XOR (Algorithm11). Ecrire les équations qui lient les 3 premiers blocs en sortie du bloc AES de déchiffrement. La clé utilisée est K, et IV est initialisé à 00….00 .
b) On remarque qu'en faisant varier la valeur de perturbation B de XOR (Algorithm11), le second bloc de la sortie de la comparaison Y du XOR(Algorithm12) est égale à la valeur de perturbation B. A partir des équations précédentes démontrer ce comportement.

3. Schéma Cryptographique

Soit le schéma



Le module Feedback permet la fonction suivante : Y = entrée IV pour t=0, sinon Y = entrée Feedback pour t = n*T où T est la période de l'horloge Clock et n est un entier.
On notera la valeur de Output de RSA Encrypt par X_n pour une valeur n, X_0 la valeur initiale, f la fonction Rsa Encrypt.

a) Ecrire la relation entre X_0, f et Salt . Ecrire la relation entre X_{n+1} et X_n .
b) En déduire la fonctionnalité de ce schéma.
c) Soit x la valeur à chiffrer en RSA mode pkcs1, décrire le format de la donnée sur laquelle sera appliquée l'exponentiation modulaire. On notera l la taille de x.
d) En lançant le schéma cryptographique, une erreur est générée par le module Cœur. A partir du point c interpréter cette erreur.
e) Que proposez-vous pour corriger l'erreur en d ?
f) Pourquoi X_n est prévisible ? Que proposez-vous pour le rendre non prévisible ?
g) Si le système est relancé, les mêmes valeurs X_n sont obtenues (système répétitif donc prévisible aussi). Que proposez-vous pour le rendre non répétitif ?

4. Padding AES

Alice envoie un message chiffré par AES un utilisant un padding Pa. Bob déchiffre le message en faisant varier le padding, qui sera noté Pb. Le but de cet exercice est d'étudier le comportement du déchiffrement selon les différentes valeurs de Pb. Compléter le tableau en indiquant si le déchiffrement est bon (OK) ou donne une erreur (NOK).

Pa	Pb = ISO 120126	Pb =Ansi X923	Pb = Pkcs7	Pb = None
ISO 10126	OK			
Ansi X923		OK		
Pkcs7			OK	

a) Pour quelle raison quand un certain mode padding Pb est utilisé par BOB le déchiffrement donnant la bonne taille du message clair est bon (OK) quel que soit la valeur du padding Pa utilisé par Alice ?
b) Si Bob fixe le padding à la valeur en a, quel est le risque auquel il est confronté ?