# Correction de Cryptographie du QCM 2020

- **2** : 1000000
- **3** : stocke des hachés des mots de passe
- **4** : n(n-1)/2
- **5** : A a une complexité exponentielle en la taille des entrées
- **7** : Repose sur la difficulté de calculer des logarithmes discrets
- **9** : Un moyen de garantir la relation univoque entre une clef publique et son véritable propriétaire
- **10** : 24
- **11** : 24
- **13** : d'accélerer le déchiffrement car l'exponentiation modulaire modulo p ou q est 8 foi splus rapide que modulo N
- **15** : 01
- **16** : C'est dangereux, ils peuvent en déduire la clé secrète de l'autre
- **17** : p, q, r ont `L^1/3` bits
- **18** : il est difficile de calculer `g^ab`
- **19** : Bob ne peut pas calculer la clé `k`
- **20** : Lorsqu'on parcourt de façon exhaustive l'espace des clés secrètes

## Réponses n'ayant pas la question disponible

- **1** : 2n
- **6** : confidentialité
- **8** : clef secrete
- **12** : Inverse modulaire
- **14** : les blocs de clairs identiques ont des chiffrés identiques