

Sécurité : une introduction

Mathieu Cunche¹

¹INSA-Lyon

1 Le cours

2 Principes de la sécurité

3 Introduction à la cryptographie

4 Conclusion

1 Le cours

2 Principes de la sécurité

3 Introduction à la cryptographie

4 Conclusion

4TC-CSC : Cryptographie et Sécurité des Communications

Objectifs :

- Principes fondamentaux de la cryptographie
- Mise en oeuvre de la cryptographie pour les communications sécurisées
- Limites de la cryptographie
- Enjeux éthiques associés également les limites de la cryptographie et les enjeux éthiques associés.

Le cours II

Les séances :

- Amphi de cours (3 x 2h) : Intro, Crypto, Protocoles
- TD Ethique (2*+2h)
- TD Usage crypto (2h*)
- TD Jeu de rôle RSA (2h)
- TD Stockage mots-de-passe (2h)
- TD PKI – infra. à clef publique (2*+2h)
- TD Communication/arpentage (2*+2h)
- TP HTTPS (4h)
- Amphi de présentation arpantage (2h)

1 Le cours

2 Principes de la sécurité

3 Introduction à la cryptographie

4 Conclusion

La sécurité : contextes



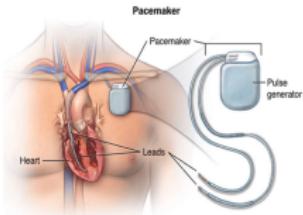
(a) Antivol



(b) Coffre-fort



(c) Carte bancaire



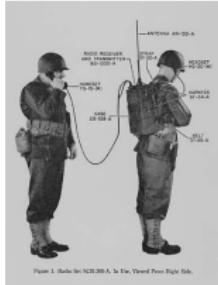
(d) Pacemaker



(e) Smartphone



(f) Messagerie



(g) Radio militaire



(h) Résistant

- Des données ou un système à protéger
 - Ex. : un **message** personnel
- Des propriétés de sécurité
 - Ex. : la **confidentialité** du contenu du message
- Des menaces pouvant compromettre ces propriétés
 - Ex. : **interception** du message par un attaquant
- Des moyens pour garantir ces propriétés
 - Ex. : le **chiffrement**¹ du contenu

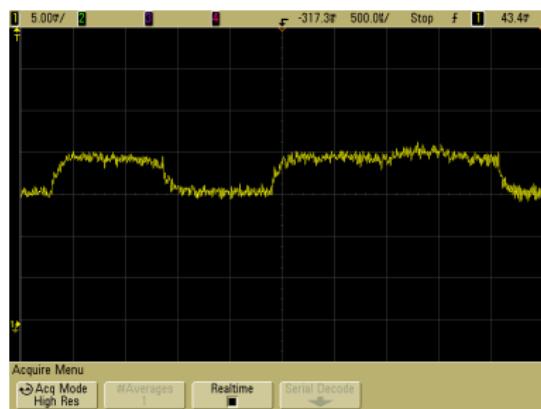
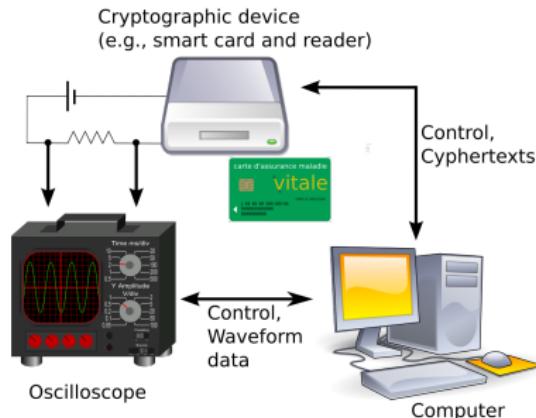
¹Abusivement désigné par *cryptage* par les néophytes.

Attaques : matériel

Analyse de consommation

Récupération d'un secret (ex.: clef) via l'analyse de la consommation électrique

- Le flot d'exécution dépend de la valeur de la clef (ex.: if $k[i]==1$)
- La consommation électrique dépend du flot d'exécution



By Audriusa. Recorded by student in ETH (Zurich) during system security laboratory work. - Own work, GPL,
<https://commons.wikimedia.org/w/index.php?curid=9762292>

By Mark Pellegrini. - Own work, LGPL/GFDL

Attaques : logiciel

Injection SQL

Utiliser une entrée *mal intentionnellement* formatée pour exécuter des actions non prévues

Exemple :

- Code préparant la requête :

```
1 txtUserId = getRequestString("UserId");
2 txtSQL= "SELECT * FROM Users WHERE UserId =" + txtUserId;
```

- Entrée *UserId* fournie par l'attaquant :

105; DROP TABLE Suppliers

- Résultat : suppression de la table Suppliers !

Source : https://www.w3schools.com/sql/sql_injection.asp

Attaques : logiciel

Buffer-overflow (Dépassement de tampon)

Écriture à l'extérieur de l'espace mémoire alloué à l'écriture. Permet de modifier des zones mémoires *sensibles* (ex. addr de retour, ou clef).

variable name	A								B
value	[null string]								1979
hex value	00	00	00	00	00	00	00	00	07 BB

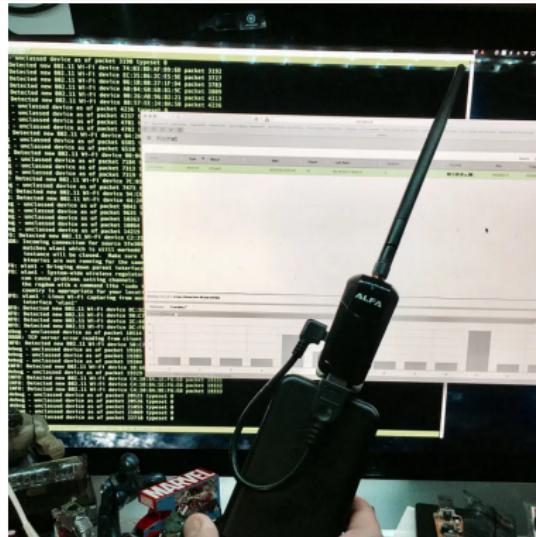
```
1 char A [8] = "";
2 unsigned short B = 1979;
3 ...
4 strcpy(A, "excessive");
5
```

variable name	A								B
value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856
hex	65	78	63	65	73	73	69	76	65 00

Attaques : réseaux I

Interception

Collecte de données transitant sur un canal de communication.



Source : <https://medium.com/@elkentaro/>

Attaques : réseaux II

Attaque par rejeux

Retransmission d'un message préalablement intercepté.

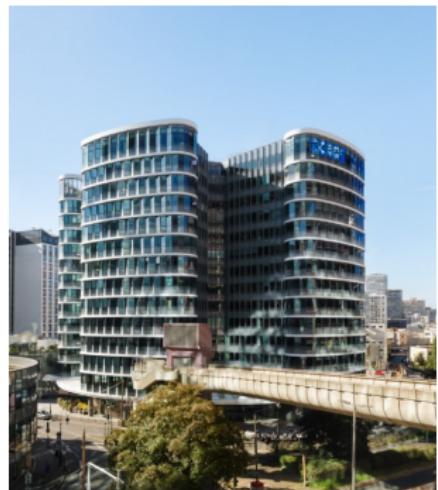
Exemple : déverrouillage de voiture



Source : plaxidityx.com

La sécurité : diversité des domaines

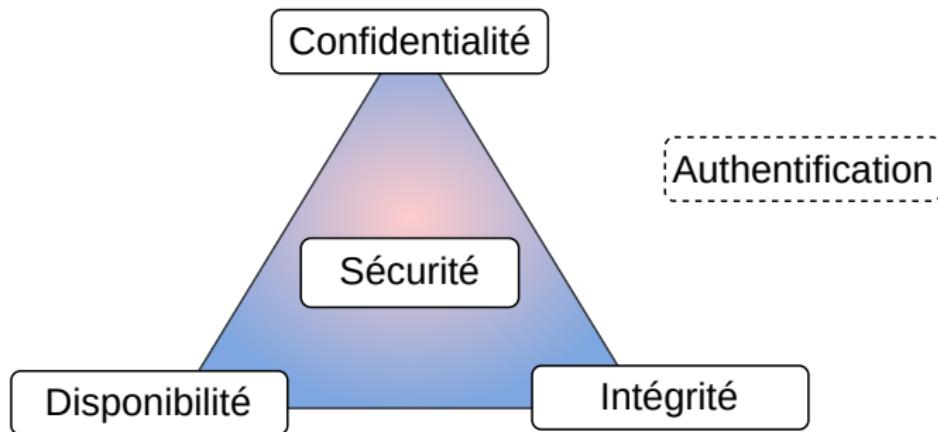
- Sécurité des systèmes informatiques (e.g. poste de travail)
- Sécurité des applications (e.g. site Web)
- Sécurité des bases de données
- **Sécurité des communications**
- ...



Campus Cyber @ Paris La Défense

La triade CIA

La triade CIA : les propriétés fondamentales de la sécurité informatique

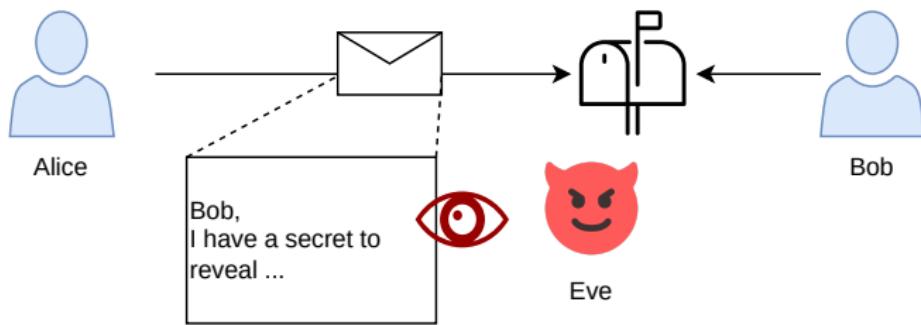


La triade CIA : Confidentialité

Confidentialité

Propriété d'une information à laquelle seuls ses destinataires peuvent avoir accès.

– *CyberDico de l'ANSSI*

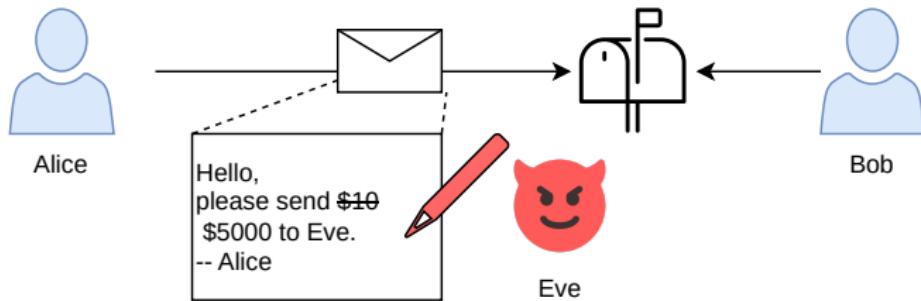


La triade CIA : Intégrité

Intégrité

Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime. Et que l'information est correcte et complète.

– *CyberDico de l'ANSSI*

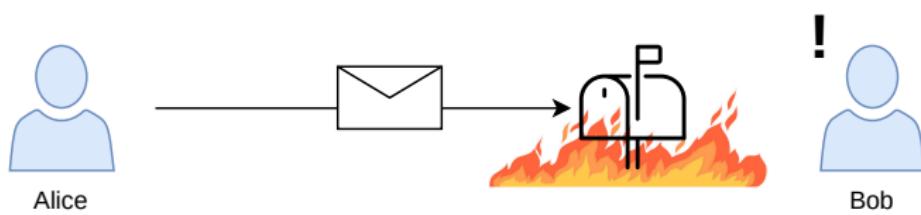


La triade CIA : Disponibilité

Disponibilité

Capacité à accéder à des données ou à un service au moment souhaité.

– *Guide formation cyber.gouv.fr*



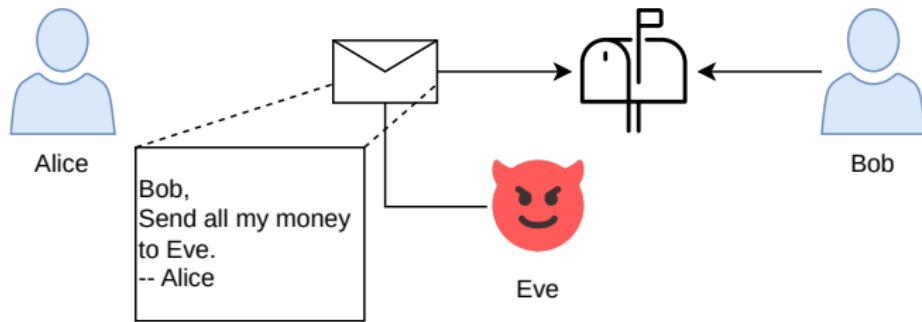
La triade CIA : Authenticité

Authenticité

L'information est attribuée à son auteur légitime.

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame.

– *CyberDico de l'ANSSI*



Moyens pour garantir la sécurité

- Moyens techniques
 - Ex. : L'accès au système est contrôlé à l'aide d'un moyen d'authentification (e.g. mot de passe)
- Moyens cryptographiques
 - Ex. : Les messages sont protégés par l'application d'une fonction de chiffrement
- Moyens organisationnels
 - Ex. : L'accès au système est désactivé lorsque la personne quitte l'organisation

1 Le cours

2 Principes de la sécurité

3 Introduction à la cryptographie

4 Conclusion

Chiffre en palissade et sytale spartiate

Chiffre en palissade (*RailFence*)

Plaintext

T H I S I S A S E C R E T M E S S A G E

Rail Fence

Encoding

key = 4

T				A				T			G
H			S	S		E	M		A	E	
I	I			E	R		E	S			
S				C			S				

Ciphertext

T A T G H S S E M A E I I E R E S S C S

2 3

Sytale spartiate



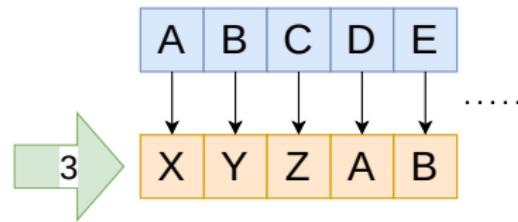
Ces chiffres mettent en oeuvre des **permutations** (les positions des caractères sont changées)

²<https://www.101computing.net/the-rail-fence-cipher/>

³CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=1698345>

Chiffre de César

Chiffre de César : substitution des lettres
après un décalage de l'alphabet par 3 positions



clair : On adore la crypto

chiffré : Rq dgruh od fubswr

Chiffre à décalage⁴ : la clef est la valeur du décalage

⁴<https://interstices.info/a-lattaque-des-codes-secrets/>

Chiffre de Vigenère

Vigenère (1586)

- Utilise une table de correspondance et un mot clef
- Le chiffré d'un caractère dépend du caractère correspondant de la clef



Figure: Blaise de Vigenère
Clef

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Chiffrement avec la clef "CLEF" :

clair : BONJOUR

chiffré : DZROQFV

César et Vigenère mettent en oeuvre des **substitutions** (les valeurs des caractères sont changées mais pas leurs positions)

Principe de Kerchoff I

Principe de Kerchoff

"La sécurité d'un chiffrement doit totalement dépendre du secret de la clé et non du secret de l'algorithme utilisé."
– La Cryptographie Militaire, 1883



Il est préférable que l'algorithme soit public. Cela permet son évaluation par des experts :

- la mise à l'épreuve de sa robustesse permet d'avoir confiance dans le système.

Principe de Kerchoff II

Contre-exemple contemporain : *Terrestrial Trunked Radio (TETRA)*

- Standard de radio numérique bi-directionnel
 - Utilisé dans 100 pays par services de secours, police ...
 - Algorithmes de chiffrement gardés secret
- Récupération des algo. de chiffrement par rétro-ingénierie (2023)
 - Leur analyse a révélé des faiblesses rendant possible le déchiffrement des communications
 - Certaines faiblesses apparaissent comme "intentionnelles" ...



Figure: Terminal TETRA du fabricant Airbus.

Chiffre Enigma I

- Machine électromécanique utilisée pour chiffrer et déchiffrer des messages
- Utilisée par l'armée allemande pendant la 2nde Guerre Mondiale
 - Armée de terre, armée de l'air, marine

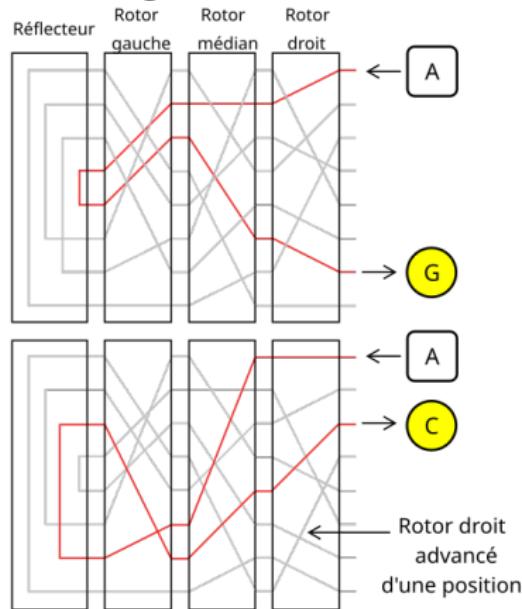


Figure: Machine Enigma I (Wikipedia – Alessandro Nassiri)

Chiffre Enigma II

Principe de fonctionnement de la machine Enigma :

- Un circuit électrique formé par
 - 3 rotors
 - 1 réflecteur
- La position des rotors change à chaque caractère
- Configuration initiale = clef



Fabriquer une machine Enigma

<https://cyber.org/find-curricula/pringles-can-enigma>

Chiffre Enigma III

Le cassage d'Enigma par les Alliés

- Cryptanalyse d'Enigma initiée avant la guerre par les polonais
- Attaque : énumération des configurations possibles
 - Une partie des messages pouvaient être deviné (e.g. "wetter" au début du message)
 - La configuration changeait tous les jours
 - 10^{15} configurations possibles ...
- Utilisation d'une machine : la *Bombe*
 - Conçue par Alan Turing @ Bletchley Park
 - Vitesse ≈ 15 opérations par seconde
 - Premier "ordinateur"
- Optimisations
 - Elimination des solutions impossibles : une lettre ne peut pas être chiffrée en elle-même



Figure: Alan Turing

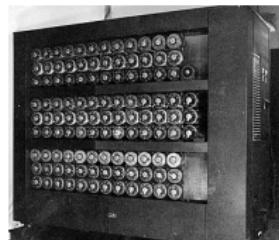


Figure: La *Bombe*

One-time-pad (Vernam) I

One-time-pad : le chiffrement parfait !

- Principe de fonctionnement

- Une clef aussi longue que le message
- On chiffre en XORant le message et la clef : $C = M \oplus K$
- On déchiffre en XORant le chiffré et la clef

Message	1	0	1	1	0	1	1	0
Clef	0	0	1	0	1	1	0	1
<hr/>								
Chiffré	1	0	0	1	1	0	1	1

One-time-pad (Vernam) II

- Une sécurité parfaite (Shannon)

- Considérons le i-eme bit : $C_i = M_i \oplus K_i$
- Quelle information peut-on déduire sur M_i à partir de C_i .

Cas où $C_i = 0$

$$P(M_i = 0 | C_i = 0) = P(C_i = 0 | M_i = 0)P(M_i = 0) / P(C_i = 0) \quad (1)$$

$$= P(K_i = 0)P(M_i = 0) / P(C_i = 0) \quad (2)$$

(3)

Mais aussi

$$P(C_i = 0) = P(C_i = 0 | M_i = 0)P(M_i = 0) + P(C_i = 1 | M_i = 1)P(M_i = 1) \quad (4)$$

$$= P(K_i = 0)P(M_i = 0) + P(K_i = 0) * (1 - P(M_i = 0)) \quad (5)$$

$$= P(K_i = 0) \quad (6)$$

One-time-pad (Vernam) III

D'où :

$$P(M_i = 0 | C_i = 0) = P(K_i = 0)P(M_i = 0)/P(K_i = 0) \quad (7)$$

$$= P(M_i) \quad (8)$$

$P(M_i = m | C_i = c) = P(M_i = m)$: la valeur du chiffré ne nous apprend rien sur la valeur du message \Rightarrow **Sécurité Parfaite !**

One-time-pad (Vernam) IV

Le *One-time-pad* a été utilisé pour sécuriser la ligne entre Washington et Moscou à partir de 1963 (après la crise des missiles de Cuba).

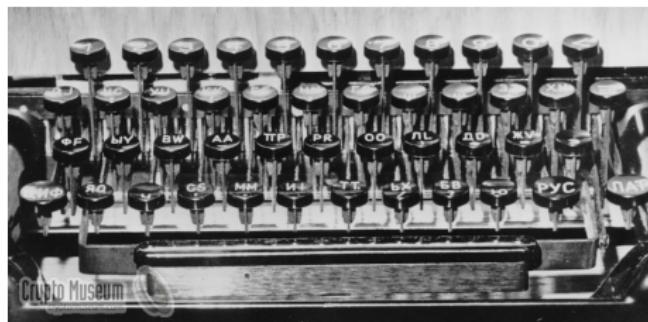


Figure: Keyboard of a Soviet teleprinter delivered to the Pentagon – Source: <https://www.cryptomuseum.com/crypto/hotline/>



Figure: Routes des liens radio et filaires entre Washington et Moscou – Source: <https://www.cryptomuseum.com/crypto/hotline/>

Cryptographie moderne

Liste (non-exhaustive) de cryptosystèmes :

- 1976 : Data Encryption Standard (DES)
- 1976 : Diffie-Hellman (DH)
- 1977 : RSA (Rivest–Shamir–Adleman)
- 2000 : Advanced Encryption Standard (AES)
- 2005 : Curve25519
- 2024 : Kyber

1 Le cours

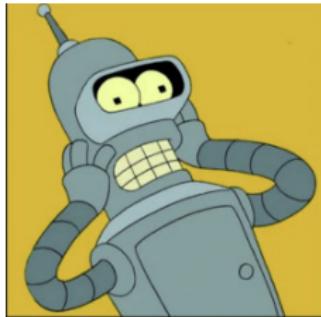
2 Principes de la sécurité

3 Introduction à la cryptographie

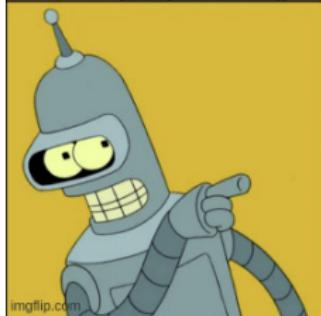
4 Conclusion

Vocabulaire I

On dit **crypter** chiffrer :

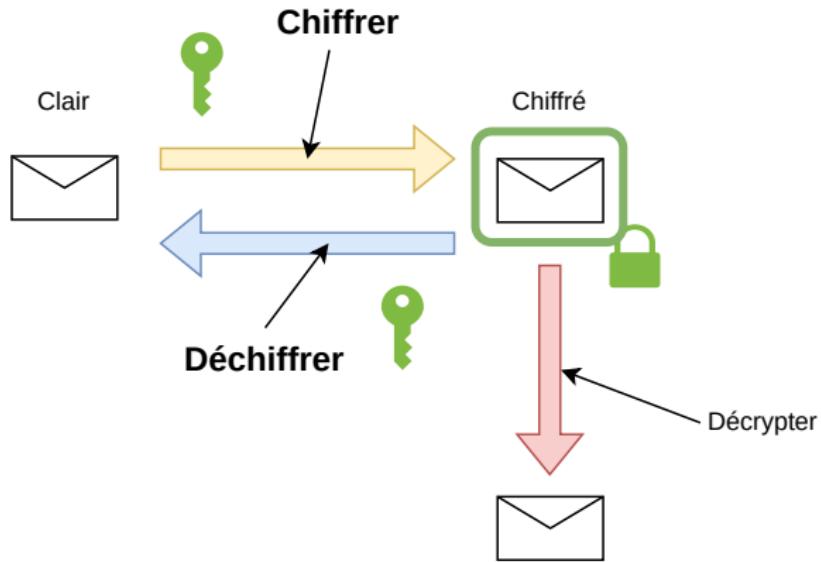


CRYPTER
CRYPTAGE
DÉCRYPTER



CHIFFRER
CHIFFREMENT
DÉCHIFFRER

Vocabulaire II



Vocabulaire III

Crypto veut dire Cryptographie

La **cryptographie** est la science des techniques de communication sécurisée en présence d'un adversaire.

La **cryptanalyse** est la science qui recherche les faiblesses des techniques cryptographiques afin de les contourner.

La **cryptologie** est l'union de la cryptographie et de la cryptanalyse.

"Crypto" Means "Cryptography," Not "Cryptocurrency"

I have long been annoyed that the word "crypto" has been co-opted by the blockchain people, and no longer refers to "cryptography." I'm not the only one.

Tags: [cryptocurrency](#), [cryptography](#)

Posted on November 22, 2021 at 8:40 AM • 94 Comments



Figure: Bruce Schneier, expert en sécurité, à propos du mot "Crypto".

⁵<https://www.schneier.com/blog/archives/2021/11/crypto-means-cryptography-not-cryptocurrency.html>

L'essentiel

- Propriétés : Confidentialité, Intégrité, Disponibilité, Authenticité
- Le secret ne doit pas résider dans l'algo, mais seulement dans la clef (Principe de Kerchoff)
- Techniques de chiffrement : substitution et permutation