# Chiffrement symétrique

*i* Le chiffrement symétrique permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

Source : CNIL

## • Chiffrement de Vigenère

### Exercice 1

Le chiffrement de Vigenère introduit le principe de clé se présentant généralement sous la forme d'un mot (ou d'une phrase) que l'on répète. Plus la clé est longue et variée, mieux le texte sera chiffré.
On considère la méthode de chiffrement suivante.

À chaque lettre de l'alphabet, on fait correspondre sa position dans l'alphabet, c'est-à-dire un entier entre 0 et 25 (A correspondant à 0, B à 1, etc.) À chaque lettre à coder, on associe l'entier $x$ correspondant. À chaque lettre de la clé, on associe l'entier y correspondant. On détermine l'entier $z$ , où $z$ est le reste de $x+y$ dans la division euclidienne par 26. La lettre chiffrée sera obtenue avec le nombre $z$.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Exemple : Codage du mot VIGENERE en utilisant la clé DEUX. On obtient le mot YMABQILB.

| Mot à coder | V | I | G | E | N | E | R | E |
|---|---|---|---|---|---|---|---|---|
| $x$ | 21 | 8 | 6 | 4 | 13 | 4 | 17 | 4 |
| Clé | D | E | U | X | D | E | U | X |
| $y$ | 3 | 4 | 20 | 23 | 3 | 4 | 20 | 23 |
| $z$ | 24 | 12 | 0 | 1 | 16 | 8 | 11 | 1 |
| Mot codé | Y | M | A | B | Q | I | L | B |

1. On considère le chiffrement de Vigenère utilisant la clé `NSI`. Par quel mot est codé le mot `RECURSIVITE` ?
2. Déchiffrer le mot CJWTJIZEM, la clé étant toujours NSI ?

*Adapté de "Le livre scolaire"*

## Chiffrement asymétrique

*i* Le chiffrement asymétrique, également connu sous le nom de chiffrement à clé publique, est une technique de cryptage qui utilise une paire de clés distinctes pour chiffrer et déchiffrer des messages. Une clé est appelée **clé publique** et est largement diffusée, tandis que l'autre clé, appelée **clé privée**, est gardée secrète par son propriétaire.

L'histoire du chiffrement asymétrique remonte aux années 1970, lorsque Whitfield Diffie et Martin Hellman ont publié leur article sur le chiffrement à clé publique. Leur travail a jeté les bases de la cryptographie moderne et a conduit à la création de plusieurs algorithmes de chiffrement asymétrique, tels que RSA, El Gamal, et DSA.

Le fonctionnement du chiffrement asymétrique est basé sur la difficulté de résoudre certains problèmes mathématiques, tels que la factorisation d'un grand nombre entier en facteurs premiers.
Dans le cas de RSA, l'algorithme de chiffrement utilise une clé publique pour chiffrer le message, qui peut être envoyé en toute sécurité sur un réseau public.
Le message chiffré ne peut être déchiffré que par la clé privée correspondante, qui est détenue uniquement par le destinataire du message.

Le chiffrement asymétrique est largement utilisé dans de nombreux protocoles de sécurité, tels que SSL/TLS, SSH, PGP, et S/MIME, pour protéger les données sensibles sur Internet.

### • Le cryptage RSA

*i*

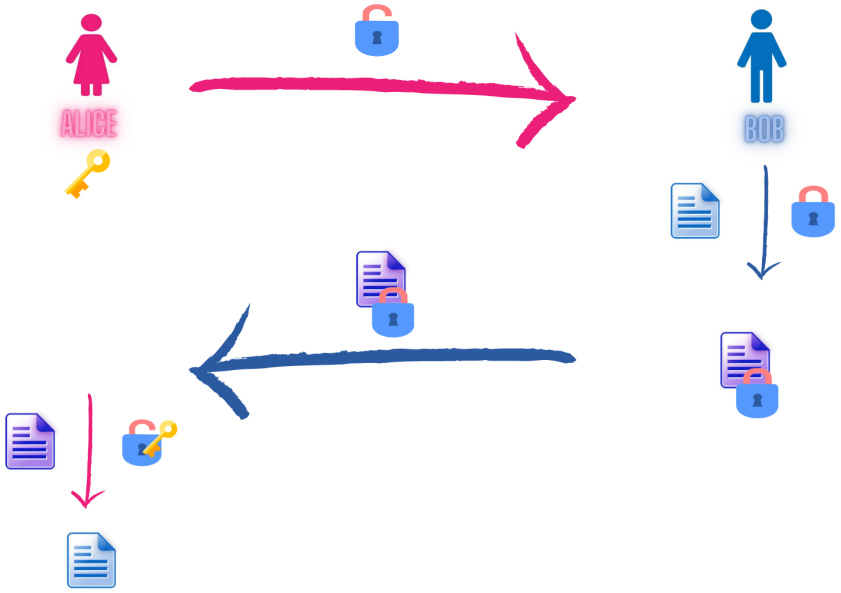
Inventé par Ron Rivest, Adi Shamir et Len Adleman, le système RSA (nommé d'après les initiales de ses auteurs) fut présenté pour la première fois en août 1977, dans la chronique mathématique de Martin Gardner de la revue Scientific American.
Les circonstances de sa découverte sont assez amusantes : ces trois auteurs avaient décidé de travailler ensemble pour démontrer l'impossibilité logique des systèmes cryptographiques « à clé publique ». Ils échouèrent donc en découvrant un système de cryptographie à clé publique, le système RSA. Mais cet échec n'en est pas vraiment un : l'efficacité du système RSA à clé publique est depuis lors reconnue et a assuré la renommée de ses auteurs !

*Source : https ://interstices.info/*

RSA est l'un des algorithmes de chiffrement asymétrique les plus populaires et est utilisé dans de nombreux protocoles de sécurité, notamment SSL/TLS et PGP.

#### •• Principe du fonctionnement du cryptage RSA

Pour illustrer le fonctionnement du cryptage RSA, on va supposer que Bob veuille inviter Alice à sortir. Il doit transmettre l'heure du rendez-vous mais ne veut que personne d'autre que Alice ne puisse le lire.
Pour ce faire il demande à Alice de lui fournir une clé de chiffrement. Cette clé peut être diffusée à tout le monde car elle ne sert qu'à crypter les données et pas à les décrypter. Cette clé s'appelle la clé **publique**.
Bob récupère la clé, crypte l'heure du rendez-vous avec et envoie le message crypté à Alice.
Quand Alice reçoit le message, elle va utiliser une seconde clé pour le déchiffrer. Cette clé s'appelle la clé **privée**. Seule Alice doit l'avoir en sa possession.
Les clés publique et privée sont liées entre elles, elles sont générées au même moment.




### •• Définition des clés

Le cryptage RSA consiste en la génération de deux clés.

- Choisir deux nombres premiers $p$ et $q$. On notera $n = p \times q$
- Calculer $\phi(n) = (p-1)(q-1)$.
- Choisir un nombre $e$ premier avec $\phi(n) = (p-1)(q-1)$.
- Déterminer $d$ l'inverse de $e$ modulo $\phi(n)$ tel que $e \times d + m \times (p-1)(q-1) = 1$ ou $m$ est un entier relatif.

- La clé publique sera le couple $(e\,;\,n)$
- La clé privée sera le couple $(d\,;\,n)$

### •• Codage / décodage

- Pour coder un nombre $a$, on calcule $b \equiv a^e [n]$.
- Pour décoder le nombre $b$, on calcule $b^d [n]$ et on retrouve $a$.

## • Exercice

**Exercice 2** ★

Dans cet exercice, on utilisera les nombres premier $p = 7$ et $q = 13$.

1. Déterminer une clé publique et une clé privée.
2. Utiliser la clé publique pour coder le nombre A = 10 en un nombre B.
3. Utiliser la clé privée pour décoder le nombre B. Vérifier que l'on retrouve effectivement le nombre A.