

L'ANSSI considère que jusqu'en 2020, un système est sûr si la meilleure attaque connue nécessite au moins 2^{100} opérations élémentaires pour réussir. 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 assure qu'RSA est sûr ?

☐ 2048

☐ 200

☐ 100

☐ 1000000

Lors d'une authentification par mot de passe sur un serveur, celui-ci :

- ☐ stocke les mots de passe en clair
- ☐ stocke les mots de passe chiffrés
- ☐ stocke les hachés des mots de passe chiffrés avec la clé publique de l'utilisateur
- ☐ stocke des hachés des mots de passe

Il reste 0 heure 58 minutes 31 secondes avant la fin de l'épreuve.

n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé secrète. Combien de clés doivent être générées ?

☐ $n!$

☐ 2^n

☒ $n(n-1)/2$

☐ \sqrt{n}

Soit a, b, c , trois entiers et considérons l'algorithme A suivant :

A(a, b, c)

R=1

Pour $i = 1$ à b faire

$R = R * a$

$r = R \% c$

Retourner r

-
- ☐ A calcule $a^c \bmod b$
 - ☐ A peut être utilisé pour un déchiffrement RSA rapide
 - ☐ A a une complexité exponentielle en la taille des entrées
 - ☐ A calcule $b^a \bmod c$

La sécurité du chiffrement Elgamal :

- ☐ repose sur la difficulté de factoriser des entiers
- ☐ repose sur la difficulté de calculer des logarithmes discrets
- ☐ est faible
- ☐ repose sur la difficulté de calculer des exponentiations modulaires

Que représente un certificat numérique ?

- ☐ Un moyen d'assurer la non-répudiation du message transmis
- ☐ Une garantie donnée sur l'intégrité du message transmis
- ☐ Un moyen de garantir la relation univoque entre une clef publique et son véritable propriétaire
- ☐ Un moyen pour chiffrer la clé secrète sur le disque dur

Combien y a-t-il d'éléments inversibles modulo 35 ?

☒ 24

☐ 12

☐ 1

☐ 34

Si $N = 35$, combien vaut $\varphi(N)$?

☒ 24

☐ 6

☐ 34

☐ 1

Le théorème des restes chinois permet

- ☐ d'accélérer le chiffrement car on peut travailler avec des entiers plus petits
- ☐ d'accélérer le déchiffrement car les calculs modulo p ou modulo q sont 4 fois plus rapides que modulo N
- ☐ d'accélérer le déchiffrement car l'exponentiation modulaire modulo p ou q est 8 fois plus rapide que modulo N
- ☐ d'accélérer le chiffrement car e modulo $p-1$ et $q-1$ est plus petit que modulo $\varphi(N)$

Les deux derniers chiffres de $3^{10^{10}}$ sont

☐ 13

☐ 99

☐ 01

☒ 27

Il reste 0 heure 54 minutes 57 secondes avant la fin de l'épreuve.

Dans le chiffrement RSA, si un utilisateur possède une clé publique $pk_1 = (e_1, N)$ et la clé secrète associée, et un autre utilisateur possède la clé publique $pk_2 = (e_2, N)$ avec la clé secrète associée, où $e_1 \neq e_2$ mais le module est le même:

- ☐ ça peut-être dangereux si d_1 ou d_2 (les exposants secrets) sont trop petits
- ☒ c'est dangereux, ils peuvent en déduire la clé secrète de l'autre
- ☐ il n'y a pas de danger
- ☐ ça peut être dangereux si e_1 et e_2 sont trop petits

Il reste 0 heure 34 minutes 55 secondes avant la fin de l'épreuve.

Si $N = p \times q \times r$ a une taille de ℓ bits, et que p, q, r ont le même nombre de bits

☐ p, q, r ont moitié moins de bits que N

☐ p, q, r font $\ell/3$ bits chacun

☒ p, q, r ont $\ell^{1/3}$ bits

☐ p, q, r ont $\sqrt{\ell}$ bits

Il reste 0 heure 34 minutes 10 secondes avant la fin de l'épreuve.

Soit G un groupe fini cyclique engendré par g .

Si on connaît g, g^a, g^b , pour des entiers a et b

☒ il est difficile de calculer g^{ab}

☐ il est difficile de calculer g^{a+b}

☐ il est facile de calculer a et b

☐ il est difficile de calculer g^{a-b}

On considère le protocole d'échange de clé suivant :

- 1) Alice tire deux suites binaires k et r aléatoires de longueur n . Elle envoie à Bob $s = k \oplus r$
- 2) Bob tire aléatoirement une suite binaire t de longueur n et envoie $u = s \oplus t$ à Alice
- 3) Alice calcule $w = u \oplus r$ qu'elle envoie à Bob et la clé partagée est k

-
- ☐ Le protocole est trop lent
 - ☐ Bob ne peut pas calculer la clé k
 - ☐ Bob peut calculer aussi la clé k
 - ☐ Le protocole est sûr

Quand parle-t-on d'attaque par force brute en cryptographie ?

- ☐ Lorsqu'on force physiquement un utilisateur à dévoiler son mot de passe
- ☐ Lorsque le message est modifié avant l'envoi
- ☒ Lorsqu'on parcourt de façon exhaustive l'espace des clés secrètes
- ☐ Lorsqu'un utilisateur essaie de se faire passer pour un autre