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 $(485, 667)$.

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

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

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 ?)

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

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 ?

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