

Principes Fondamentaux de la Cryptographie

par Stéphane LARCHER

Principe de Kerckhoffs

Sécurité par la clé

La sécurité ne doit pas reposer sur le secret de l'algorithme ou des détails de mise en œuvre, mais uniquement sur la clé secrète.

Transparence algorithmique

Un système cryptographique doit rester sûr même si tout est connu à son sujet, à l'exception de la clé.

Fondement moderne

Ce principe est également connu sous le nom de principe de Shannon dans la cryptographie contemporaine.



Robustesse face à la divulgation



Sécurité par l'obscurité

Si la sécurité dépend d'un algorithme tenu secret, la moindre fuite d'information peut compromettre l'ensemble du système.



Protection par la clé

Si la sécurité dépend uniquement de la clé, même si l'algorithme est publié, il reste nécessaire de trouver la clé pour casser le système.



Sécurité mathématique

Trouver ou deviner la clé doit être mathématiquement hors de portée pour garantir la sécurité du système.



Amélioration de la confiance



Examen public

Un algorithme public peut être examiné et testé par la communauté scientifique ou les pairs.



Détection des failles

Les failles potentielles sont détectées et corrigées plus rapidement grâce à l'examen collectif.



Confiance accrue

On obtient un niveau de confiance bien supérieur comparé à un algorithme "fermé" dont les vulnérabilités pourraient rester inconnues.

Facilité de mise à jour

Découverte de vulnérabilité

Identification d'une faille dans
l'algorithme cryptographique ouvert

Déploiement

Proposition d'une version corrigée
facilement déployable



Modification

Facilité de modifier l'algorithme pour
corriger la vulnérabilité

Test

Possibilité de tester à nouveau
l'algorithme modifié

Problèmes des systèmes fermés



Algorithme secret compromis

Les secrets de l'algorithme sont exposés



Difficultés de transition

Transition chaotique vers un nouveau "secret"



Vulnérabilités cachées

Faibles inconnues exploitées par des adversaires

Chiffrement classique

Historique

Les premiers systèmes de chiffrement (dits « classiques ») reposaient souvent sur des transformations simples du texte en clair (le message à protéger). On trouve notamment :





Chiffrement classique

Le chiffre de César

Principe : Décaler chaque lettre de l'alphabet d'un certain nombre de positions (par exemple 3 : $A \rightarrow D$, $B \rightarrow E$, $C \rightarrow F$, etc.).

Faible sécurité : Une analyse de fréquences (observer la fréquence des lettres chiffrées) permet de retrouver assez facilement le décalage. En effet, dans une langue donnée, certaines lettres apparaissent plus souvent que d'autres (en français, E est très fréquent, en anglais E ou T, etc.).



ENCRYPTED

Chiffrement classique

Le chiffre de Vernam ou « One-Time Pad » (1917)

Principe : Utiliser une clé de la même longueur que le message à chiffrer, et faire un XOR (ou une addition modulo, selon la formulation) entre chaque caractère du message et la clé.

Utilisation unique

La clé doit être utilisée une seule fois, puis détruite.

Sécurité parfaite

Claude Shannon a démontré mathématiquement que si la clé est véritablement aléatoire, qu'elle a la même longueur que le message et qu'elle n'est jamais réutilisée, alors ce système est inattaquable (on parle de "perfect secrecy").

Limite pratique

Il est très contraignant de gérer autant de clés aléatoires que de messages, surtout si ces clés doivent rester secrètes et ne jamais être réutilisées. Dans la pratique, le « One-Time Pad » n'est donc guère employé qu'à des fins très particulières (ex. télégrammes diplomatiques ultra-sensibles, communications militaires pointues, etc.).



SecureData

Théorie de l'information de Shannon

Sécurité parfaite

Aucune information sur le texte en clair

Selon Shannon, un système de chiffrement est dit parfaitement sûr si la connaissance du texte chiffré n'apporte **aucune** information sur le texte en clair.

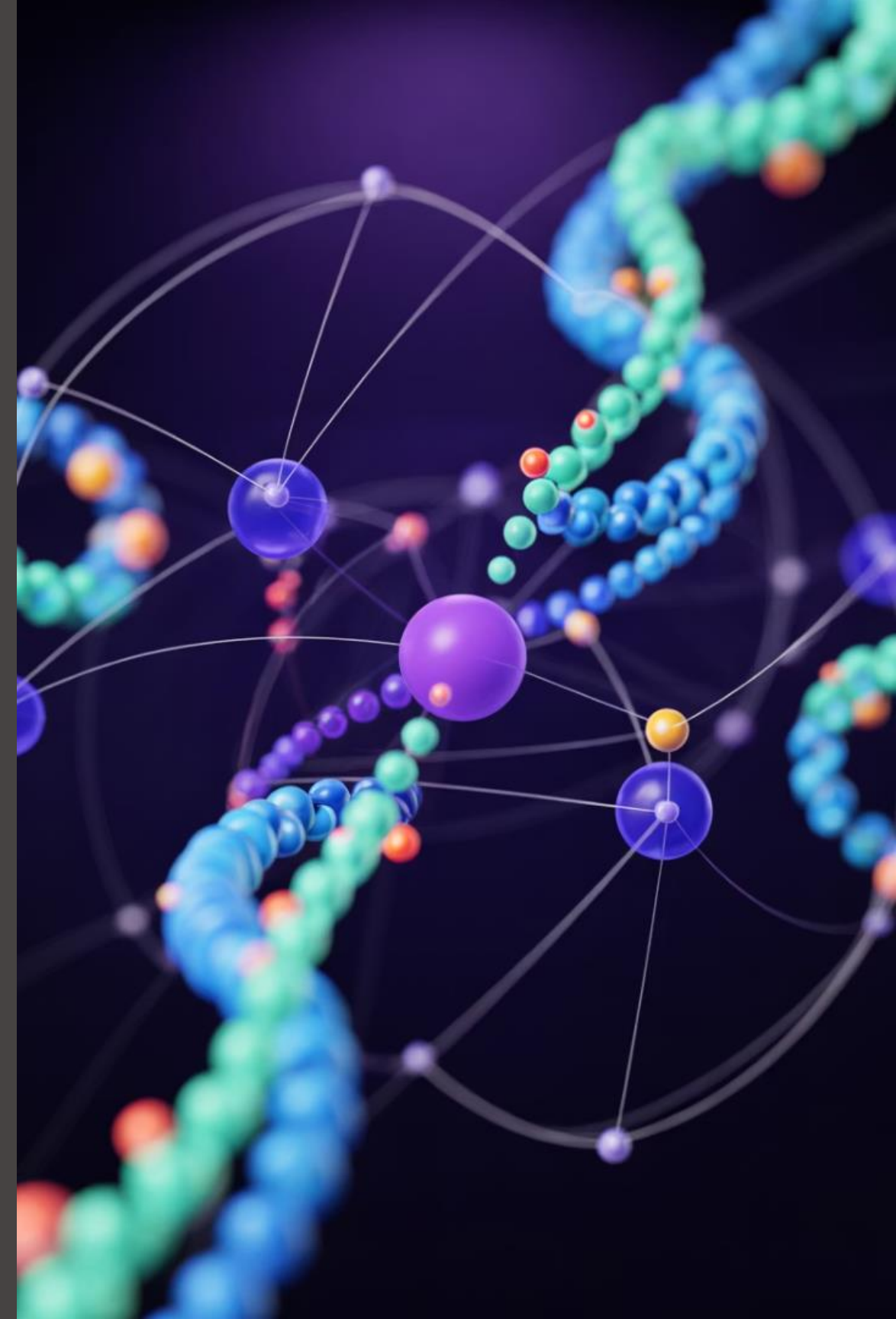
Le « masque jetable » remplit cette condition, car pour un message chiffré donné, **tous** les messages de même longueur sont possibles, rendant toute interprétation aussi probable qu'une autre.

Théorie de l'information de Shannon

Longueur de clé

Clé aussi longue que le message

Pour atteindre cette sécurité parfaite en théorie, il faut que la clé soit au moins aussi longue que le message. Si la clé est réutilisée pour un autre message, on perd la propriété d'imprévisibilité parfaite.





Théorie de l'information de Shannon

1 Notion d'entropie

Mesure l'imprévisibilité de l'information

2 L'entropie mesure l'imprévisibilité ou l'incertitude d'une source d'information.

Plus un message est « aléatoire » ou imprévisible, plus son entropie est élevée.

Si un texte contient beaucoup de redondances (par exemple, en français, des structures de phrases courantes), il est plus facile pour un attaquant de deviner une partie du contenu ou d'exploiter des régularités.

Évolution vers la cryptographie moderne



Des chiffres classiques aux algorithmes modernes

Les chiffrements classiques (César, Vigenère, etc.) sont aujourd'hui trop faibles pour la moindre utilisation sérieuse.

Les besoins (banque en ligne, e-commerce, télécommunications sécurisées, etc.) demandent des algorithmes bien plus robustes.



Évolution vers la cryptographie moderne



Algorithmes symétriques et asymétriques

Algorithmes symétriques

Symétriques : Comme le DES (aujourd'hui obsolète), Triple DES, AES, ChaCha20, etc. Ici, la même clé sert à chiffrer et à déchiffrer.

Algorithmes asymétriques

Asymétriques : Comme RSA, Diffie-Hellman, ECC (cryptographie à courbes elliptiques). On sépare la clé en deux moitiés : une clé publique (pour chiffrer) et une clé privée (pour déchiffrer).



Évolution vers la cryptographie moderne

1 Sécurité aujourd'hui

Robustesse mathématique : Ces algorithmes reposent sur des problèmes mathématiques difficiles (logarithme discret, factorisation de grands nombres, etc.).

2 Standardisation

Standardisation : L'important est d'utiliser des protocoles et des standards approuvés (TLS/SSL, IPSec, PGP, etc.) et des longueurs de clé suffisantes.



Cryptographie quantique et post-quantique



Cryptographie classique

Algorithmes traditionnels basés sur des problèmes mathématiques difficiles



Menace quantique

Les futurs ordinateurs quantiques pourraient casser certains algorithmes asymétriques actuels (RSA, ECC)



Cryptographie post-quantique

Des nouvelles primitives sont en cours de standardisation (algorithmes basés sur les réseaux euclidiens, par exemple)

