



Information, Calcul et Communication

Compléments de cours

J.-C. Chappelier

Leçon « Sécurité » – Points clés

- ▶ La sécurité totale n'existe pas.
 - ☞ compromis entre *risque* d'une attaque et *prix* (au sens large) d'une défense
- ▶ menaces (vol, manipulation, destruction, démenti, usurpation d'identité, contournement des défenses)
et les défenses correspondantes
(confidentialité, intégrité, disponibilité, responsabilité, authentification, autorisations)
- ▶ cryptographie : confidentialité, intégrité (, responsabilité)
- ▶ cryptographie symétrique à clé secrète (One-time pad, DES, AES)
/ cryptographie asymétrique à clé « publique » (RSA)
- ▶ confidentialité parfaite (au moins autant de clés que de messages et d'entropie supérieure à celle des messages)
/ confidentialité pratique (protection par complexité algorithmique)
- ▶ RSA :
 - ▶ $M^x \pmod n$
 - ▶ confidentialité : on encrypte avec la clé publique de l'autre
 - ▶ responsabilité (et intégrité) : on encrypte avec sa propre clé privée

Leçon « Sécurité » – Etude de cas

Si je veux transmettre vos notes au service académique (SAC) à la fin de l'année, mais souhaite qu'elles restent lisibles (par exemple par vous), alors j'assure :

- A]** l'intégrité des notes en les chiffrant avec la clé publique du SAC.
- *B]** l'intégrité et l'identité de l'auteur des notes en les signant avec ma clé privée.
- C]** l'identité de l'auteur des notes en les chiffrant avec la clé publique du SAC.
- D]** la confidentialité des notes en les chiffrant avec ma clé privée.

Leçon « Sécurité » – Etude de cas

Dans un système de cryptographie à clé publique,

- A] aucune confidentialité n'est possible puisque la clé est publique.
- B] on ne peut pas avoir à la fois de la confidentialité et de la responsabilité.
- C] chaque participant possède au moins deux clés et utilise sa propre clé privée pour envoyer des messages confidentiels.
- *D] chaque utilisateur a une clé publique et une clé privée qu'il est, à l'heure actuelle, pratiquement impossible de retrouver avec la clé publique.

Leçon « Sécurité » – Etude de cas

Vous souhaitez communiquer de façon confidentielle en utilisant RSA.

Votre clé publique est (79, 899) ; votre clé privée est (319, 840).

La clé publique de votre destinataire est (485, 667).

A] Comment transmettez vous l'entier 238 ?
Donnez la réponse sous la forme « $a^b \bmod c$ ».

$238^{485} \bmod 667$
(qui vaut 399)

B] Si vous recevez l'entier 532, comment le décidez vous ?

$532^{319} \bmod 899$
(qui vaut 408)

Leçon « Sécurité » – Etude de cas

Vous souhaitez envoyer, de façon confidentielle en utilisant RSA, une image dont le début du contenu est 10001101110101100101...

La clé de votre destinataire est (5, 69). Votre clé publique est (7, 33) et votre clé privé (3, 20).

A] Comment découpez vous le message à envoyer ?

(Combien de bits pouvez-vous encrypter au maximum ?)

6 bits (inférieur ou égal à 63, donc strictement inférieur à 69) si l'on ne s'intéresse qu'à cette question (confidentialité))

et 5 bits (donc strictement inférieur à 33) si l'on veut aussi pouvoir signer ou recevoir des images en retour

B] Supposons que vous découpiez le message par paquets de 4 bits, quel est, en *binaire*, le premier message que vous envoyez ? (*sans* calculette !)

Les 4 premiers bits sont 1000, soit la valeur 8.

On envoie donc $8^5 \pmod{69}$

Notez que $8^2 = 64 = -5 \pmod{69}$, donc $8^4 = 25 \pmod{69}$, et $8^5 = 200 = 62 \pmod{69}$ (2×31). Et donc, en binaire : 111110 (63 - 1).

Leçon « Sécurité » – Etude de cas

En fait, l'image n'est **pas** confidentielle, mais votre correspondant souhaite s'assurer que c'est bien vous qui avez envoyé cette image.

A] Quel est alors le premier message que vous envoyez ?

$$8^3 = 17 \pmod{33} \quad (\text{note : } 64 = -2 \pmod{33})$$

B] Cette façon de communiquer garantit-elle l'intégrité de l'image ?

oui... mais il faut alors aussi envoyer toute l'image d'origine (pour vérification) : la signature et l'image

Fin du cours d'ICC

- ▶ demain :
 - ▶ 13h15–15h00 : quelques questions de l'examen d'il y a deux ans (je vous laisse celui de l'an passé comme « vrai entraînement à blanc »)
 - ▶ 15h00–16h15 : exercices « comme d'habitude » :
 - ▶ exercices sur la sécurité informatique
 - ▶ révisions : examens passés
- ▶ **jeudi prochain, 8h15 – 11h00 : examen final**