REPONSES DE CRYPTO - QCM 2019

(Si vous voyez une erreur, n'hésitez pas à le faire remonter)

Questions	Réponse
n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé secrète. Combien de clés doivent être générées ?	$n(n-1)/2$
n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé publique. Combien de clés doivent être générées ?	2n
Un système est considéré comme sûr si la meilleure attaque connue nécessite au moins 2^{128} opérations élémentaires. Si le meilleur algorithme pour factoriser des entiers de taille n a pour complexité $2^{\sqrt[3]{n}}$, quelle est la valeur de n qui permet à un système cryptographique reposant sur la difficulté de la factorisation d'être sûr ?	2097152
Quelle est le chiffré du message m=10110101 par le chiffrement de Vernam en utilisant la clé k=01011101, sachant que le chiffrement se fait par un ou exclusif bit à bit entre la clé et le message ?	11101000
Quel est le message clair dont le chiffré est c = 00010010 en utilisant le chiffrement de Vernam avec comme clé k = 01011101 ?	01001111
Soient a, b et c trois entier et considérons l'algorithme A suivant. **A(a,b,c) :** **R = 1** **Pour i = 1 à b faire :** **R = R * a** **r = R [c]** **Retourner r**	A peut être utilisé dans le déchiffrement RSA
Quelles propriétés sont assurées par la signature ?	Intégrité et authenticité
Dans un algorithme de chiffrement à clé publique, quelle est la clé utilisée pour chiffrer ?	La clé publique

Que représente un certificat numérique ?	Un moyen de garantir la relation univoque entre une clef publique et son véritable propriétaire
Quelle complexité est la plus proche de celle de la meilleure méthode de factorisation ?	2^(n^(1/3)) (mais je ne suis pas sûr.e)
Combien y a-t-il d'éléments inversibles modulo 21 ?	12
Parmi ces problèmes, quel est celui qui est « facile » ?	Résoudre $X^2 = 3$ [p] avec p premier
A quoi peur servir le théorème des restes chinois ?	Accélérer le déchiffrement RSA
Si N = 77 que vaut $\varphi(N)$?	60
A quoi sert l'algorithme d'Euclide étendu ?	Il est utilisé pour calculer un inverse modulaire