1 Consignes

Vous devez faire une présentation de 30 minutes par personne sur un des sujets. La présentation doit être compréhensible par tous les élèves, les éléments de cryptographie vu en cours peuvent être supposés connus mais pas des éléments spécifiques au sujet. Les présentations auront lieu le 7 et le 14 décembre, le planning sera fait en fonction des sujets.
La notation est individuelle, chacun sera évalué sur la partie qu'il présentera, à vous de répartir de manière équilibrée. Les principaux éléments de notations seront : Le sujet est-il correctement couvert ? Pas de faits importants laissés de côté, pertinence de ce qui est présenté..., niveau de la présentation : la présentation est-elle compréhensible sans être simpliste, justesse scientifique ,pédagogie et clarté de la présentation.

2 Sujets

Vous pouvez travailler sur un des sujets proposés ou un de votre choix (à faire valider).

- **Encryption AES et DES** : 2 personnes
  Cryptographie symétrique, ancien et actuel standard.
- **Analyse linéaire et différentielle** : 2 personnes
  Cryptanalyse, méthode d'attaque
- **Fonctions et générateurs pseudo-aléatoires (PRF,PRG)** : 2 personnes
  Utilité et création d'aléatoire dans les protocoles cryptographiques
- **Cryptographie post-quantique** : 1 ou 2 personnes
  Comment faire de la cryptographie dans un monde avec des ordinateurs quantiques
- **Identity based encryption** : 1 ou 2 personnes
  Étude d'un schéma cryptographique.
- **Utilisations des réseaux (lattices) en cryptographie** : 1 ou 2 personnes
  Utilisation d'un objet mathématique pour la cryptographie.
- **Encryption homomorphe** : 1 personne
  Comment faire du calcul sur des données chiffrées ?
- **Preuves à divulgation nulle de connaissance** : 1 personne
  Comment prouver que l'on connaît une information sans donner cette information ?
- **Protocole d'échange de clef Diffie-Hellman et Attaque "man in the middle"** : 1 personne
  Protocole classique d'échange de clef et une attaque.