|  |  |
| --- | --- |
| C:\Users\luciefortin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\LogoDICJ.PNG**Évaluation 1** |  |
| ***Exploration technologique*** | |

Nom :

Consignes

* Vous n'avez pas droit à votre voisin et au professeur pour cet examen.
* L’évaluation vaut 15% de la note finale.
* L’examen doit être remis à la fin du cours.
* La matière couverte comprend les semaines 1-3 et 6 inclusivement.
* Vous répondez directement dans le document sur Team's pour les questions 1 à 6 et 8 – 9.

Cryptographie

**Q01 : Combien y avait-il de combinaisons possibles pour la clef brute du message dans la machine Enigma ? (2 pts)**

**Q02 : Quel est la plus grande problématique liée à l'utilisation des clés symétriques ? (2 pts)**

**Q03 : Quel sont les éléments qui composent la cryptographie ? (2 pts)**

**Q04 : Qu'est-ce que le chiffrement polygraphique ? (2 pts)**

**Q05 : Quel est le plus grand risque que l'on court avec l'algorithme de chiffrement RSA (ne répondez pas l'ordinateur quantique) ? (2 pts)**

**Q06 : En quoi consiste le hachage cryptographique ? (5 pts)**

Chiffrement

**Q07 : Modifiez l'application AppChiffrement (téléchargés AppChiffrement.zip) afin de simuler deux utilisateurs qui s'échangent des messages cryptés. Votre application doit simuler l'échange de message avec clé publique et avec clé privée. L'envoyeur écrit un message dans la zone de texte de son formulaire, l'encrypte et l'envoie. Le destinataire reçoit le message crypté et le décrypte à l'aide de la clé publique ou de la clé privée. Vous avez analysé le fonctionnement de l'application à la semaine 3, donc vous connaissez son fonctionnement. Vous remettrez le répertoire compressé de votre application sur Team's. Des images exemples sont disponibles sur Team's. (25 pts)**

Protocoles réseau

**Q08 : Quelle est la différence entre les protocoles HTTPS – SSH - TLS. (5 pts)**

**Q09 : Qu'est-ce qu'un certificat de sécurité ? (5 pts)**