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 :
  - $M^x \mod n$
  - confidentialité : on encrypte avec la clé publique de l'autre
  - responsabilité (et intégrité) : on encrypte avec sa propre clé privée

publique : (e, n)
privée : d
lien : $ed = 1 \mod m$

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 :

notre clé à nous

seul le SAC peut lire

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.

publique du SAC

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).

d m

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

$238^{485} \mod 667$

2. Si vous recevez l'entier 532, comment le décodez vous ?

$532^{319} \mod 899$

$M^x \mod n$ ici x = notre d

p q

$n = q \cdot p$

d

$e \cdot d = 1 \mod m$

$m = (p-1)(q-1)$

public e et n

⇒ privé : d p q m

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 $(485, 667)$.

1. Comment transmettez vous l'entier 238 ?
   Donnez la réponse sous la forme « $a^b \mod c$ ».
   $238^{485} \mod 667$
   (qui vaut 399)

2. Si vous recevez l'entier 532, comment le décodez vous ?
   $532^{319} \mod 899$
   (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 10001101110101101001101... publique
La clé de votre destinataire est $(5, 69)$. Votre clé publique est $(7, 33)$ et votre clé privé $(3, 20)$.

1. Comment découpez vous le message à envoyer ?
   (Combien de bits pouvez-vous encrypter au maximum ?)

   5 6 7

   $M^5 \mod 69$
   $\Rightarrow M \leq 68$

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

   $M = 1000 = 8$ $\quad 8^5 \mod 69 =$

   $8^2 = 64 \equiv (-5) \mod 69$ $\quad 8^4 = (-5)^2 = 25 \mod 69$

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 $(3,20)$.

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

Leçon « Sécurité » – Etude de cas

⇒ responsabilité : $M^{d_{nous}} \bmod n_{nous}$

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

1. Quel est alors le premier message que vous envoyez ?

$M^3 \bmod 33 = 8^3 \bmod 33$

2. Cette façon de communiquer garantit-elle l'intégrité de l'image ?

ou si vous savez d'image

⇒ envoyer aussi l'image

(confidentiel $(M')^5 \bmod 69$

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.

1. Quel est alors le premier message que vous envoyez ?
   $8^3 = 17 \mod 33$ (note : $64 = -2 \mod 33$)

2. 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 entrainement à blanc »)
  - 15h15–16h00 : exercices « comme d'habitude » :
    - exercices sur la sécurité informatique
    - révisions : examens passés

    (et, pour rappel : soutien de 16h15 à 18h00 en CE 106)

- jeudi prochain : réponses aux questions :
  - 8h15–10h00 : en salles d'exercices, avec les assistant(e)s, comme d'habitude
  - 10h15–11h00 : ici en amphi CE 1 4 avec moi

- **vendredi en huit (19 décembre), 13h15 – 16h00 : examen final**

Et n'oubliez pas de **faire le quiz de sensibilisation à la cybersécurité opérationnelle** avant vendredi 19 décembre au soir