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. Générateur de Mots de Passes

a) Enumérer quatre caractéristiques de bons mots de passes ?
b) On désire utiliser un générateur de nombre aléatoires comme noyau de générateurs de mots de passe aléatoires mais de taille fixe qui seront distribués aux utilisateurs ; en tenant compte des réponses du point a et de la taille paramétrable de la sortie du générateur de nombres aléatoires décrire les traitements à effectuer sur les nombres aléatoires
Utiliser n= taille du mot de passe, r_i la valeur de l'octet du nombre aléatoire à l'indice i, p_i la valeur du caractère du mot de passe à l'indice i

2. Interprétation PKCS1

On utilise le RSA pour une taille de clé x, et l'un des algorithmes hash suivants :
SHA256, SHA384 et SHA512. Le mode utilisé est le PKCS1V1.5

La zone PKCS1 avant l'application de l'exponentiation modulo est la 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 00 30 51 30
0D 06 09 60 86 48 01 65 03 04 02 03 05 00 04 40
1F 40 FC 92 DA 24 16 94 75 09 79 EE 6C F5 82 F2
D5 D7 D2 8E 18 33 5D E0 5A BC 54 D0 56 0E 0F 53
02 86 0C 65 2B F0 8D 56 02 52 AA 5E 74 21 05 46
F3 69 FB BB CE 8C 12 CF C7 95 7B 26 52 FE 9A 75
```

a) Quelle est la taille de la clé RSA utilisée ?
b) Quelle clé est utilisée pour l'exponentiation modulo. Justifier.
c) Décrire les diverses zones et leurs valeurs.
d) Comment connaître l'algorithme hash utilisé sans connaître l'oid?

3. Mesures de Temps RSA

Les temps d'exécution signature RSA T1 et T2 ont été réalisés sur plusieurs machines(M1, M2, …M8) pour deux clés différentes C1 et C2 de tailles respectives 1024 bits et 2048 bits. (T1 temps pour C1 et T2 temps pour C2)

Les temps d'exécutions sont les suivants :

Machine	T1 (ms)	T2(ms)	T2/T1
M1	13	105	
M2	20	155	
M3	25	202	
M4	15	120	
M5	22	178	
M6	18	137	
M7	10	70	
M8	5	25	

a) Quel doit être le rapport théorique T2/T1 et pourquoi ?
b) Compléter sur votre copie les rapports T2/T1
c) Pour M8 que le rapport T2/T1 est très éloigné du rapport théorique. Quel phénomène peut expliquer cette différence.
d) Donner une valeur numérique du phénomène constaté en c.

4. Chiffrement Homomorphique

a) Quelle est le concept d'un chiffrement homomorphique ?
b) On appelle un chiffrement homomorphique complet s'il l'est pour les opérations + (addition) et * (multiplication) . Il est dit partiel s'il l'est pour une des deux opérations. Démontrer que le RSA est partiellement homomorphique pour la multiplication entre deux messages chiffrés.

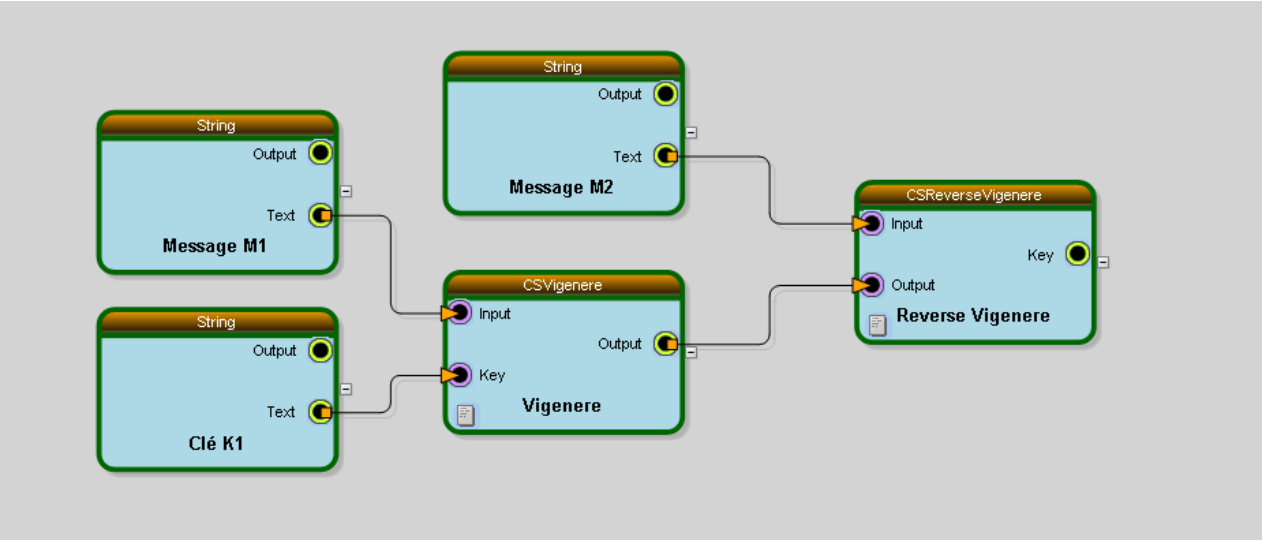
5. **Vigenère et Facebook**

Dans le royaume de Wouroudistan, l'expression sur Facebook est permise mais soumise à contrôle par l'état. Le parti des utilisateurs de l'internet de Wouroudistan (PUIW) a imaginé la technique suivante :

- Mettre un message MC de critique d'une personne sans préciser de nom,
- Faire suivre le message MC de la zone chiffrée par l'algorithme de Vigenère M' d'une phrase en clair M décrivant la personne avec éventuellement son nom.

On utilisera les conventions suivantes :
$m_1m_2…m_n$ le message à chiffrer par Vigenère, mi étant les caractères du message M,
$c_1c_2…c_n$ la clé Vigenère, ci étant les caractères de la clé K,
$m'_1m'_2…m'_n$ le message chiffré, m'i étant les caractères du message chiffré M'

a) Rappeler le fonctionnement de l'algorithme de Vigénère.
b) Quelles techniques de cryptanalyse permettent d'attaquer l'algorithme Vigenère ?
c) Ecrire la relation entre mi et m'i sous la forme d'une addition avec un nombre ki modulo 26 dépendant de l'indice i. Préciser la relation qui existe entre ci et ki.
d) A partir de la formule précédente donner la valeur de ki en fonction de mi et m'i.
e) Comment on peut faire varier M tout en gardant M' constant ?
f) On va supposer que deux personnes différentes de l'état se sentent critiquées par le message MC. Comment PUIW peut ne pas être attaqué en justice pour diffamation ?
g) Est-ce que cette technique peut être utilisée avec plus que deux personnes ?
h) Pour la génération de M' le schéma suivant a été utilisé :



La trace d'exécution du diagramme est la suivante :
20140411:125406 Entering Message M1(String)
Output: ELLEESTRETROUVEEQUOILETERNITECESTLAMERALLEEAVECLESOLEIL

20140411:125407 Exiting Message M1(String) ReturnCode=0
20140411:125407 Entering Clé K1(String)
Output: PAYSJOLI
20140411:125407 Exiting Clé K1(String) ReturnCode=0
20140411:125407 Entering Vigenere(CSVigenere)
Init input Input=ELLEESTRETROUVEEQUOILETERNITECESTLAMERALLEEAVECLESOLEIL

Init input Key=PAYSJOLI
Output Output=TLJWNGEZTTPGDJPMFUMAUSEMGNGLNQPAILYENFLTAECSESNTTSMDNWW

20140411:125407 Exiting Vigenere(CSVigenere) ReturnCode=0
20140411:125407 Entering Message M2(String)
Output: DANSLERAVINJUDASCRAPAUDDRAPEDETOILESBALANCESESREMORDSXX
20140411:125407 Exiting Message M2(String) ReturnCode=0
20140411:125407 Entering Reverse Vigenere(CSReverseVigenere)
Init input Input=DANSLERAVINJUDASCRAPAUDDRAPEDETOILESBALANCESESREMORDSXX
Init input Output=TLJWNGEZTTPGDJPMFUMAUSEMGNGLNQPAILYENFLTAECSESNTTSMDNWW

Output Key=QLWECCNZYLCXJGPUDDMLUYBJPNRHKMWMAAUMMFATNCYAAAWPHEVAVZZ
20140411:125407 Exiting Reverse Vigenere(CSReverseVigenere) ReturnCode=0

- Quelle est la valeur de M' ?
- Quel est le rôle de Reverse Vigenere ?

i) Modifier le schéma pour vérifier que la clé en sortie de Reverse Vigenere peut être utilisée.
j) Est-ce que le M' peut être cryptanalysé ?et pourquoi ?
k) A partir des points j et g, modifier le schéma pour aboutir à une amélioration du système utilisé.