Introduction à la sécurité

Module 1

Introduction à la cryptologie

Pablo Rauzy <pr@up8.edu>
pablo.rauzy.name/teaching/is

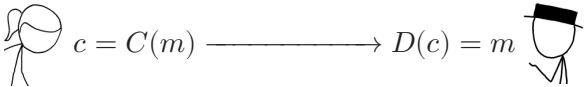
Introduction à la cryptologie

La cryptologie

- Étymologiquement, c'est "la science du secret".
- Un art ancien : les premiers documents chiffrés qu'on retrouve datent de l'Antiquité.
- Une science récente : sujet de recherche académique seulement depuis les années 60.
- La cryptologie étudie notamment
  - la confidentialité,
  - l'authentification,
  - la non-répudiation,
  - l'intégrité,
  - la preuve à divulgation nulle de connaissance, et
  - l'anonymat.
- Ses deux branches principales sont
  - la cryptographie, et
  - la cryptanalyse.

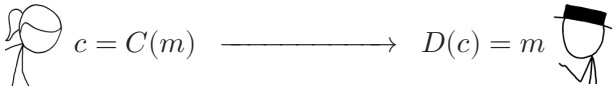
La cryptographie

- Étymologiquement, “l’écriture secrète”.
- Le but de cette discipline est de protéger les messages, en assurant leurs
  - confidentialité,
  - authenticité, et
  - intégrité.
- La cryptographie moderne utilise des clefs.
- Il y a deux grandes familles :
  - la cryptographie symétrique (à clef secrète), et
  - la cryptographie asymétrique (à clefs publique et privée).
- La cryptographie s’occupe principalement de la mise au point d’algorithmes et de protocoles permettant le chiffrement, de déchiffrement, et l’échange de messages.



La cryptanalyse

- Étymologiquement, “défaire le secret”.
- Le but de cette discipline est de casser la cryptographie.
  - C’est à dire décrypter un message chiffré, sans connaître la clef de chiffrement.
  - On appelle ce processus une attaque.
- On catégorise souvent les attaques par ce à quoi l’attaquant a accès :
  - seulement des messages chiffrés,
  - certaines correspondances entre messages clairs et chiffrés,
  - certaines correspondances entre messages clairs choisis et leur chiffré,
  - certaines correspondances entre messages chiffrés choisis et leur clair,
- Il existe de nombreuses techniques d’attaques, mais on peut distinguer deux familles :
  - la cryptanalyse classique, et
  - les attaques par canaux auxiliaires.

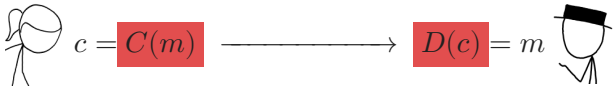


La cryptanalyse

- Étymologiquement, “défaire le secret”.
- Le but de cette discipline est de casser la cryptographie.
  - C’est à dire décrypter un message chiffré, sans connaître la clef de chiffrement.
  - On appelle ce processus une attaque.
- On catégorise souvent les attaques par ce à quoi l’attaquant a accès :
  - seulement des messages chiffrés,
  - certaines correspondances entre messages clairs et chiffrés,
  - certaines correspondances entre messages clairs choisis et leur chiffré,
  - certaines correspondances entre messages chiffrés choisis et leur clair,
- Il existe de nombreuses techniques d’attaques, mais on peut distinguer deux familles :
  - la cryptanalyse classique, et
  - les attaques par canaux auxiliaires.

La cryptanalyse

- Étymologiquement, “défaire le secret”.
- Le but de cette discipline est de casser la cryptographie.
  - C’est à dire décrypter un message chiffré, sans connaître la clef de chiffrement.
  - On appelle ce processus une attaque.
- On catégorise souvent les attaques par ce à quoi l’attaquant a accès :
  - seulement des messages chiffrés,
  - certaines correspondances entre messages clairs et chiffrés,
  - certaines correspondances entre messages clairs choisis et leur chiffré,
  - certaines correspondances entre messages chiffrés choisis et leur clair,
- Il existe de nombreuses techniques d’attaques, mais on peut distinguer deux familles :
  - la cryptanalyse classique, et
  - les attaques par canaux auxiliaires.



Les attaques par canaux auxiliaires

- Ici, on suppose la robustesse théorique de la cryptographie.
- En revanche, on cherche à exploiter des failles au niveau de l'implémentation.
- Aussi bien au niveau logiciel que matériel.
- Il existe différentes catégories d'attaques par canaux auxiliaires passives :
  - analyse de temps de calcul,
  - analyse de consommation de courant,
  - analyse des émanations électromagnétiques,
  - analyse acoustique ou lumineuse ;
- ainsi qu'active :
  - injection de fautes,
  - sondage (attaque invasive).

Chapitres du module

- Le chiffrement par substitution (et histoire de la crypto).
- La cryptographie symétrique.
- La cryptographie asymétrique.
- La cryptanalyse classique.
- Les attaques par canaux auxiliaires.