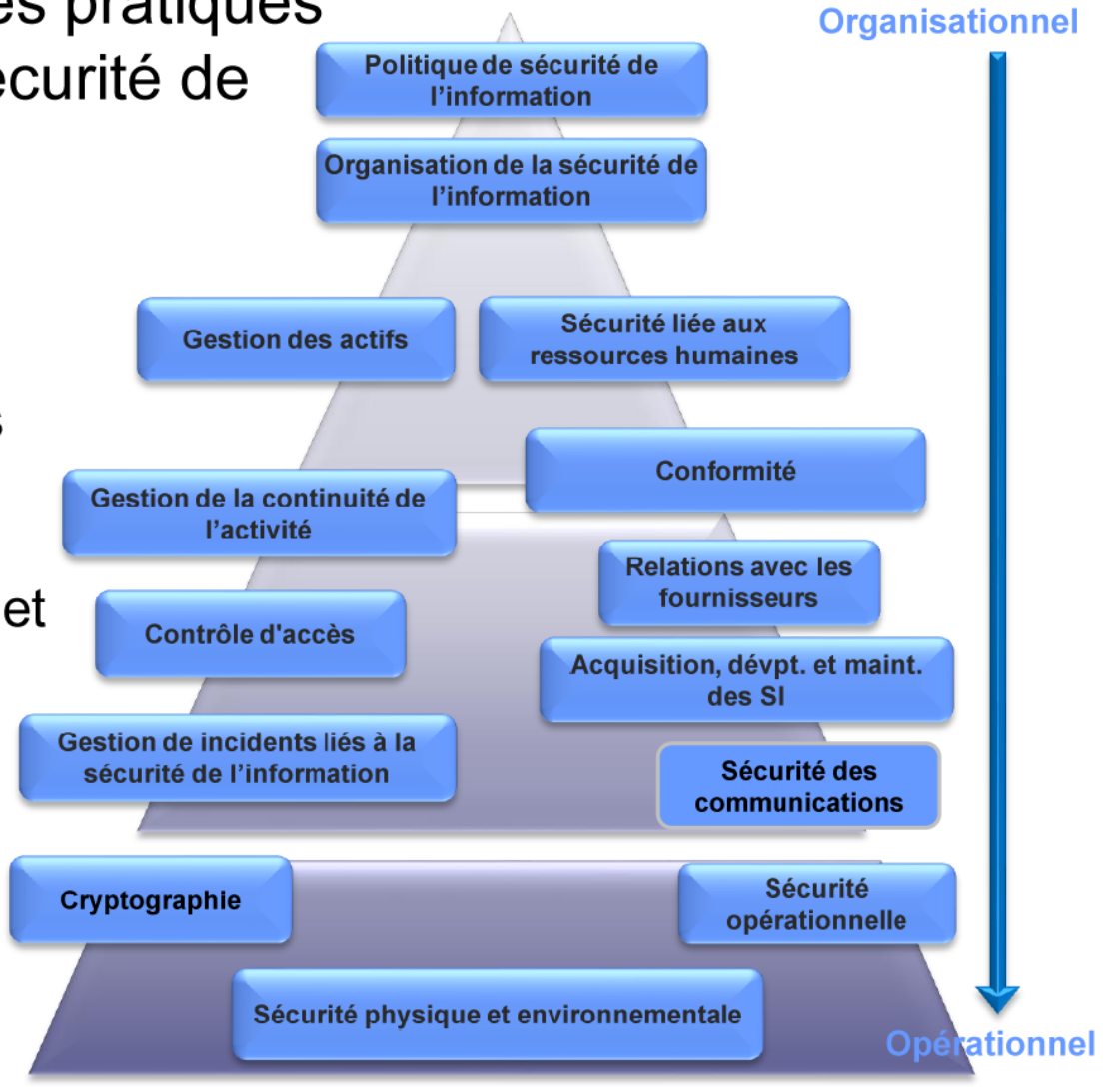
Normes ISO 27000

- 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information

- Approche globale de la sécurité des S.I.
- Composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques
- Référentiel de mise en œuvre
  - « Check-list » en cas d'audit



Normes ISO 27000

- 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information
- Exemples de mesures du chapitre « Contrôle d'accès »
  - L'accès aux fichiers/répertoires doit être restreint conformément aux politiques de contrôle d'accès
    - Seuls les professeurs autorisés doivent pouvoir accéder à un répertoire contenant les épreuves des futurs examens/concours
  - Les propriétaires de l'information doivent vérifier les droits d'accès à intervalles réguliers
    - Le responsable des concours doit contrôler les droits d'accès au répertoire contenant les épreuves des futurs examens/concours pour s'assurer qu'il n'y a pas d'étudiants qui auraient été rajoutés
- Exemple de mesures du chapitre « Sécurité opérationnelle »
  - L'installation et la configuration de logiciels doivent être encadrés
    - Seuls les administrateurs doivent pouvoir installés un logiciel sur un poste
  - Des sauvegardes doivent êtres régulièrement effectuées et testées
    - Un espace de sauvegarde des données peut être mis à disposition des utilisateurs

Normes ISO 27000

- 27005 : Gestion des risques
- La norme 27005 présente une démarche
  - Donne les lignes directrices relatives à la gestion des risques de sécurité
- Avantages
  - Utilisable seule
  - Plusieurs méthodes sont compatibles IS0 27005
    - Exemple : EBIOS RM
  - Méthode générique, peut être utilisée en toutes circonstances
- Limites
  - C'est plus une démarche qu'une vraie méthode
    - L'organisation doit définir sa propre approche
  - Tendance à l'exhaustivité
  - Accumulation de mesures techniques sans cohérence d'ensemble

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

À la prochaine séance

Nora Cuppens

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420a: Sécurité Informatique
Cryptographie I

Frédéric Cuppens

Nora Cuppens & José Fernandez

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Aperçu du module – Cryptographie

- Définitions et histoire
- Notions de base (théorie de l'information)
- Chiffrement
  - Méthodes « classiques »
  - Chiffrement symétrique
  - Chiffrement à clé publique
- Cryptanalyse de base
- Autres primitives cryptographiques
  - Hachage cryptographique
  - Signature numérique
  - Infrastructure à clé publique (ICP)
- Principes d'applications de la cryptographie
- Risques résiduels d'applications de la cryptographie

Cryptographie I (aujourd'hui)

- Définition et nomenclature
- Historique
- Théorie de l'information
  - Modèle de Shannon
    - Source d'information
    - Codage et compression
  - Entropie
- Chiffrement
  - Chiffrement et codage
  - Algorithmes « classiques »
- Cryptanalyse de base
  - Force brute
  - Reconnaissance de texte
  - Analyse de fréquences

CRYPTOGRAPHIE I – INTRODUCTION ET HISTOIRE

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

Définitions et terminologie

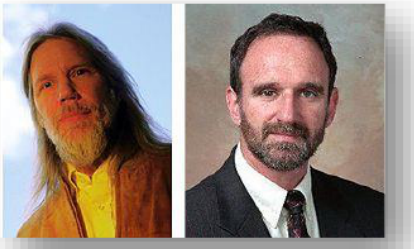
- Un peu de grec classique…
  - Kryptos = « caché », « secret »
  - Graphos = écriture
  - ⇒ Cryptographie
  - ⇒ Cryptanalyse
  - Logos = « savoir »
  - ⇒ Cryptologie
  - Stéganos = « couvert », « étanche »
  - ⇒ Stéganographie
- Un peu d'américain…
  - Alice
  - Bob
  - Ève
  - (Charlie)
  - Encrypt and Decrypt
- Un peu de français
  - Chiffrer et déchiffrer
  - Coder et décoder
  - Crypter et décrypter (!)
  - Irène !!! (l'ingénieure)
- Un peu de math…

Historique

- Les trois ères de la cryptographie
  - « Classique »
    - Jusqu'au masque jetable (chiffre de Vernam)
    - Chiffrement manuel ➔ chiffrement faible
  - « Moderne »
    - Crypto électro-mécanique et WWII (voir applet Enigma)
    - Guerre froide …
    - Crypto électronique et informatique – DES
    - Chiffrement par machines spécialisées ➔ chiffrement plus complexes
    - Réservés aux organisations pouvant acquérir l'équipement

Historique

- Les trois ères de la cryptographie (suite)
  - « Âge d'or »
    - Cryptographie à clé publique
    - 1976 - Whitfield Diffie & Martin Hellman
      - Introduise la notion de **cryptographie à clé publique**
      - Algorithme d'échange de clé (DH)
      - Introduise la notion de **signature numérique**
    - 1978 - Ronald Rivest, Adi Shamir, Leonard Adleman
      - Premier algorithme à clé publique (RSA)
    - 1973 – Clifford Cocks
      - Invente en parallèle un algorithme équivalent à RSA au sein du GCHQ
      - L'algorithme est classifié « TOP SECRET »
      - Existence dévoilée seulement en 1997



Historique

- Les trois ères de la cryptographie (suite)
  - « Âge d'or » (suite)
    - « Démocratisation » de la cryptographie
      - Années 80

        Cryptographie sur PC (PGP = Pretty Good Privacy))
      - Années 90 et 00

        Levée des restrictions d'exportations de cryptographie

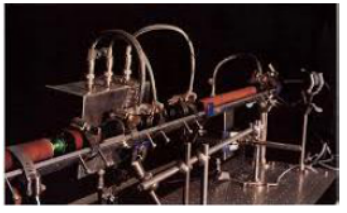
        Internet et Web
        - Protocoles réseaux sécurisés : SSH, SSL/TLS, IPSEC, etc.

        Infrastructures à clé publique et signature numérique
        - Transactions commerciales (bancaire et parabancaires)
        - Identité numérique
        - Cryptomonnaie
        - …

Historique

- Les trois ères de la cryptographie (suite)
  - Apocalypse « imminent » et ère post-quantique
    - 1984 – Charles Bennett et Gilles Brassard
      - Invention de la cryptographie quantique –
        - base sa sécurité sur les propriétés de la mécanique quantique

    - 1994 – Peter Shor (suivant les travaux de Dan Simon)
      - Découverte de la cryptanalyse quantique
        - Casse tous les algorithmes à clé publique connus
        - Nécessite d'un ordinateur quantique…

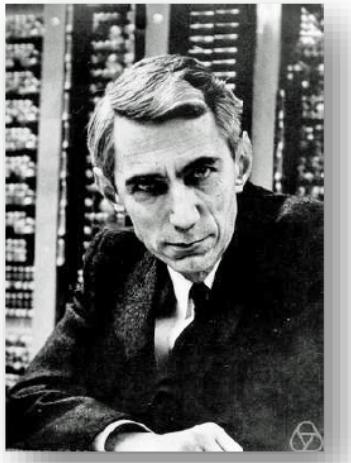


    - Années 10
      - Proposition d'algorithmes à clé publique « post quantiques »
        - Semblent résister à la cryptanalyse quantique
        - Peu pratiques à utiliser
        - Pas (encore) de standard établi
        - Adoption très lente…

CRYPTOGRAPHIE I – THÉORIE DE L'INFORMATION – MODÈLE DE SHANNON

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Claude Shannon



- IIe guerre mondiale
  - Contribue aux efforts de cryptanalyse de guerre
- Père de la Théorie de l'information
  - 1948 – « A Mathematical Theory of Information »
- Fondement théorique de la cryptographie
  - 1945 – « A Mathematical Theory of Cryptography »
    - Classifié – basée sur ses travaux de cryptanalyse
  - 1949 – « Communication Theory of Secrecy Systems »
    - Version non-classifiée, publié dans Bell Technical Journal

Claude Shannon

- Contributions
  - Introduit une définition mathématique de l'information
    - Source d'information
    - Modèle de Shannon – transmission d'information
  - Introduit la notion d'entropie (dans le contexte de l'information)
    - Définit le **bit** comme unité de mesure de l'information
    - Établit les limites fondamentales de la compression
    - Capacité maximale d'un canal de transmission (sans bruit)
    - Introduit une notion mathématique du bruit
      - Établit les limites fondamentales des codes correcteur d'erreurs
  - Introduit une théorie du « secret » en information
    - Modèle de Shannon révisé – transmission d'informations **secrètes**
      - Décrit le lien entre codage et chiffrement

Théorie de l'information

- « Information »
  - Valeur instantanée d'une variable aléatoire qui est transmise vers un récepteur à travers un canal de communication
- Concepts importants
  - Variable aléatoire
  - Canal de communication – Transmission
    ou
  - Moyen de stockage
- Exemples
  - La couleur du ciel (variable aléatoire) transmise via les ondes lumineuses (canal de transmission) vers votre œil (récepteur)
  - Contenu d'un fichier (variable aléatoire) transmise via le réseau téléphonique (canal de transmission) vers votre collègue (récepteur)

Théorie de l'information

- L'information est un concept *abstrait*
  - la valeur de l'information dépend des attentes du récepteur
    - Couleur du ciel : est-ce vraiment une information ?
    - (théorie de la décision) Est-ce que la température du soleil est critique à ma décision d'investir dans une entreprise web ?

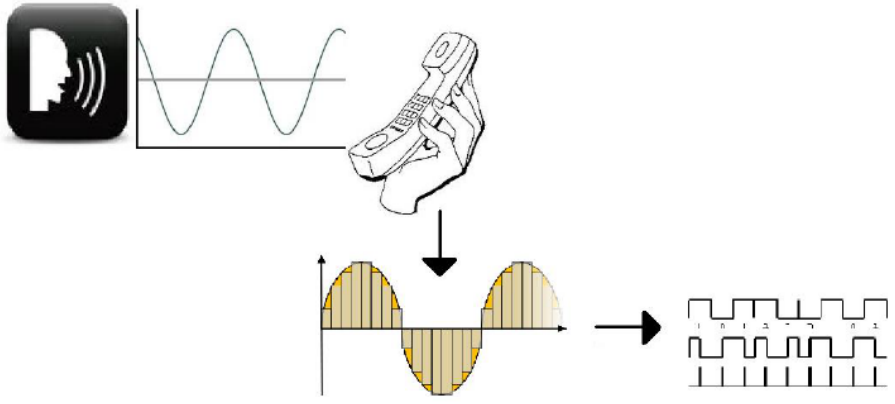
- Théorie de l'information (« Communication Theory »)
  - Ne s'intéresse pas à la sémantique de l'information (son « sens »)
  - S'intéresse à la quantité d'information qui manque au récepteur
    - Wheeler
      - *« information » in communication theory is not related to what you do say, but to what you could say*
  - Information = manque de connaissance du récepteur

Théorie de l'information

- Pour mesurer cette méconnaissance
  - Quantité d'information obtenue par observation directe de l'information obtenue/transmise
    - Représentée par la valeur de la variable aléatoire
    - Plus cette valeur est « aléatoire »
      - Plus grande est la méconnaissance du récepteur **avant** sa transmission
      - Plus sa transmission « ajoute » de l'information
    - Si cette valeur est peu aléatoire ou déterministe
      - Le récepteur a peu d'incertitude sur la valeur (méconnaissance faible)
      - La transmission n'apprend pas grand-chose au récepteur (valeur information de l'information faible)
  - Mesure mathématique d'information
    - Entropie de la variable aléatoire
  - Unité de mesure
    - Généralement le *bit*
      - Défini ainsi pour faciliter la représentation et calculs mathématiques

Théorie de l'information

- Source d'information
  - « Boîte noire »
  - Produit des symboles
    - selon un processus stochastique
    - seront codés (transformés)
    - seront stockés ou transmis
  - Variable aléatoire
    - associée au symbole produit
  - Série de symboles
    - différente à chaque fois (« réinitialisation »)
    - produite selon le même processus stochastique



- Source discrète
  - un symbole à la fois
  - sur demande (« bouton »)

« a », « z », « θ », …