Matière :	Niveau :	Examen :
Sécurité Avancée des Systèmes Informatiques	2ème Année Master AD	Session normale
Documents non autorisés	Durée : 01h 30mn	Calculatrice scientifique autorisée.

Mercredi 18/01/2023

Répondre clairement et brièvement

Exercice 1 : 08 pts (Système RSA)

Ali utilise un système RSA avec $p = 37$ et $q = 43$.

1) Calculez les valeurs de n le module RSA et de $\varphi(n)$ l'indicatrice d'Euler ?
2) Quelle est la plus grande valeur de l'exposant de chiffrement **e** utilisable tel que **e** ≤ 10 ? Justifiez votre réponse.
3) Quelle est la valeur de la clé publique et de la clé privée d'Ali ?
4) Omar veut envoyer le message $m = 20$ à Ali sous forme chiffrée c.
   (a) Quel est la valeur de c ?
   (b) Quels sont les objectifs de sécurité atteints dans ce cas ?
5) Quel est le message clair m correspondant au cryptogramme $c = 23$ envoyé par Omar à Ali ?
   Omar possède la clé publique $(n_{\text{Omar}}, e_{\text{Omar}})$ et la clé privée $(n_{\text{Omar}}, d_{\text{Omar}})$. Il informe Ali qu'il va lui envoyer des messages m sous forme chiffrés c comme suit : $c = y^e \mod n$ tel que $y = m^{d_{\text{Omar}}} \mod n_{\text{Omar}}$.
6) Quels sont les objectifs de sécurité atteints dans ce cas ?

Remarque : $\forall m \in \mathbb{Z}_n - \{0\}, m^{253} \equiv m \mod n$. Si $PGCD(m, n) = 1$ alors $m^{252} \equiv 1 \mod n$.

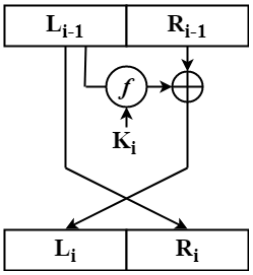
Exercice 2 : 06 pts (Système ElGamal)

Soit le système ElGamal avec $p = 37$, g et une clé privée $x = 17$. Tel que g est le plus petit générateur du groupe multiplicatif cyclique $\mathbb{Z}_{37}^{\times}$.

1) Donnez la valeur de g ?
2) Quelle est la clé publique dans ce cas ?
3) Chiffrez message clair $m = 27$ en utilisant la valeur aléatoire $k = 29$?
4) Déchiffrez le cryptogramme $c = (21, 33)$?

Exercice 3 : 06 pts (Schéma de Feistel)

Considérons le schéma de Feistel modifié illustré par la figure ci-contre.



1) Donnez les formules permettant le chiffrement d'un bloc clair ?
2) Donnez les formules permettant le déchiffrement d'un bloc chiffré ?

Si $f_k(x) = \overline{x \oplus k}$ (par exemple $k = 1001$ et $x = 1011$, alors $f_k(x) = \overline{1011 \oplus 1001} = \overline{0010} = 1101$) :

3) Donnez le résultat de chiffrement du bloc $m = (5AEC)_{16}$ et $k = (84)_{16}$?
4) Donnez le résultat de déchiffrement du bloc $c = (D27B)_{16}$ et $k = (E6)_{16}$?

Bon courage