1. ***Logarithme discret et courbes elliptiques***
   * **Logarithme discret sur :** Introduction puis extension à un groupe quelconque
   * **Courbe elliptique sur un corps** .
   * **Structure de groupe de**  :
     + Point de vue géométrique de la loi (avec )
     + Point de vue algébrique
   * **Logarithme discret sur**  :
   * **Programmation** : langage, méthode, choix…
2. ***ECC : Elliptic Curve Cryptography***
   * Transmission de message en cryptographie :
     + Principe général : clé publique et privée (cf [Diffie-Hellman](https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman))
     + Principe détaillé pour des courbes elliptiques (cf [Elliptic Curve Diffie Hellman](https://youtu.be/F3zzNa42-tQ?t=709))
   * Implémentation de la transmission :
     + Algorithme *'Double and add'* (*Addition et doublement*) pour calculer en
     + Traduction du message en un point de 🡪 ???
     + Décryptage du message par le récepteur
   * Interception du message :
     + « Brute Force »
     + Algorithme de décryptage plus efficace : …
3. ***Application à un cas concret :***
   * Valeur des paramètres : p, a, b
   * Choix du message
   * Algorithme de hash (SHA-1, SHA-256, MD5, CRC32…)
   * Comparaison des différents algos de d’interception du message
4. ***Autres :***
   * Signature du message pour assurer l’intégrité de la transmission
   * ECDSA : *Elliptic curve digital signature algorithm*, algorithme de signature électronique à clé publique utilisé par certaines cryptomonnaies (Bitcoin, Ethereum) (cf [ECDSA](https://fr.wikipedia.org/wiki/Elliptic_curve_digital_signature_algorithm))