Sécurité et réseaux

Contrôle modalités

2 notes projets (une présenation) + controle final.

Déroulement

Proposer 12 sujets qui seront étudiés par des groupes de 5. 1ere note : contenu exposé, **vulgarisation** 2eme : libérer imaginatio, perspectives, comment cette technologie peut être utilisée ? Proposer un produit disruptif, argumenter. Business developper mes couilles, concept, blahblahblah. un peu de science fiction → (black mirror ?) 20 min strict présentation (à 5 ça fait pas bcp)

Les supers sujets

- Le Quantique
- Deep Learning
- Cloud computing
- Domotique
- Crypto-Monnaies
- IoT
- Deep Web
- Biométrie
- Réalité augmentée
- Machine Learning
- Voitures autonimes
- Hacking
- Emulation
- Big Data
- Serious Gaming
- Dark Web
- Intégration logicielle
- E-commerce
- Informatique “écologique”
- Information et “vie privée”
- Numérisation : vers la dématérialisation
- Virtualisation

Cryptographie et crytanalyse

Steganogaphie

Naissance d'une méthode de crypto : utilisation de **clés**

P → [Cryptage] → [cryptogramme] → [Décryptage] → P texte en clair | clée de cryptage k | C = Ek(P) | clé k | texte en clair

Ici : Espion passif lit le message, l'actif le modifie également

Problème de la cryptanalyse

- textes chiffrés uniquement
- textes en clair connus
- textes en chair **choisis**

Méthodes traditionnelles

Par substitution ou par transposition

Substitution mono-alphabétique

s : symboles en clair s' : " chiffrés

f: s→s'

On joue sur la fréquence d'apparition de lettres, de digrammes, trigrammes

Substitution poly-alphabétique

f:s postition → s'

Code de Vigenève