Chapitre 6

CONCLUSION

Conclusion

- **Cryptologie = cryptographie + cryptanalyse**

  - La cryptographie doit fournir un certain nombre de services de sécurité :
    1. Confidentialité
    2. Intégrité
    3. Authentification
    4. Non répudiation

  - La cryptanalyse sert à vérifier l'efficace des méthodes de cryptographie contre les attaques.

Conclusion

- **Trois méthodes de cryptographie :**
  - Simple ou par substitution :
    - simple, rapide, mais facilement attaquable
  - Symétrique ou à clé privée/secrète :
    - Shannon : clé privée de longueur égale au moins au message
    - Canal sécurisé pour le transport de la clé privée
    - Avoir N * (N – 1) / 2 clés pour un groupe de N personnes.
    - Facilement attaquable si la clé privée est interceptée avec le message.
  - Asymétrique ou à clé publique :
    - Algorithmes complexes et plus lents que ceux à clef privée
    - Utilisé pour chiffrer une clef de session ou pour établir une signature.

Conclusion

- **Pour satisfaire les critères de sécurité d'une communication entre deux tiers :**
  - La vérification d'intégrité :
    - comparaison des condensés du message reçu et du message envoyé.
  - L'authentification :
    - s'assurer de l'identité d'une entité ou de l'origine d'une communication/fichier.
    - Authenticité = authentification + intégrité
  - La signature électronique :
    - garantir l'authenticité de l'expéditeur,
    - vérifier l'intégrité du message reçu,
    - assurer une fonction de non-répudiation.
  - Le certificat :
    - associer une clé publique à une entité, au moyen de la signature d'une autorité de confiance/certification afin d'en assurer la validité

Conclusion

- **Pour satisfaire les critères de sécurité d'une communication entre deux tiers :**
  - Le scellement des données :
    - garantir que le condensé utilisé pour vérifier l'intégrité des données a bien été envoyé par le bon expéditeur.
    - sceau = condensé signé à l'aide d'un chiffrement
  - La clé de session = clé secrète
    - utilisée pour chiffrer chaque jeu de données dans un système de transaction ou de communication.
    - différente à chaque communication
- **Plusieurs protocoles, situés dans la couche d'application :**
  - SSL / TLS
  - SSH
  - S-HTTP
  - SET
  - S/MIME