Pratique de la cryptographie

Master Informatique — Semestre 1 — UE optionnelle de 3 crédits

Année 2015-2016

Version du 6 septembre 2015

À quoi sert la cryptographie ?

① À résoudre trois types de **problèmes fondamentaux** :

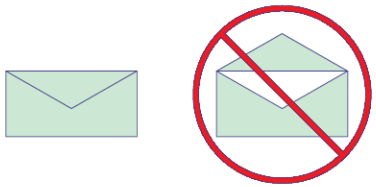
- Intégrité : téléchargement, signature, etc.
- Confidentialité : sur un support ou sur un canal.
- Authentification : interactive ou non.

② À garantir la **sécurité** d'un protocole ou d'un logiciel

- contrôle d'accès : local ou à distance
- signature électronique : commerce en ligne, non répudiation.
- vote électronique.
- code mobile.
- etc.

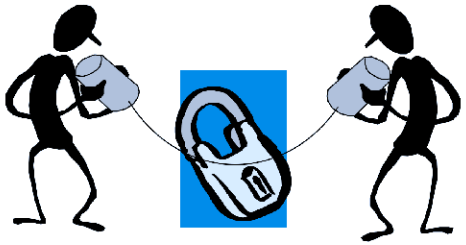
Les trois concepts de base : intégrité, confidentialité et authentification

Intégrité : Garantir qu'un message (un document, ou encore un fichier) n'a pas subi de modification (aussi bien accidentelle qu'intentionnelle)



Deux types de confidentialité :

Archiver des données sur un **support**



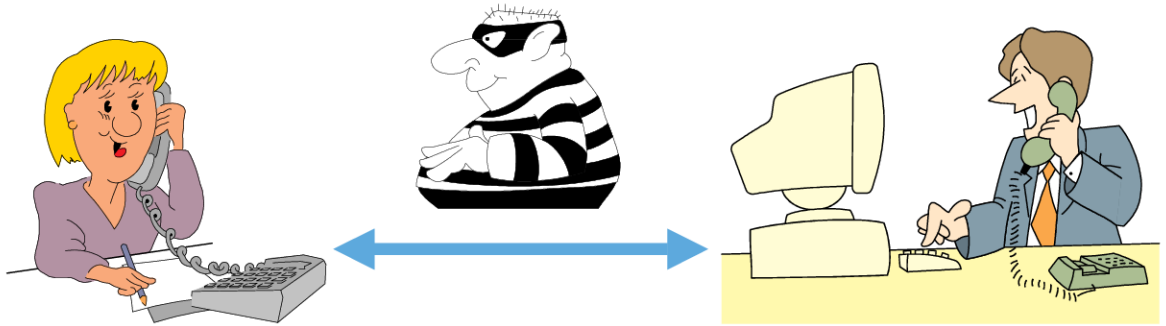
Communiquer des données sur un **canal**

de façon qu'un tiers ne puisse en prendre connaissance

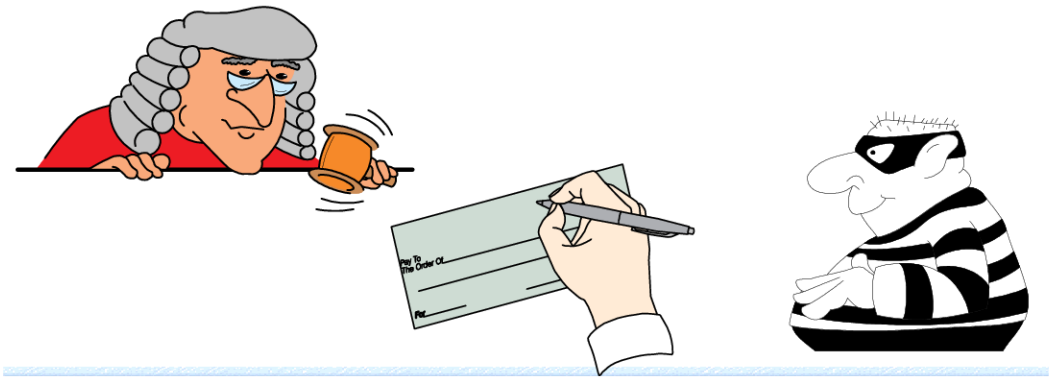
Les trois concepts de base : intégrité, confidentialité et authentification

Deux types d'authentification :

① Prouver de façon **interactive** son identité à un interlocuteur.



② Attacher, à un message, une preuve **non-interactive** de son origine.



Qu'apprend-t-on dans cette UE ?

① Comprendre les **problèmes** de confidentialité, d'authentification, d'intégrité, mais aussi les notions de **signature** et de **certificats**.

② Les types de **solutions** : cryptographie symétrique, asymétrique, par flot, par blocs, fonctions de hâchage, architecture à clefs publiques.

③ Les **techniques** éprouvées : RC4, AES, RSA, DSA, etc.

④ Le détail des **calculs** pour le codage de ces méthodes en C ou Java
- $\mathbb{Z}/n.\mathbb{Z}$ pour le RSA et le DSA ;
- $\mathbb{F}_{256}$ pour l'AES.

⑤ L'utilisation de *librairies* pour le calcul avec de grands entiers, à savoir **`GMP`** en C ou **`BigInteger`** en Java, ainsi que le fonctionnement de l'extension JCE (Java Cryptography Extension).

Ce que ne comprend pas cette UE

① Les **preuves** des résultats mathématiques élémentaires utilisés : le lemme de Gauss, le théorème d'Euler, le lemme de Miller-Rabin, le théorème des nombres premiers, etc. Néanmoins quelques annexes seront mises à la disposition des étudiants curieux.

② Il ne sera pas non plus question d'**entropie** (vue dans l'option de L3) ni de calcul sur les courbes elliptiques.

③ Les applications à la **sécurité des réseaux**.

- ⇝ SSH ne sera même pas évoqué !
- ⇝ OpenSSL et l'extension JSSE (Java Secure Socket Extension) seront étudiés en M2, dans la filière FSIL (option FSI).

④ Les applications à la **sécurité du logiciel**.

- ⇝ Le JAAS (Java Authentication and Authorization Service) sera vu en M2, dans la filière FSIL (option FSI).

Modalités de Contrôle de Connaissance

Cette option se compose cette année de 10 cours de 1h et de 10 séances TD/TP de 2h (sur machine) répartis sur 11 semaines.

— La note finale est $\texttt{NF} = 0.6 * \texttt{Examen} + 0.4 * \texttt{Projet}$.

- L'examen sert principalement au contrôle des connaissances.

  Les documents ne sont pas autorisés.
- Le projet évalue le savoir-faire acquis en programmation de fonctions cryptographiques.

— En seconde session, la note de projet est conservée et la formule devient $\texttt{NF}' = \max\{\texttt{Examen}', 0.6 * \texttt{Examen}' + 0.4 * \texttt{Projet}\}$.

Prérequis

- Programmation en C et en Java
- Ne pas être allergique aux termes suivants : probabilité, division euclidienne, reste, PGCD, nombre premier, polynôme, produit matriciel, exponentielle, logarithme.

À propos du projet

① Le projet doit être réalisé **en binôme ou bien seul**.

② Il s'appuie en partie sur quelques **exercices proposés en TP**.

③ Les binômes seront constitués dès la deuxième semaine d'enseignement.

④ **Le plagiat**, c'est-à-dire rendre un travail récupéré sur Internet ou échangé avec un autre binôme, conduit à la note 0/20.

⑤ Échanger des idées entre binômes, pour mieux comprendre le sujet, est autorisé ; **lire le code** d'un autre binôme ne l'est pas.