



Introduction à la cryptologie

Chapitre 0 Présentation du cours Introduction



Pablo Rauzy <pr@up8.edu>
pablorausy.fr/teaching/crypto

Présentation du cours

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des **systèmes informatiques**,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.

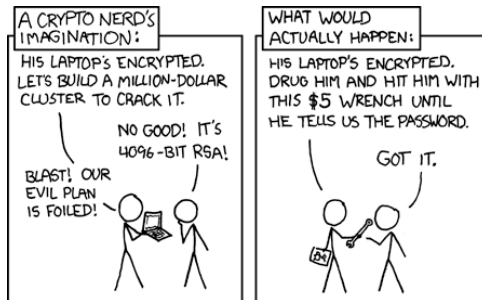
- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?
 - Protection des personnes.
 - Protection d'intérêts (financiers généralement).

- ▶ La *sécurité informatique* est un domaine très vaste.
- ▶ On la présente habituellement en affirmant que :
 - son objectif est de garantir la sécurité des systèmes informatiques,
 - ses moyens sont bien sûr techniques, mais aussi juridiques et humains.
- ▶ Pourquoi vouloir garantir la sécurité des systèmes informatiques ?
 - Protection des personnes.
 - Protection d'intérêts (financiers généralement).
- ▶ La sécurité informatique est donc elle-même un *moyen* et pas une *fin en soi*.

Les moyens de la sécurité informatique

- ▶ Dans ce cours on va principalement s'intéresser aux moyens *techniques*.
- ▶ Cependant, gardez à l'esprit qu'ils ne sont pas suffisant à eux seuls.



Les moyens techniques de la sécurité informatique

- ▶ Les moyens techniques de la sécurité informatique peuvent être catégoriser par *niveaux* qui correspondent à des *disciplines* plus ou moins distinctes :
 - la protection des *données brutes* avec la *cryptologie*,
 - la protection des *systèmes et infrastructures* avec la *sécurité des systèmes d'information*,
 - la protection des *personnes* avec la *privacy*.
- ▶ En pratique, la protection des personnes implique souvent la protection d'un système qui à son tour implique la mise en œuvre de cryptologie.
- ▶ Et il y a bien sûr des champs disciplinaires transverses :
 - la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle,
 - la recherche de vulnérabilité, l'analyse de *malware*,
 - le contrôle d'accès et le contrôle d'usage,
 - l'ingénierie sociale,
 - etc.

 Objectifs :

- Comprendre les bases de la cryptologie.
- Saisir l'importance de se poser la question de la sécurité dès la phase conception d'un projet, par un aperçu en largeur du domaine de la sécurité informatique.
- Acquérir des bases de sécurité par la pratique.

Organisation

- ▶ Chiffrement par substitution.
- ▶ Cryptographie symétrique.
- ▶ Cryptographie asymétrique.
- ▶ Cryptanalyse classique.
- ▶ Canaux auxiliaires.

Évaluation

- Votre évaluation pour ce cours prendra en compte :
- les TPs,
 - un projet.

Un mot sur les projets tuteurés

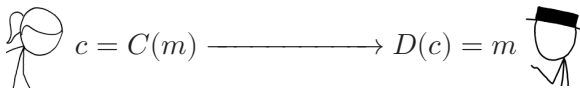
- ▶ Premier semestre, état de l'art :
 - comprendre où en est la science sur le sujet,
 - s'appropriier la problématique,
 - commencer à esquisser une solution,
 - produire un rapport intermédiaire.
- ▶ Second semestre, implémentation :
 - proposer une solution,
 - mettre en œuvre celle-ci par la programmation,
 - faire une démonstration à la fin de l'année,
 - mettre à jour le rapport avec les résultats obtenus.
- ▶ Les projets tuteurés se font en binôme.
- ▶ Si le domaine de la crypto/sécurité/privacy vous intéresse : contactez-moi !

Introduction

- ▶ 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.


$$c = C(m) \longrightarrow D(c) = m$$

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).