# La Cryptographie : le chiffrement symétrique

[sommaire]

1. ## Objectifs

- Découvrir le chiffrement symétrique ;
- Utiliser un algorithme de chiffrement symétrique.

- ## Le chiffrement symétrique ou à "clé secrète"

  - Le chiffrement symétrique permet de chiffrer et de déchiffrer un contenu avec la même clé.
  - 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 précaution, sans quoi la clé pourrait être récupérée par les mauvaises personnes (pirates), ce qui n’assurerait plus la confidentialité du message.




  - Le `chiffrement symétrique`, ou chiffrement à clé secrète, utilise une seule clé pour chiffrer et déchiffrer les données. Vous devez partager cette clé avec le destinataire.
  - Le `chiffrement symétrique` est un type de chiffrement dans lequel **une seule clé** (une clé secrète) est utilisée pour chiffrer et déchiffrer les données électroniques.
  - **Les entités communiquant via un chiffrement symétrique doivent échanger la clé afin qu'elle puisse être utilisée dans le processus de déchiffrement. Cette méthode de chiffrement diffère du chiffrement asymétrique où une paire de clés - une publique et une privée - est utilisée pour chiffrer et déchiffrer les messages.**

- ## Types d'algorithmes de chiffrement symétrique

  - Il existe deux types d'algorithmes de chiffrement symétrique :
    - **Algorithmes de bloc**. Des longueurs définies de bits sont cryptées dans des blocs de données électroniques à l'aide d'une clé secrète spécifique. Au fur et à mesure que les

apcpedagogie.com

données sont cryptées, le système conserve les données dans sa mémoire en attendant des blocs complets.

- **Algorithmes de flux**. Les données sont cryptées lors de leur diffusion au lieu d'être conservées dans la mémoire du système.

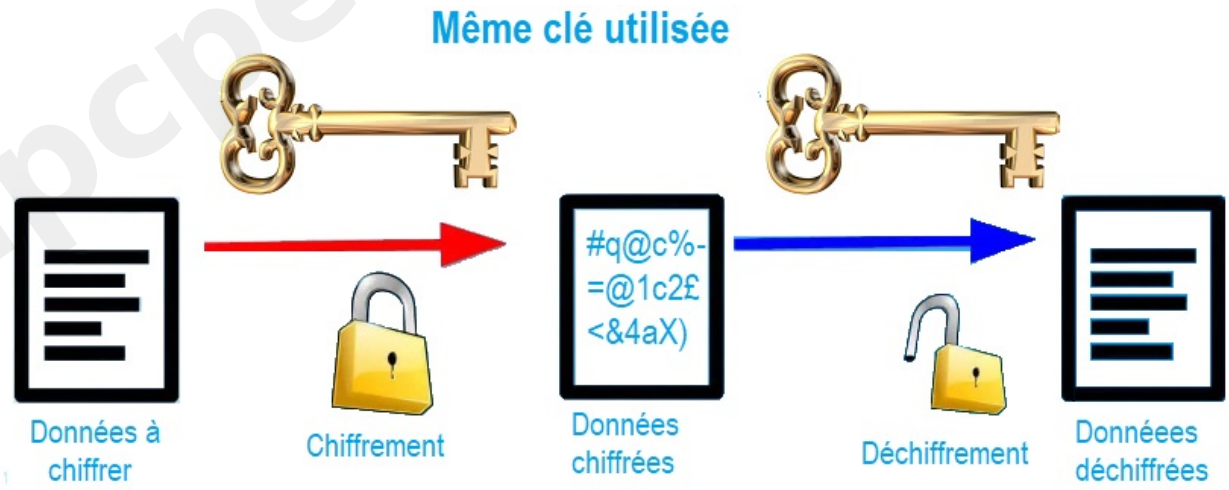
## Exemples d'algorithmes de chiffrement symétrique

- Voici quelques exemples d'algorithmes de chiffrement symétrique :

  **AES** (norme de chiffrement avancé) **DES** (norme de chiffrement des données) **IDEA** (Algorithme international de chiffrement des données) **Blowfish** (remplacement direct pour DES ou IDEA) **RC4** (Cryptographe Rivest 4) **RC5** (chiffre Rivest 5) **RC6** (chiffre Rivest 6)
- AES, DES, IDEA, Blowfish, RC5 et RC6 sont des chiffrements par blocs. RC4 est un chiffrement de flux.

## Qu'est-ce que le chiffrement (cryptage) AES

- L'`Advanced Encryption System` est un standard très répandu pour réaliser du chiffrement symétrique.
- Il possède énormément de bonnes propriétés : facile à calculer, implémentation possible au niveau logiciel comme au niveau matériel (implémentation câblée).
- Ce type de chiffrement est utilisé notamment pour des protocoles tels que SSL (sécurisant les connexions HTTP) ou encore pour chiffrer son disque dur.




- L'algorithme symétrique le plus couramment utilisé est l'Advanced Encryption Standard (AES), qui était à l'origine connu sous le nom de Rijndael.

apcpedagogie.com

- Il s'agit de la norme établie par le National Institute of Standards and Technology des États-Unis en 2001 pour le cryptage des données électroniques annoncée dans US FIPS PUB 197.
- Cette norme remplace DES, qui était utilisée depuis 1977. Sous NIST, le chiffrement AES a une taille de bloc de 128 bits, mais peut avoir trois longueurs de clé différentes comme indiqué avec AES-128, AES-192 et AES-256.

## Avantages et inconvénients du chiffrement symétrique

- Les **avantages du chiffrement symétrique** sont qu'il est facile à mettre en place et qu'il peut être réalisé en un clin d'œil. De plus, il est assez simple, tous les âges et tous les milieux peuvent l'utiliser.
- Le chiffrement asymétrique est plus difficile à comprendre et à utiliser.
- L'**inconvénient** est que la clé secrète doit être partagée avec le destinataire.
- Dans le cas du PEM, la clé secrète est chiffrée avec le mot de passe de l'utilisateur. Ainsi, il suffit de s'assurer que le mot de passe n'est pas facile à deviner.
- Si vous utilisez la même clé secrète pour chiffrer tous vos emails et si quelqu'un apprend cette clé secrète, tous vos emails chiffrés seront compromis.

## À retenir

- Le chiffrement symétrique permet de sécuriser ses propres données avec une unique clé.
- Le chiffrement symétrique permet d'échanger des données avec des pairs s'ils disposent eux aussi de la clé.
- Le partage de clé est très complexe et doit rester exceptionnel pour conserver sa confidentialité.
- L'algorithme AES permet de réaliser un chiffrement symétrique.

---

**Sommaire du cours Administration et sécurité des sites web**

Source : https://apcpedagogie.com/la-cryptographie-le-chiffrement-symetrique · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com