Cryptographie à clé publique

MAT 2450

Janvier 2022

La cryptographie

- **Principe de base :** transmettre de l'information en s'aidant de codes secrets pour la cacher

- Historiquement, il a été difficile de trouver des codes secrets qui résistent longtemps

- Des scientifiques astucieux et astucieuses finissent souvent, avec assez de temps, par trouver la clé

Hahpsoh

- Considérons un code qui permute les lettres de l'alphabet de la façon suivante:

$$a \to d,\ b \to e,\ c \to f,\ \ldots$$

$$\cdots\ x \to a,\ y \to b,\ z \to c$$

- Il est très facile de briser ce code. Voici comment on pourrait procéder:
  - En français, le *e* est la lettre la plus utilisée
  - En examinant les messages, on finirait par déduire que $e \to h$ et le reste de la clé du code suivrait.

Une autre faille

- Pour que le receveur du message secret soit capable de le décrypter, l'expéditrice doit lui envoyer la clé.

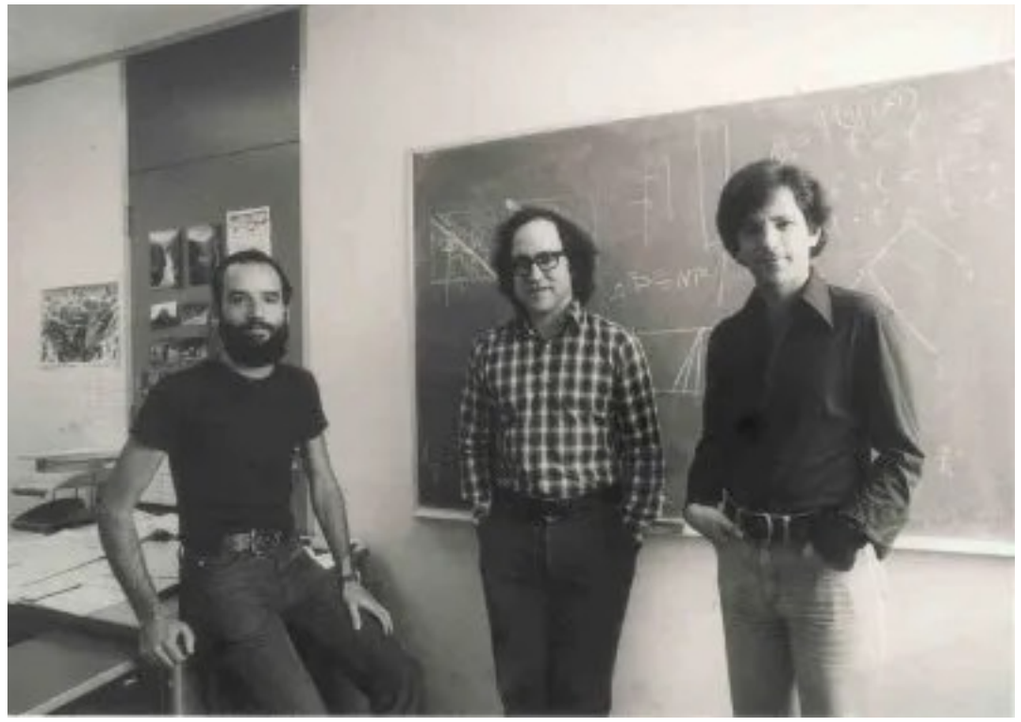
- Comme tout autre échange d'information, il est fort possible que quelqu'un intercepte la clé

- Et si la clé était publique pour commencer?

Le code RSA

Rivest-Shamir-Adleman

- Un code à **clé publique**!
- Ce code tient depuis 1978
- Il suffit d'apprendre à un ordinateur à factoriser des grands nombres
- Ce code est utilisé partout sur internet. Par exemple lorsque je transfère mes informations bancaires à un marchant en ligne.



Dan Wright, RSA Algorithm course, imps.mcmaster.ca

Le code RSA utilise quoi comme maths?

- Le code RSA est basé sur la théorie des nombres, plus particulièrement sur l'arithmétique

$$(+, \times) \mod n$$

- On utilise aussi le petit théorème de Fermat généralisé par Euler. Un résultat qui date du 18e siècle.

Pourquoi le code RSA fonctionne aussi bien?

- **Difficile** pour un ordinateur de **factoriser un grand nombre en ses facteurs premiers**

- **Facile** pour un ordinateur de **construire un grand nombre premier**

- **Facile** pour un ordinateur de **décider si un grand nombre est premier**

Forces du code RSA

- Clé publique : impossible que la clé soit intercepter par erreur. Tout le monde l’a déjà dans sa tête.
- Il est possible de signer un message. On peut alors s’assurer de sa provenance.