L'AN élén	NSSI considère que jusqu'en 2020, un système est sûr si la meilleure attaque connue nécessite au moins 2^{100} opérations nentaires pour réussir. Si le meilleur algorithme pour factoriser des entiers de taille n a pour complexité $2^{n^{1/3}}$, quelle est aleur de n qui assure qu'RSA est sûr ?
0	2048
0	200
0	100
0	1000000

Page 3 (1/17)	
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	
o 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.

Page 4 (5/17)

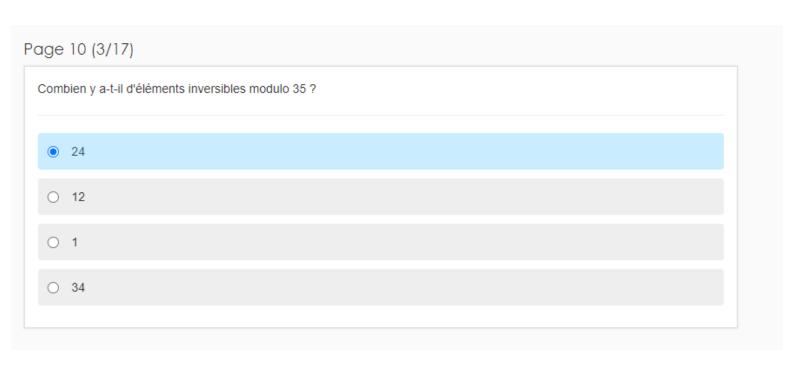
n utilisateurs souhaitent communiquer 2 à 2 de façon confidentielle grâce à la cryptographie à clé secrète. Combien de clés doivent être générées ?

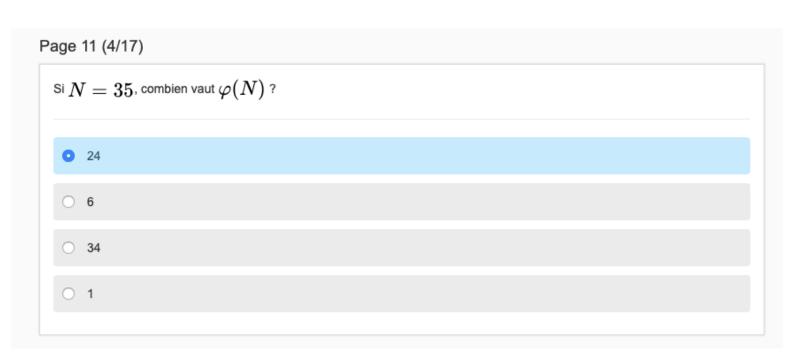
- \circ n!
- \circ 2^n
- ullet n(n-1)/2
- \circ \sqrt{n}

Page 5 (5/17) 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 rA calcule $a^c \mod b$ A peut être utilisé pour un déchiffrement RSA rapide A a une complexité exponentielle en la taille des entrées A calcule $b^a \mod c$

Page 7 (9/17) La sécurité du chiffrement Elgamal : orepose 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

Page 9 (4/17) 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





_	e 13 (3/17) héorème des restes chinois permet
0	d'accélérer le chiffrement car on peut travailler avec des entiers plus petits
0	d'accélérer le déchiffrement car les calculs modulo p ou modulo q sont 4 fois plus rapides que modulo N
0	d'accélérer le déchiffrement car l'exponentiation modulaire modulo p ou q est 8 fois plus rapide que modulo N
0	d'accélérer le chiffrement car e modulo p-1 et q-1 est plus petit que modulo $arphi(N)$

Page 15 (2/17)

Les deux derniers chiffres de $3^{10^{10}}$ sont				
0	13			
0	99			
0	01			
•	21			
0	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:

- $\, \bigcirc \,$ 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
- O il n'y a pas de danger
- \bigcirc 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 imes q imes r a une taille de ℓ bits, et que p,q,r ont le même nombre de bits

- $\ \bigcirc \ p,q,r$ font $\ell/3$ bits chacun
- ullet p,q,r ont $\ell^{1/3}$ bits
- $\ \circ \ p,q,r$ ont $\sqrt{\ell}$ bits

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

Page 18 (2/17) Soit G un groupe fini cyclique engendré par g. Si on connaît g, g^a , g^b , pour des entiers a et bIl est difficile de calculer g^{ab} Il est difficile de calculer g^{a+b} Il est facile de calculer a et bIl est difficile de calculer a et b

Page 19 (2/17) 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 kLe protocole est trop lent Bob ne peut pas calculer la clé kBob peut calculer aussi la clé kLe protocole est sûr

Page 20 (3/17) 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