Nom : MARCELIN

Prénom : Dieunel

No étudiant : 12207041

Formation : 3e année de Licence Informatique

Université : Université Sorbonne Paris Nord

Composante : Institut Galilée

Cours : Cryptologie

Professeur : Ali AKHAVI

Devoir : CC2 de cryptologie

Date de soumission : 02/01/2024

Question 1

Voir le fichier python *rsadecole.py* en annexe

1- Le chiffre de $2m$ est :

$$E\big((n,\ e),\ 2m\big) = (2m)^e \ mod\, n = (2^e * m^e)\ mod\, n = (2^e \ mod\, n) * (m^e \ mod\ n)$$

Or le chiffré de m est $c = m^e \ mod\ n$, et $(a * b) mod\, n = (a\, mod\ n) * (b\ mod\ n)\ pour\ n \in \mathbb{N}^*,\ et\ a,\ b \in \mathbb{N}$

$$\boxed{\Longrightarrow E\big((n,\ e),\ 2m\big) = (2^e \ mod\ n) * c}$$

2- Oui on peut calculer le chiffre de $2m$ en fonction du chiffre de m en utilisant la même clé publique $(n,\ e)$. Le chiffre de $2m$ est proportionnel au chiffre de m , et le facteur de proportionnalité est $(2^e \ mod\, n)$

3- L'énoncé de cette partie n'est pas trop clair. On ne met aucun chiffre en relation. Je ne vois pas l'opération qu'on doit faire avec le chiffre pour déterminer l'ordre de grandeur entre $2m$ et n

4-

5-

Question 2

La fonction à sens unique avec trappe reliée à RSA est facile à calculer dans un sens mais difficile à inverser. Elle est définie comme suit :

1. Génération des clés
   - Choisir 2 entiers distincts premiers grands aléatoirement $p\, et\, q$
   - Calculer le produit $n = p * q$
   - Déterminer 2 nombres publics et prives tels que $e * d = 1\, mod\big((p-1)(q-1)\big)$
   - La clé publique est $pk = (n,\, e)$ et la clé privée est $sk = (n,\, d)$
2. Chiffrement $\big(a\, sens\, unique\, (pk,\, m)\big)$

$$E(m) = m^e\, mod(n)$$

3. Déchiffrement $\big(Fonction\, de\, trappe\, (sk,\, c)\big)$

$$D(c) = c^d\, mod(n)$$

La trappe dans ce cas est d. La fonction à sens unique avec trappe reliée à RSA est difficile à inverser dans la connaissance de d

Si e et$f$ sont premiers entre eux, alors il existe $u,\, v \in \mathbb{Z}^*$ tels que $ex + fy = 1$

Soit m un message clair, et $c_1$son chiffre avec $(n,\, e)$ et $c_2\; son\, chiffre\, avec\; (n,\, f)$

$$c_1 = m^e\, mod\, n$$

$$c_2 = m^f\, mod\, n$$

$$\Longrightarrow$$

$$m^e \equiv c_1[n]$$

$$m^f \equiv c_2[n]$$

$$\Longrightarrow$$

$$m^{ex} \equiv c_1^x[n]$$

$$m^{fy} \equiv c_2^y[n]$$

$$\Longrightarrow$$

$$m^{ex+fy} \equiv c_1^x * c_2^y[n] \text{ car}$$

$$\text{Pour tout } a,\ b,\ c,\ d \in \mathbb{N} \ et\ n \in \mathbb{N}^* \quad \begin{matrix} a \equiv b\ [n] \\ c \equiv d\ [n] \end{matrix} \implies a * c \ \equiv \ b * d\ [n]$$

$$\text{Or } ex + fy \ = 1$$

$$\implies$$

$$m \ \equiv \ \left(c_1^x * c_2^y\right)[n]$$

$$\implies il\ existe\ k \in \mathbb{Z}\ tel\ que\ m \ = \ k * n \ + \ \left(c_1^x * c_2^y\right)$$

Application

$$n = 493,\ e = 3,\ f = 5,\ c_1 = 293,\ c_2 = 421$$

En développant l'algorithme d'Euclide étendu, on trouve $3 * (2) + 5 * (-1) = 1$ d'ou $x = 2\ et\ y = -1$

$$c_1^x * c_2^y = 293^2 \ * 421^{-1}$$

Trouvons l'inverse de 421 dans $\mathbb{Z}_{493}^*$. L'inverse existe si et seulement si $421\ et\ 493$ sont premiers entre eux. Le résultat de l'algorithme d'Euclide étendu donne :

$$493(-76) + 421(89) = 1$$

Donc, ils sont premiers entre eux. Et l'inverse de 421 dans $\mathbb{Z}_{493}^*$ est 89.

$$\implies c_1^x * c_2^y = 293^2 * 421^{-1} \ = 85849 * 89 = 7640561 \ \equiv \ 47[493]$$

$$\boxed{\text{D'ou } m = k * 493 \ + 47\ pour\ k \in \mathbb{N}}$$

Pour $k = 0$, le message est 47

Comme on vient juste de le voir, l'utilisation de la fonction à sens unique avec trappe reliée à RSA n'est pas fiable. On peut retrouver un message en connaissant deux chiffrés différents avec 2 clés différentes. L'utilisation du même n dans les 2 clés rend le système vulnérable.

Nous proposerons que la clé publique soit différente de la clé privée. Il faut qu'il y ait une trappe impossible à calculer dans temps raisonnable pour déchiffrer. En dernier le chiffrement doit être probabiliste.

Question 3

Les systèmes de chiffrements symétriques utilisent des clés bien plus courtes ($256\ bits\ ou\ moins$) en comparaison aux clés asymétriques ($2048\ bits\ ou\ plus$) pour chiffrer et déchiffrer. Ce qui fait que les chiffres asymétriques sont beaucoup plus longs que le message clair d'origine. La taille du chiffre est aussi liée à la longueur de la clé. Donc on ne peut pas chiffrer des messages clairs de 32 bits en des chiffres de 32 bits avec les systèmes de chiffrement asymétriques.

Si le système asymétrique $(G - E - D)$est sémantiquement sur, alors la sécurité est assurée contre certaines attaques comme les attaques à clairs choisis. Ne pas être déterministe est un des critères pour qu'un système de chiffrement soit sémantiquement sur. Sinon le même message clair produirait exactement le même chiffré avec la même clé publique. Cela produirait potentiellement des vulnérabilités car un attaquant pourrait étudier les chiffres même s'il n'a pas le texte clair.

En fin de compte, pour garantir la sécurité sémantique, E doit être probabiliste, c'est-à-dire, E doit produire 2 chiffres différents pour le même message clair avec la même clé publique. Cela peut être réalisé en introduisant un élément aléatoire dans l'algorithme.

Question 4

Montrons que 7 est un générateur de $\mathbb{Z}_{13}^{*}$. On va montrer que $7^n\ mod\ 13$prend toutes les valeurs possibles entre 1 a 12 pour $n = \overline{1,\ 12}$

$$7^1\ mod\ 13 = 7$$

$$7^2\ mod\ 13 = 10$$

$$7^3\ mod\ 13 = 5$$

$$7^4\ mod\ 13 = 9$$

$$7^5\ mod\ 13 = 11$$

$$7^6\ mod\ 13 = 12$$

$$7^7\ mod\ 13 = 6$$

$$7^8\ mod\ 13 = 3$$

$$7^9 \; mod \; 13 = 8$$

$$7^{10} \; mod \; 13 = 4$$

$$7^{11} \; mod \; 13 = 2$$

$$7^{12} \; mod \; 13 = 1$$

D'où 7 est un générateur de $\mathbb{Z}_{13}^*$

3 est-il un générateur de$\mathbb{Z}_{13}^*$?

Nous allons vérifier si $3^n \; mod \; 13$ prend toutes les valeurs possibles entre $1 \; a \; 12$ pour $n = \overline{1, \; 12}$

$$3^1 \; mod \; 13 = 3$$

$$3^2 \; mod \; 13 = 9$$

$$3^3 \; mod \; 13 = 1$$

$$3^4 \; mod \; 13 = 3$$

La séquence ne sera pas complète car $3^1 \; mod \; 13 = 3^4 \; mod \; 13 = 3$. Donc 3 n'est pas un générateur de $\mathbb{Z}_{13}^*$.

Le logarithme discret de 10 en base 7 dans $\mathbb{Z}_{13}^*$ est l'entier x tel que $7^x \; mod \; 13 = 10$, c'est-à-dire résoudre l'équation $7^x \equiv 10[13]$.

Au début de l'exercice on avait $7^2 \; mod \; 13 = 10$. D'où 2 est le logarithme discret de 10 en base 7 dans $\mathbb{Z}_{13}^*$.

Question 5

Calculons $2^{245}\ mod\ 35$.

Nous allons calculer les puissances successives $2^k\ mod\ 35$ ($k \geq 1$) jusqu'à ce qu'on tombe sur $2^k\ mod\ 35 = 1$ ou bien sur un cycle de longueur i .

$$2^1 \equiv 2[35] \quad 2^2 \equiv 4[35] \quad 2^3 \equiv 8[35] \quad 2^4 \equiv 10[35]$$

$$2^5 \equiv 32[35] \quad 2^6 \equiv 29[35] \quad 2^7 \equiv 23[35] \quad 2^8 \equiv 11[35]$$

$$2^9 \equiv 22[35] \quad 2^{10} \equiv 9[35] \quad 2^{11} \equiv 18[35] \quad 2^{12} \equiv 1[35]$$

Or $245 = 20 * 12 + 5$

$$\Longrightarrow 2^{245} = 2^{(20*12+5)} = 2^{(12)*20} * 2^5 \equiv 1 * 2^5[35]$$

$$\Longrightarrow 2^{245} \equiv 32[35]$$

Car pour tout $a,\ b,\ c,\ d \in \mathbb{N}\ et\ n \in \mathbb{N}^*$ $\begin{matrix} a \equiv b[n] \\ c \equiv d[n] \end{matrix} \Longrightarrow a * c \equiv b * d \equiv [n]$

Au final,

$$\boxed{2^{245}\ mod\ 35 = 32}$$

Les autres questions ont été déjà répondues dans la partie 4 du devoir.