Présentation de l'UE Cryptographie

Master Informatique — Semestre 2 — UE optionnelle de 3 crédits

Année 2018-2019

Version du 6 janvier 2019

À quoi sert la cryptographie ?

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

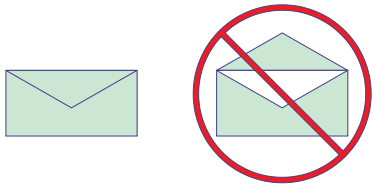
- Intégrité : téléchargement, signature, etc.
- Confidentialité : sur un support ou sur un canal.
- Authentification : interactive ou non.

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.

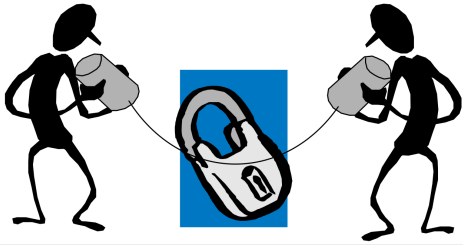
Les trois concepts de base : intégrité, confidentialité et authentification

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**



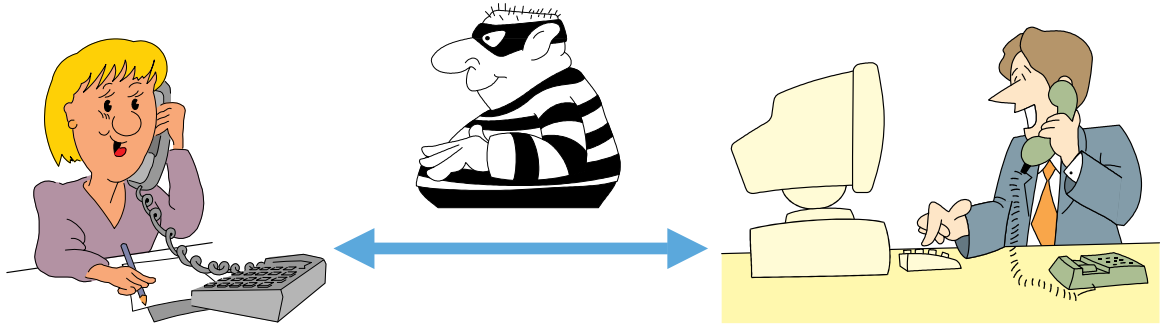
Communiquer des données sur un **canal**

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 Le fonctionnement précis des **techniques** éprouvées : AES, RSA, DSA, etc.

④ Le détail des calculs effectués :
- $\mathbb{Z}/n.\mathbb{Z}$ 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.

⑥ L'**emploi 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** ni, probablement, de calcul sur les **courbes elliptiques**.

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

- ⇝ SSH ne sera même pas évoqué !
- ⇝ L'extension JSSE (Java Secure Socket Extension) sera étudiée dans un TP de l'UE ≪ Sécurité Internet et Réseaux ≫.

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

- ⇝ Le JAAS (Java Authentication and Authorization Service) sera étudié dans l'UE ≪ Politiques et modèles de contrôle d'accès ≫.

Modalités de Contrôle des Connaissances

Cette option se compose de 9 h. de cours et de 18 h. de TD/TP répartis sur 6 semaines.

— La note finale est $\texttt{NF} = 0.75 * \texttt{Examen} + 0.25 * \texttt{Projet}$.

- Le projet évalue le savoir-faire acquis en programmation.
- L'examen sert principalement au contrôle des connaissances.

  Les documents ne sont pas autorisés.

— En seconde session, la note de projet est conservée et la formule devient $\texttt{NF}' = \max\{\texttt{2ndExamen}, 0.75 * \texttt{2ndExamen} + 0.25 * \texttt{Projet}\}$.

Prérequis

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

À propos du projet

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

② Il consiste en des rendus d'**exercices de TP**.

③ Les **binômes** seront constitués dès la fin de la première 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.