Composition de Cryptographie - 2012

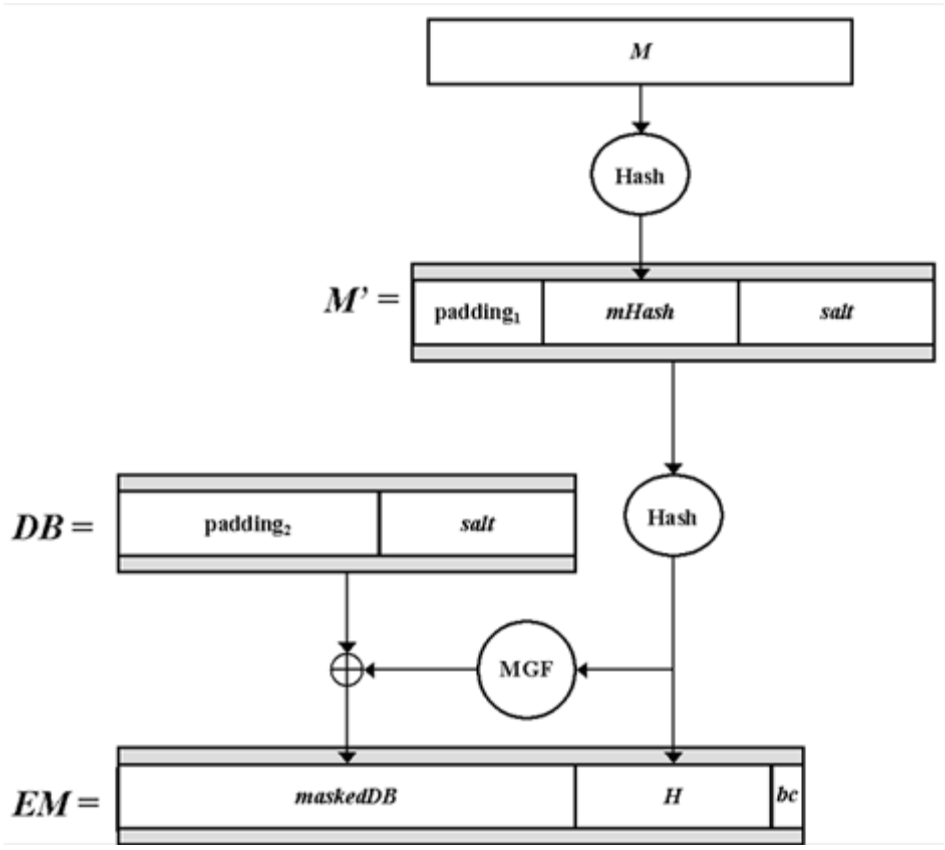
Il est recommandé aux élèves de bien choisir l'ordre des questions selon leurs compétences et rapidités.

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. RSA mode OAEP

Soit la signature utilisant le mode OAEP selon le schéma suivant :



Où

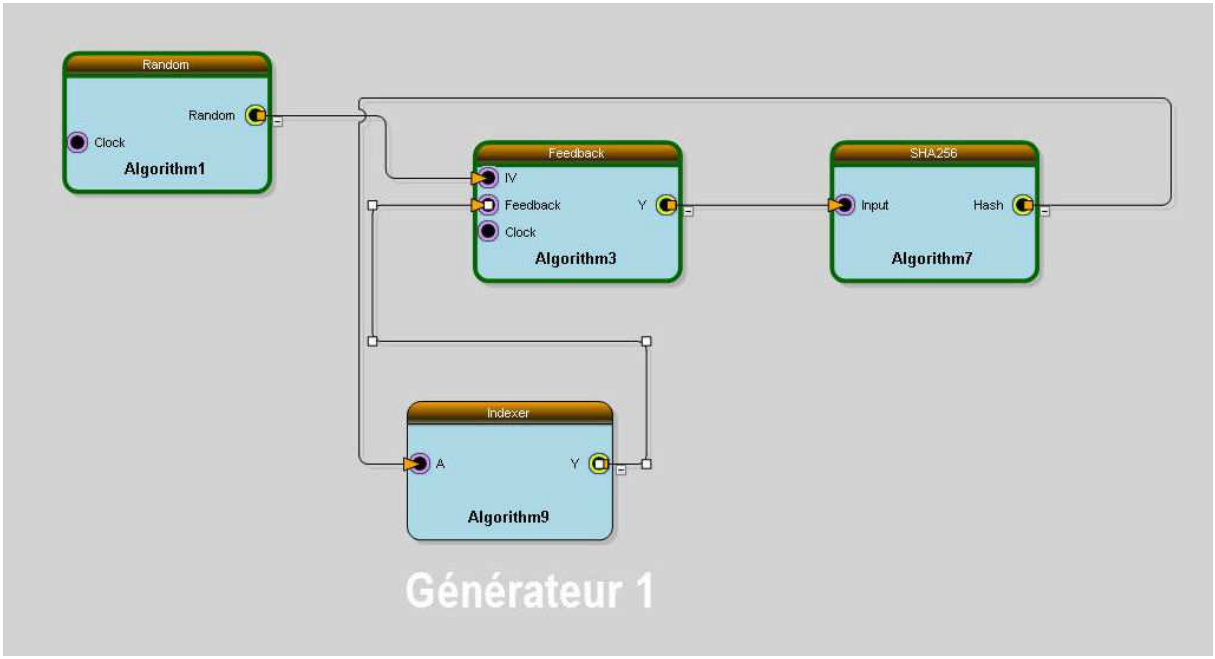
M est le message à signer, Hash est la fonction hash SHA256, la taille de la clé RSA 2048 bits est emLen.

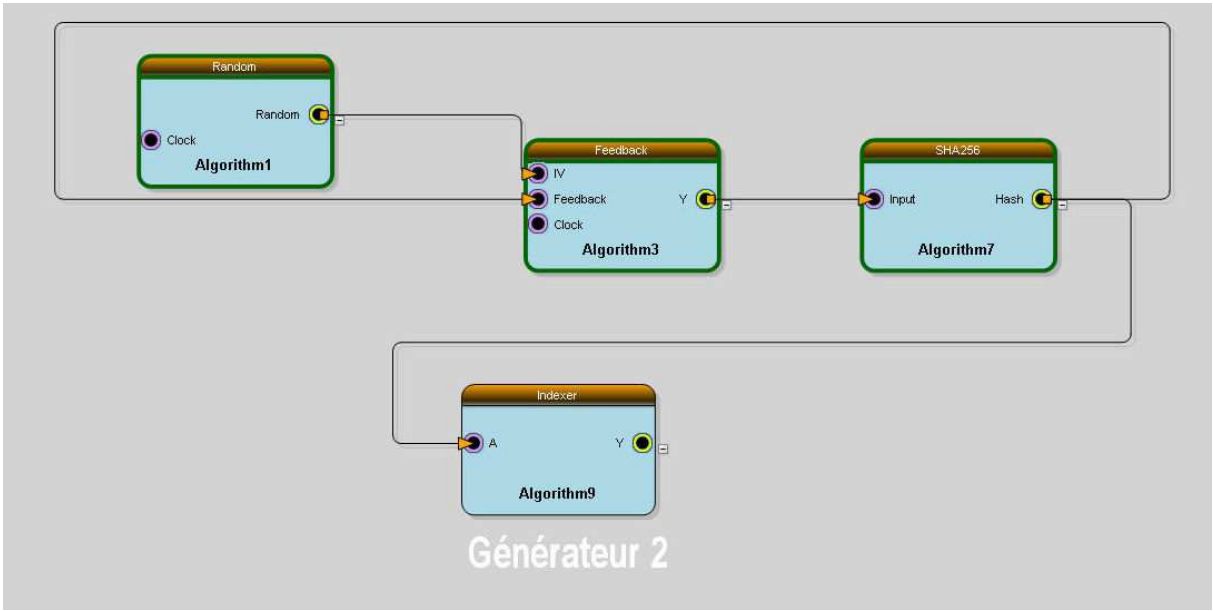
- Soit mHash = Hash (M), de taille hLen.
- salt est un nombre aléatoire de taille sLen = hLen.
- M' = (0x)00 00 00 00 00 00 00 00 || mHash || salt;
- Soit H = Hash (M'), de taille hLen.
- Générer un padding PS, de taille emLen - sLen - hLen - 2 d'octets à zeros.
- Soit DB = PS || 0x01 || salt.
- Soit maskedDB = MGF (H)
- Mettre le bit de poids fort de EM à 0
- EM = maskedDB || H || bc . bc vaut 0xbc

La signature consiste à appliquer la clé privée sur EM ainsi obtenu.

a) Quelle est la valeur hLen en octets?
b) Quelle est la taille de M' en octets ?
c) Quelle est la taille de maskedDB ?
d) En déduire la fonction logique de base MGF ?
e) Si le même message est signé une seconde fois, obtiendrons la même valeur binaire de signature ?
f) En déduire la qualité de OAEP par rapport à PKCS1V1.5
g) Décrire toutes les étapes de l'opération de vérification de la signature S d'un message M.

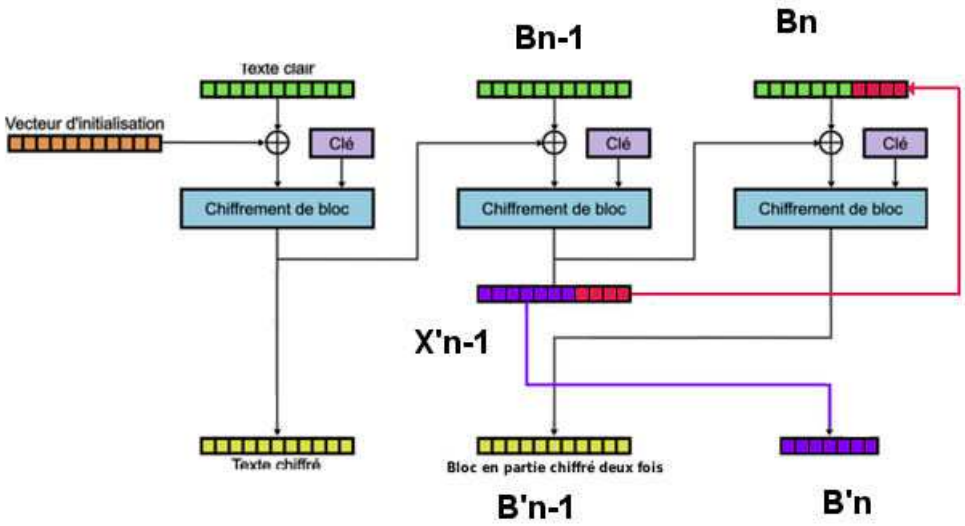
2. Générateurs Aléatoires





a) Pour chacun des générateurs expliquer le fonctionnement
b) Quel générateur est meilleur et pourquoi?
c) En faisant un parallèle avec les modes flux des algorithmes symétriques, donner les noms adéquats aux deux générateurs.

3. AES en mode Mode CBC_CTS



Le mode CBC_CTS ressemble au mode CBC sauf au niveau des deux derniers blocs, où :

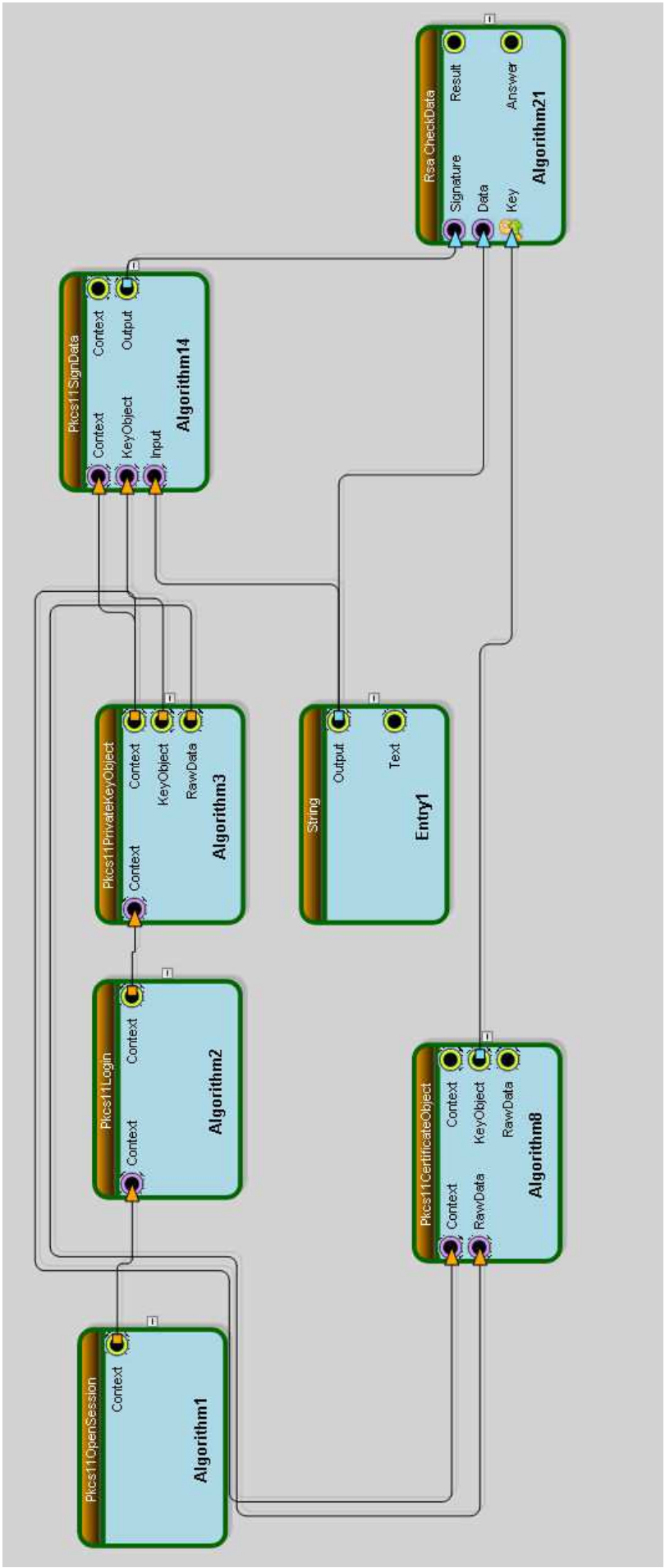
Soit t = taille de Bn, m est taille du bloc nécessaire au AES, et K la clé AES.

$X'_{n-1} = AES(B_{n-1} \text{ XOR } B'_{n-2}, K)$.
$B'_n = X'_{n-1}[0..t-1]$

$B'_{n-1} = AES\ (\ (B_n \,||\, X'_{n-1}[t..m-1]) \text{ XOR } X'_{n-1}\ , K)$

a) Quelle est l'utilité de ce mode ?
b) Ecrire les équations du déchiffrement en mode CBC_CTS des blocs B'_0, B'_1, B'i, B'_{n-1} et B'_n en fonction de K, IV.

4. Schéma Cryptographique



Soit le schéma bloc constitué des blocs suivants :

Numéro Bloc	**Type**
Algorithm1	Pkcs11OpenSession
Algorithm2	Pkcs11Login
Algorithm3	Pkcs11PrivateKeyObject
Entry1	String
Algorithm8	Pkcs11CertificateObject
Algorithm1	Pkcs11SignData
Algorithm21	RsaCheckdata

L’enchainement des entrées/sorties nommées Context correspond à un contexte de type Pkcs11.

a) Décrire le fonctionnement de ce schéma bloc.
b) Lors de l’exécution du schéma, un PIN est demandé. Quel bloc peut le demander et pour quelle raison a-t-on besoin de présenter un PIN ?
c) Pour quelle raison RsaCheckData n’a pas besoin d’une entrée Context ?
d) Même si le schéma fonctionne bien, qu’est-ce qu’il faut ajouter comme blocs (les déduire à partir des types des blocs) pour être complet logiquement.
e) La sortie Answer d’Algorithm21 est la suivante :

Answer:
```
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 00 30 31 30
0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20
CA 97 81 12 CA 1B BD CA FA C2 31 B3 9A 23 DC 4D
A7 86 EF F8 14 7C 4E 72 B9 80 77 85 AF EE 48 BB
```

- D’après sa forme à quoi peut correspondre cette sortie ?
- Quels sont les divers champs de cette sortie ?
- Sachant que la valeur du bloc Entry1 est ‘a’, quelle est sa valeur hash ?
- Comment peut-on savoir le type de la fonction hash utilisée pour hasher ‘a’ ?
- A entrées identiques est ce que la sortie Output d’Algorithm14 peut changer à chaque exécution ?