Nom :
Prénom :
Numéro étudiant :

Questions	Réponses
n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé *secrète*. Combien de clés doivent être générées?	☐ $n!$ ☐ $n(n-1)/2$ ☐ 2^n ☐ $\sqrt{n}$
n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé *publique*. Combien de clés doivent être générées?	☐ $2n$ ☐ $2^{n/2}$ ☐ $n!$ ☐ $\sqrt{n}$
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 $2^{n^{1/3}}$, quelle est la valeur de n qui permet à un système cryptographique reposant sur la difficulté de la factorisation d'être sûr?	☐ 128 ☐ 384 ☐ 2097152 ☐ 2048
Quel 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?	☐ 00010101 ☐ 00000000 ☐ 11101000 ☐ 10010101
Quel est le message clair dont le chiffré est $c = 00010010$ en utilisant le chiffrement de Vernam avec comme clé $k = 01011101$	☐ 00010000 ☐ 01001111 ☐ 10101010 ☐ 10101001
Soit a, b, c trois entiers et considérons l'algorithme A suivant. A(a,b,c) : R = 1 Pour i = 1 à b faire R = R × a r = R (mod c) Retourner r	☐ A peut être utilisé dans le déchiffrement RSA ☐ A calcule $a^c \mod b$ ☐ A est efficace ☐ A a une complexité exponentielle en la taille des entrées
Quelles propriétés sont assurées par la signature?	☐ confidentialité et intégrité ☐ intégrité et authenticité ☐ authenticité et confidentialité ☐ confidentialité, intégrité et authenticité

Questions	Réponses
Dans un algorithme de chiffrement à clé publique, quelle est la clé utilisée pour chiffrer?	☐ la clé publique ☐ la clé secrète ☐ les deux ☐ aucune
Que représente un certificat numérique?	☐ Un moyen d'assurer la non-répudiation du message transmis ☐ Un moyen de garantir la relation univoque entre une clef publique et son véritable propriétaire ☐ Une garantie donnée sur l'intégrité du message transmis ☐ Un moyen pour chiffrer la clé secrète sur le disque dur
Quelle complexité est la plus proche de celle de la meilleure méthode de factorisation?	☐ 2^n ☐ $2^{n/4}$ ☐ $2^{n^{1/3}}$ ☐ n^8
Combien y a-t-il d'éléments inversibles modulo 21?	☐ 20 ☐ 12 ☐ 1 ☐ 8
Parmi ces problèmes, quel est celui qui est « facile »?	☐ Résoudre $X^2 = 3 \mod p$ avec p premier ☐ Factoriser $N = p \times q$, avec p et q premiers ☐ Calculer un logarithme discret modulo p ☐ Aucun n'est facile
À quoi peut servir le théorème des restes chinois?	☐ Accélérer le chiffrement RSA ☐ Accélérer le déchiffrement RSA ☐ Accélérer la génération des clés RSA ☐ Il ne sert qu'à attaquer RSA
Si $N = 77$, que vaut $\varphi(N)$?	☐ 1 ☐ 6 ☐ 10 ☐ 60
À quoi sert l'algorithme d'Euclide étendu?	☐ Il permet de factoriser les grands entiers ☐ Il est utiliser pour calculer un inverse modulaire ☐ Il permet de tester la primalité des entiers ☐ Il ne sert à aucune de ces propositions