



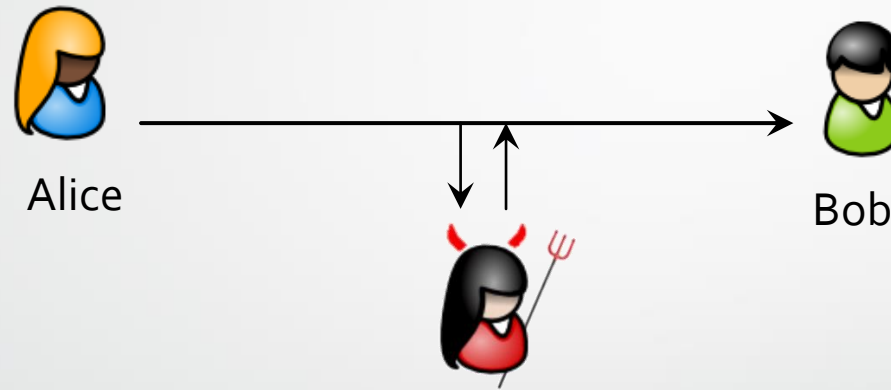
Sécurité et réseaux

Responsable : **Cristina ONETE**

Matériel : <https://community-iut.unilim.fr/course/view.php?id=2161>

Contact : cristina.onete@gmail.com

La cryptographie et la sécurité informatique



- Problème de base : Alice veut communiquer avec Bob
 - **Confidentialité** : l'Adversaire ne voit pas le contenu des messages entre Alice et Bob
 - **Authenticité** : Bob peut être sûr qu'un message qu'il reçoit vient d'Alice
 - **Intégrité** : Bob peut être sûr que le message reçu n'a pas été modifié par personne

La cryptographie met en place des outils pour assurer une communication sécurisée

Des outils cryptographiques variés

- Le chiffrement : assure la confidentialité (optionnellement l'authenticité)
- Les codes MAC, les signatures : assurent l'authenticité de messages
- Les fonctions de hachage : assurent l'intégrité contre un adversaire passif
- Des protocoles :
 - D'authentification
 - D'échange de clés
 - De vote électronique
 - Etc.

Ce module

- 1 CM, 4 TD, 6 TP
- **1 TP noté** (binome) = 25% de votre note
- **Le devoir (CC)** = le dernier TD, 75% de votre note

- Les TDs : comprendre les principes d'utilisation de qq. primitives & protocoles
- Les TPs : mettre en pratique vos connaissances crypto

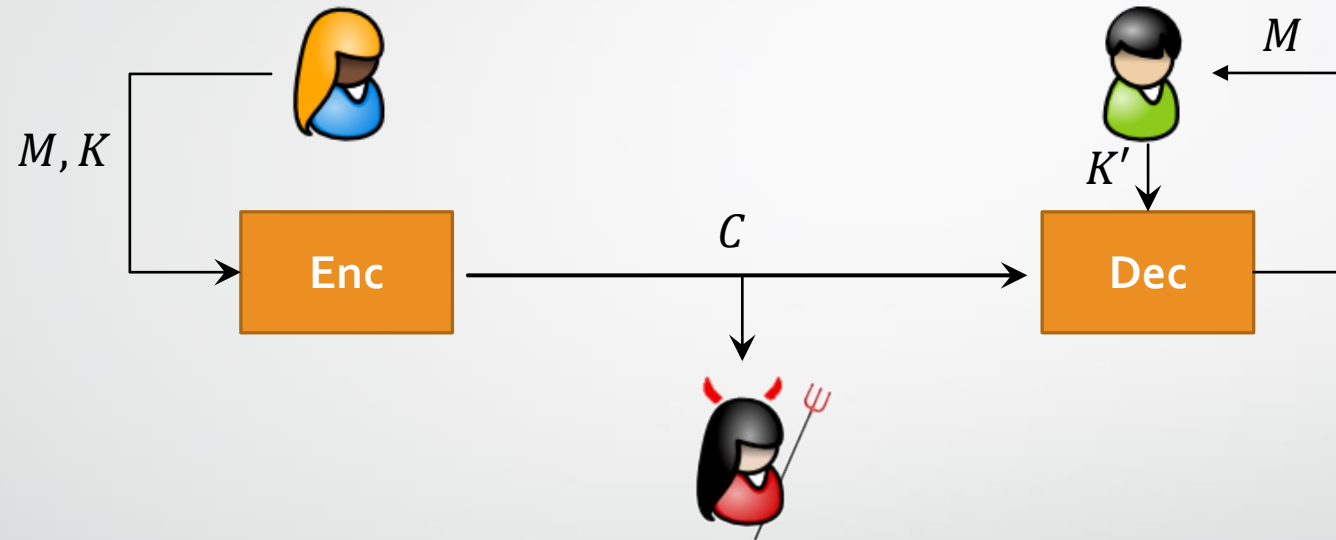
Aujourd'hui

- Le chiffrement en general
- Les schémas de chiffrement à clé symétrique
 - Le chiffrement de César
 - Le schema de Vigènere
 - Le chiffrement par bloc
- En TP : Implémentation du schema de Vigènere



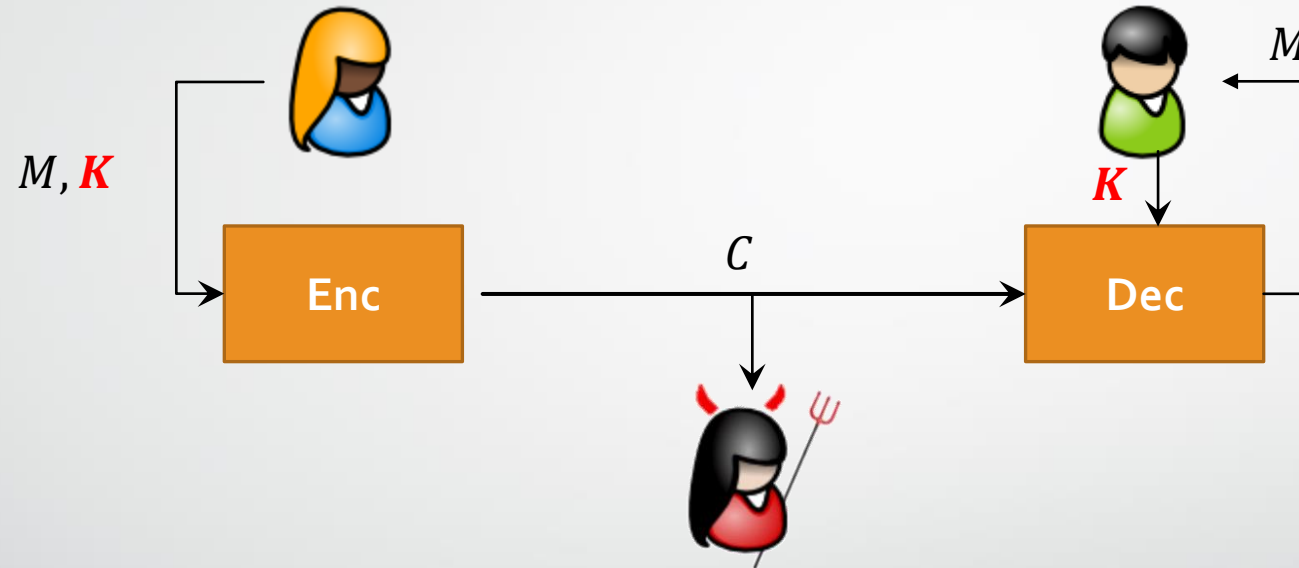
Les bases du chiffrement à clé symétrique

Les schémas de chiffrement : le principe



- Alice chiffre un texte clair (plaintext) M avec une clé K
- Elle obtient et envoie le message chiffré (ciphertext) C à Bob
- Bob déchiffre le chiffré C avec une clé K'
- On veut : 1) que Bob déchiffre C à M avec K'
2) que C ne donne aucun indice sur M

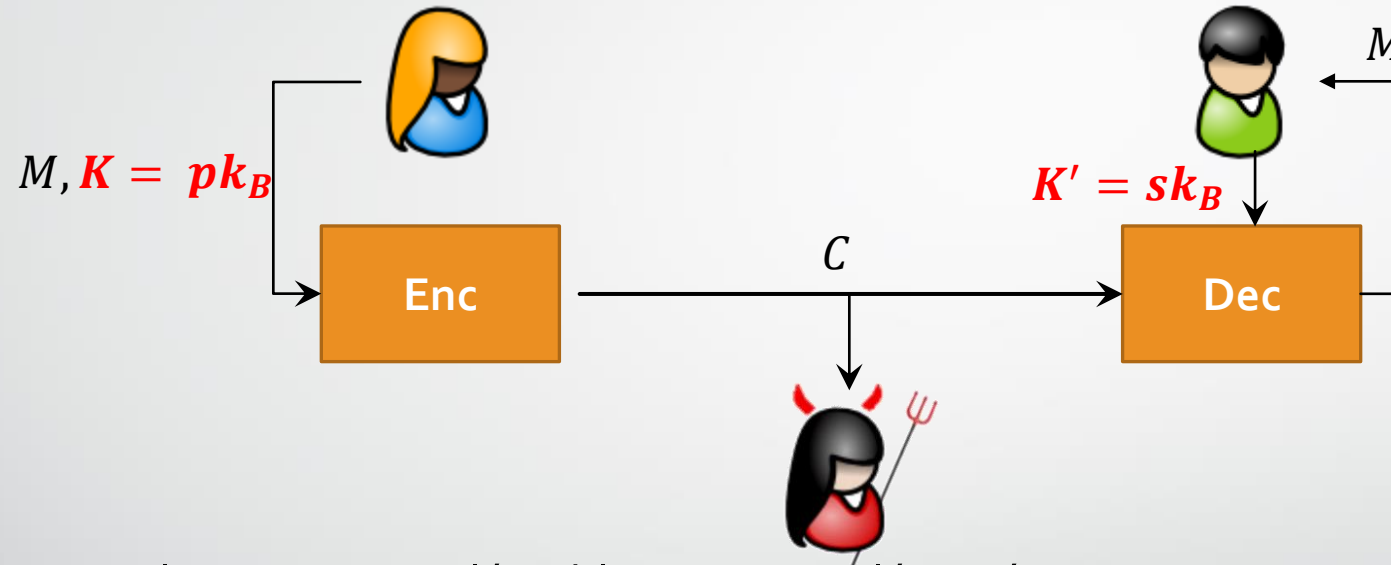
Le chiffrement à clé symétrique



- Le chiffrement et déchiffrement se font avec la même clé
- Attention : cela ne veut pas dire qu'on utilise le même algorithme !
- Le chiffrement est sécurisé tant que l'adversaire n'a aucune information sur la clé K
- Ce type de chiffrement est efficace mais présente aussi des inconvénients

Lesquels ?

Le chiffrement à clé publique



- Chaque utilisateur a une clé publique et une clé privée
- Bob publie sa clé publique
- Alice chiffre son message avec la clé publique de son interlocuteur
- Bob déchiffre avec sa clé secrète
- Le schema fonctionne tant que l'adversaire n'a aucune information sur la clé secrète de Bob

Exemples de chiffrement symétrique

- Le chiffre de César :
 - un système basé sur la permutation
- Principe :
 - chaque lettre de l'alphabet est permutée par un nombre de lettres
 - $A \rightarrow D, B \rightarrow E, C \rightarrow F$, etc.
- Le chiffre de César est un chiffrement à clé symétrique

Avec quelle clé ?

La cryptanalyse du chiffre de César

- Cryptanalyse = "casser" le chiffrement en regardant seulement l'algorithme
- Pour le chiffre de César : essayer de deviner la clé
 - Comment peut-on savoir si on a la bonne clé ?
- Attaque par "force brute" (brute force) :
 - Essayer toutes les possibilités jusqu'à trouver la valeur cherchée

Exemple

- Chiffrer/Déchiffrer avec la clé $K = 3$:

T	E	X	T	E	C	L	A	I	R
W	H	A	W	H	F	O	D	L	U

- Deviner la clé :
 - Déchiffrer pour toute clé possible
 - Probabilité de succès : $1/26$
 - Speed-up : les statistique de la langue (une lettre est toujours chiffrée de la même façon)

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

Les vulnérabilités du chiffre de César

- Un espace de clés très petit (26 possibilités pour un alphabet à 26 lettres)
- Comportement déterministe : lettres chiffrées de la même façon, toujours
- Une solution : le chiffre de Vigenere
 - La clé est un mot (disons de taille l)
 - On interprète chaque lettre de la clé et des messages comme un nombre entre 0 et 25
 - Si le texte clair est plus long que la clé, on répète la clé
 - On chiffre chaque lettre du texte clair avec une lettre de la clé
 - Le chiffrement est une addition mod 26, le déchiffrement est une soustraction mod 26

Le chiffrement/déchiffrement Vigènere

- Chiffrer avec Vigènere :
 - Message : TEXTECLAIR
 - Clé : CLEF
- Même lettre du chiffré ne veut pas dire qu'on a la même lettre dans le texte clair

T	E	X	T	E	C	L	A	I	R
19	4	23	19	4	2	11	0	8	17
2	11	4	5	2	11	4	5	2	11
C	L	E	F	C	L	E	F	C	L
21	15	1	24	6	13	15	5	10	2
V	P	B	Y	G	N	P	F	K	C

La cryptanalyse du chiffre de Vigènere

- Vigènere = plus difficile à casser que le chiffre de César
- Cependant, étant donné un chiffré assez long, on peut le faire
- La méthode de Kasiski :
 - Premier pas : trouver des répétitions dans le chiffré
 - A partir de cela, trouver la taille de la clé
 - Utiliser une attaque par dictionnaire pour trouver la clé

Cryptanalyse sur Vigènere : les répétitions

- Une répétition d'une lettre du chiffré peut être une coïncidence
- Mais si un fragment de quelques lettres se repète ?
- Ce qu'on cherche :

T	E	X	T	E	C	L	A	I	R
19	4	23	19	4	2	11	0	8	17
2	11	4	5	2	11	4	5	2	11
C	L	E	F	C	L	E	F	C	L
21	15	1	24	6	13	15	5	10	2
V	P	B	Y	G	N	P	F	K	C

T	E	X	T	E	C	L	A	I	R
19	4	23	19	4	2	11	0	8	17
2	11	4	2	11	4	2	11	4	2
C	L	E	C	L	E	C	L	E	C
21	15	1	21	15	6	13	11	12	19
V	P	B	V	P	G	N	L	M	T

Quelle est la différence entre les deux situations ?

Analyse

- Le même fragment du texte Claire (TE) chiffré avec les mêmes lettres de la clé (CL)
- Ceci veut dire que la distance entre les deux répétitions est un multiple de la taille de la clé
- Quelques répétitions peuvent être une coïncidence, mais le plus longue le texte répété, le plus probable qu'il ne s'agit pas d'une coïncidence

T	E	X	T	E	C	L	A	I	R
19	4	23	19	4	2	11	0	8	17
2	11	4	2	11	4	2	11	4	2
C	L	E	C	L	E	C	L	E	C
21	15	1	21	15	6	13	11	12	19
V	P	B	V	P	G	N	L	M	T

Cryptanalyse de Viginère

- 1) Méthode de Kasiski : trouver la taille de la clé
- 2) Utiliser une attaque par dictionnaire pour trouver la clé
 - Ceci veut dire essayer tous les mots d'un dictionnaire en déchiffrant à chaque fois pour trouver une solution
 - Comment sait-on quand il faut s'arrêter ?
- 3) Speed-up pour 2) : voire les statistiques de la langue -- e.g. la méthode de l'index de coïncidence https://en.wikipedia.org/wiki/Index_of_coincidence

Les faiblesses de Vigènere

- Quelles conditions favorisent la cryptanalyse de Vigènere ?
 - a) taille du chiffré ?
 - b) taille de la clé ?
 - c) des répétitions au niveau du texte clair ?
 - d) la langue du texte clair ?
 - e) le contenu du texte clair ?
 - f) les informations concernant le texte de l'adversaire ?
 - g) autre chose ? (Notamment ... ?)



Le chiffrement idéal et les chiffres par bloc

Un chiffre parfait

- Idéalement le chiffrement devrait "cacher" le texte clair complètement
- Ce type de chiffrement existe : le chiffement à masque unique (one-time pad)
- Principe :
 - A chaque chiffrement, choisir une clé aléatoire et chiffrer
 - La clé doit impérativement être aléatoire, unique, et de la même taille que le message

Le chiffrement à masque unique

- En général sur un alphabet binaire ($\{0,1\}$)
- Le chiffrement : l'opération de XOR (OR exclusif) = addition mod 2
- Mais on peut voir mieux sur un alphabet à 26 caractères
 - Le chiffrement = l'addition modulo 26
- Générer la clé : choisir chaque lettre de la clé aléatoirement, jusqu'à avoir une clé de la taille indiquée

B	L	O	C	K	C	I	P	H	E	R
P	R	Z	A	N	I	B	Q	T	C	S
R	C	N	D	Y	L	K	F	A	H	J

Meilleure attaque contre un tel chiffre

- Si la clé est non-aléatoire : utiliser les statistiques de la langue
- Si la clé est aléatoire mais se répète :
 - Etant donné $c_1 = m_1 \text{ XOR } k$ et $c_2 = m_2 \text{ XOR } k$ nous trouvons $m_1 \text{ XOR } m_2 = c_1 \text{ XOR } c_2$
 - Puis on utilise des statistiques pour trouver les mots
- Si la clé est aléatoire mais se répète, nous ne pouvons pas distinguer le texte clair d'un autre texte clair de la même taille !
 - **BLOCKCIPHER** + "**PRZANIBQTC**" = RCNDYLKFAHJ
 - **UNIVERSALLY** + "**XOEHUUSEPW**" = RCNDYLKFAH
 - **YETIMONSTER** + "**TYUVLXXNGC**" = RCNDYLKFAHJ

Les inconvénients de ce chiffre

- Est-ce qu'on utilise le chiffrement à masque unique dans la vraie vie ?
- Pourquoi pas ? Quels sont ses inconvénients selon vous ?

Le chiffrement symétrique moderne

- Deux types de méthodes : les chiffres par bloc et les chiffres par flot
- Le chiffrement par bloc :
 - Diviser le messages en plusieurs blocs d'une certaine taille
 - Chaque bloque chiffré avec un schéma (par exemple AES)
 - A partir des chiffrés des blocs, obtenir le chiffré final (mode d'opération)
- Le chiffrement par flot :
 - Générer une masque pseudo-aléatoire
 - Utiliser le chiffrement de type OTP pour un flot de messages

L'algorithme AES (variante Rijndael)

- Développé par Vincent Rijmen et Joan Daemen en 1998
- Opère sur des blocs de 128 bits avec une clé de taille variable (128, 192 ou 256)
- Le chiffrement de chaque bloc se fait en tours (rounds)
 - Le nombre de tours est 10, 12 ou 14, en fonction de la taille de clé
 - Une clé plus longue permet plus de tours
- 4 opérations sur chaque bloc :
 - SubBytes, ShiftRows, MixColumns -- sans utiliser la clé
 - AddRoundKey -- avec la clé

Structure du chiffrement

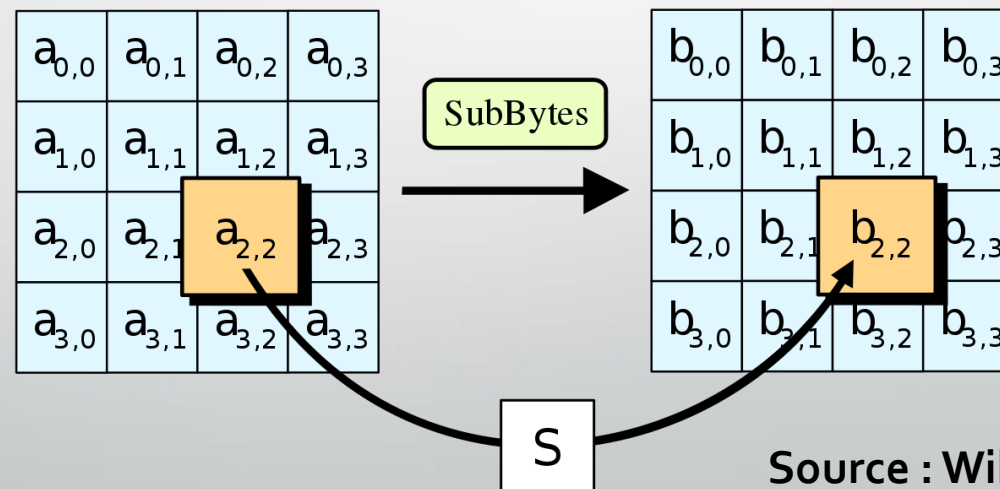
Input : 128 bits de texte clair, = 16 octets

- 1. L'expansion de clé** : à partir de la clé, obtenir une clé pour chaque tour + 1
- 2. Première addition de clé** : on fait l'XOR du bloc avec la clé
- 3. Les premiers tours** (9/10, 11/12, 13/14) :
 - SubBytes, ShiftRows, MixColumns, AddRoundKey
- 4. Le dernier tour** :
 - SubBytes, ShiftRows, AddRoundKey

Output : 128 bits de chiffré

SubBytes

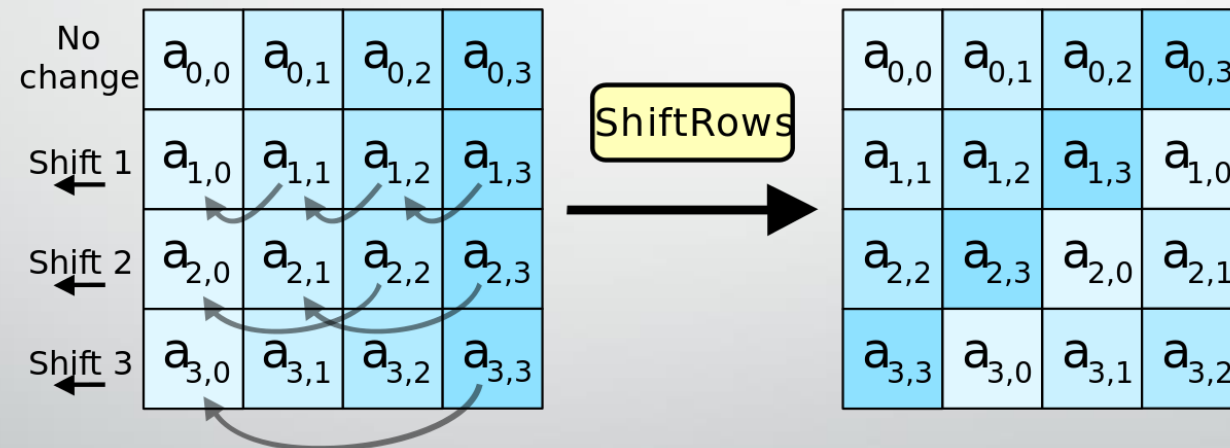
- La seule opération non-linéaire
- On soustitue des octets du message par d'autres octets, selon un tableau S



Source : Wikipedia.org

ShiftRows

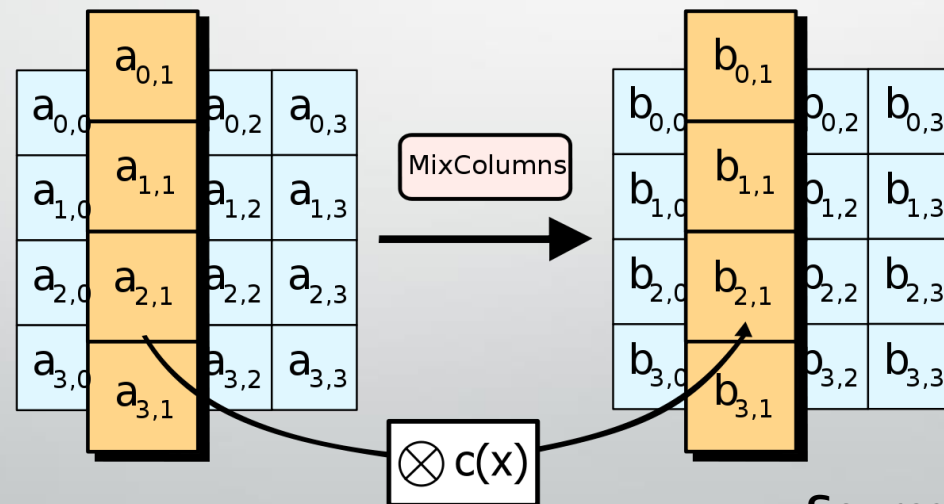
- Décale les éléments de chaque rang par un nombre variable de positions



Source : Wikipedia.org

MixColumns

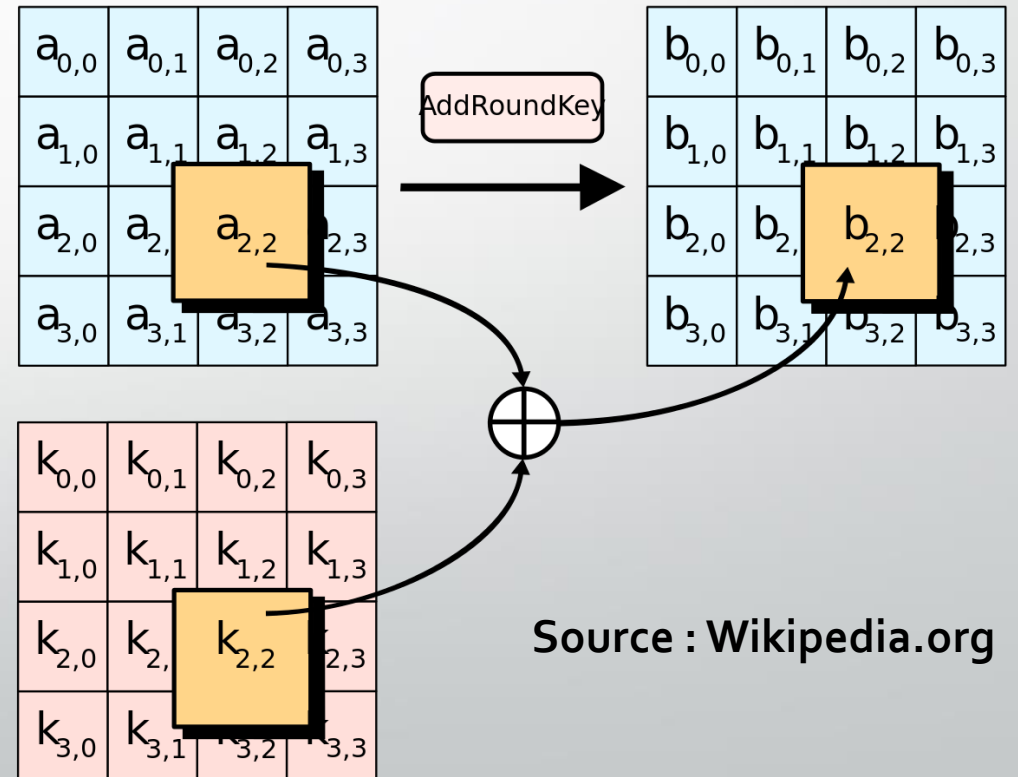
- Utiliser une transformation lineaire (donnée par une matrice 4×4) pour transformer chaque colonne



Source : Wikipedia.org

AddRoundKey

- En utilisant XOR on combine la matrice d'octets avec la clé du tour



Source : Wikipedia.org

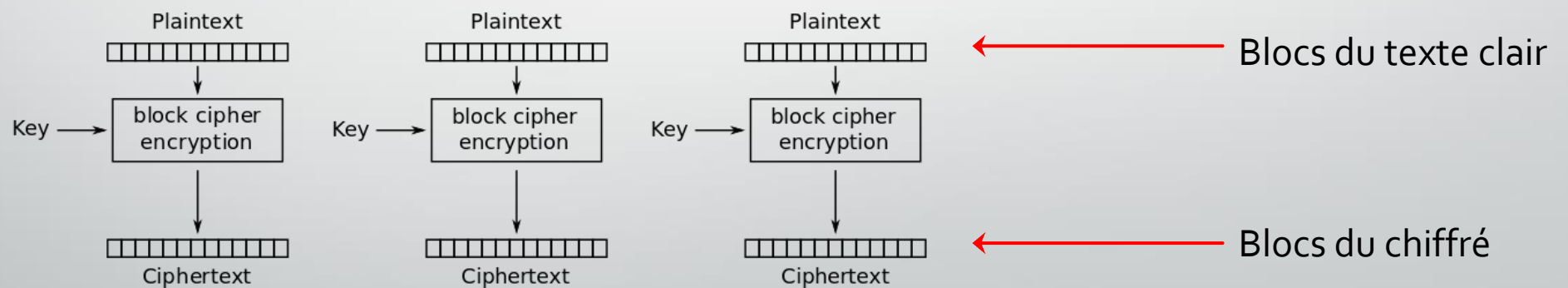
La sécurité d'AES

- A ce jour, AES reste le meilleur chiffre par bloc qu'on connaît
- Les seules attaques qu'on connaît exploitent :
 - Soit des faiblesses d'implémentation (attaques par des canaux auxiliaires)
 - Soit des faiblesses de choix de clé (related-key attacks)
- Attention : ceci est vrai pour le chiffrement de chaque bloc, individuellement

Comment chiffrer des messages à plusieurs blocs ?

Le mode d'opération d'un chiffre par bloc

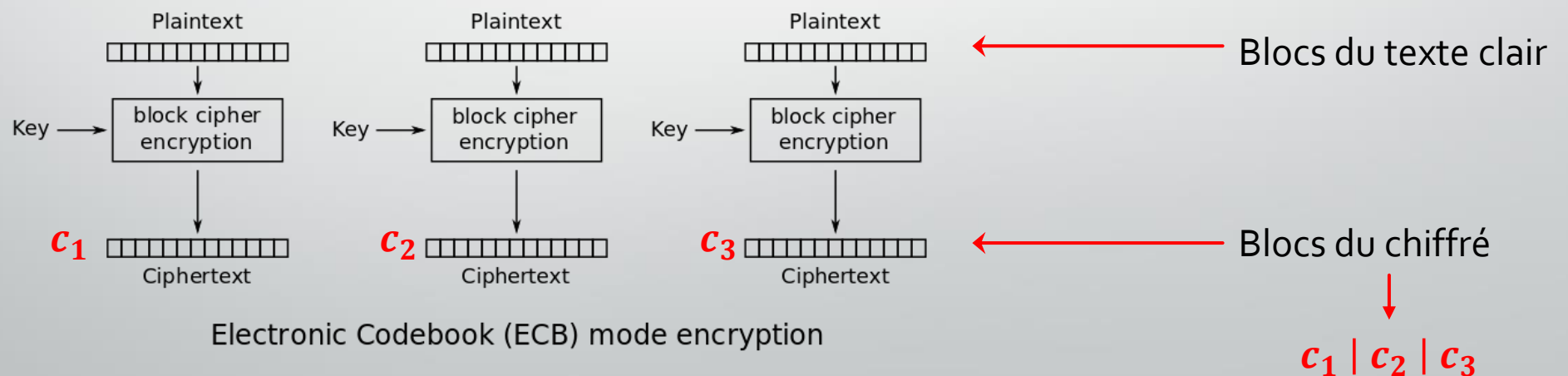
- Indique comment les chiffrés des blocs individuelles donnent le chiffré final
- Un mauvais mode d'opération peut casser la sécurité du chiffré obtenu
 - Malgré la sécurité du schéma de chiffrement utilisé



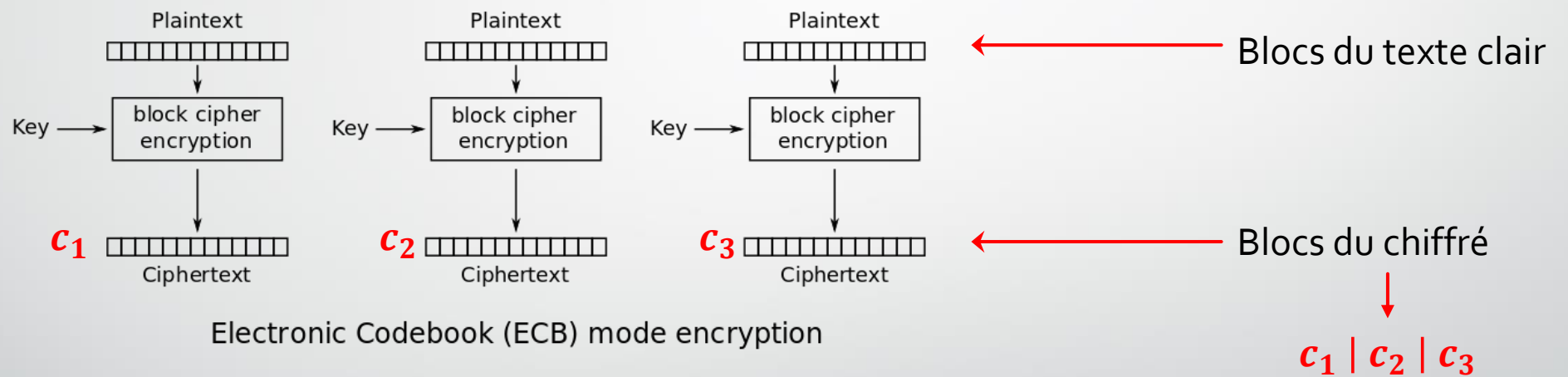
Electronic Codebook (ECB) mode encryption

Le mode d'opération d'un chiffre par bloc

- Indique comment les chiffrés des blocs individuelles donnent le chiffré final
- Un mauvais mode d'opération peut casser la sécurité du chiffré obtenu
 - Malgré la sécurité du schéma de chiffrement utilisé



Problèmes du mode ECB

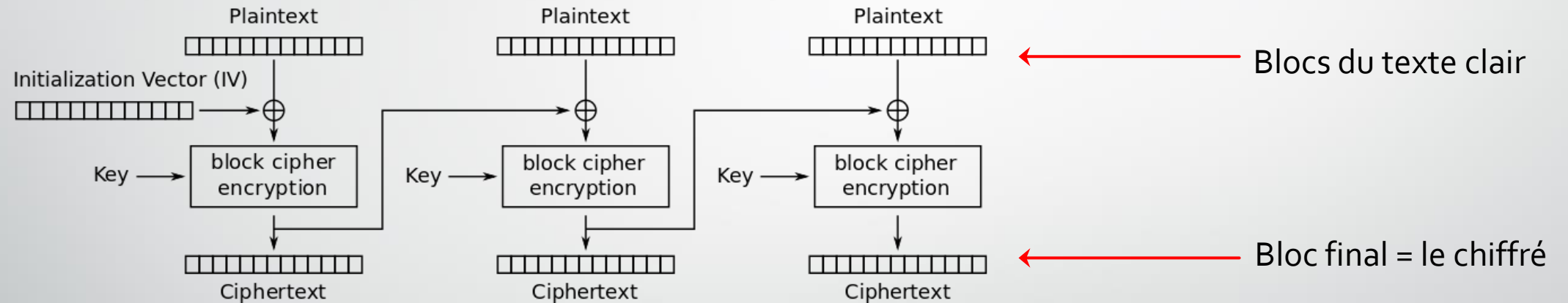


Source : Wikipedia.org

- Ce mode d'opération n'est pas du tout sécurisé

Pourquoi pas ?

Le mode CBC

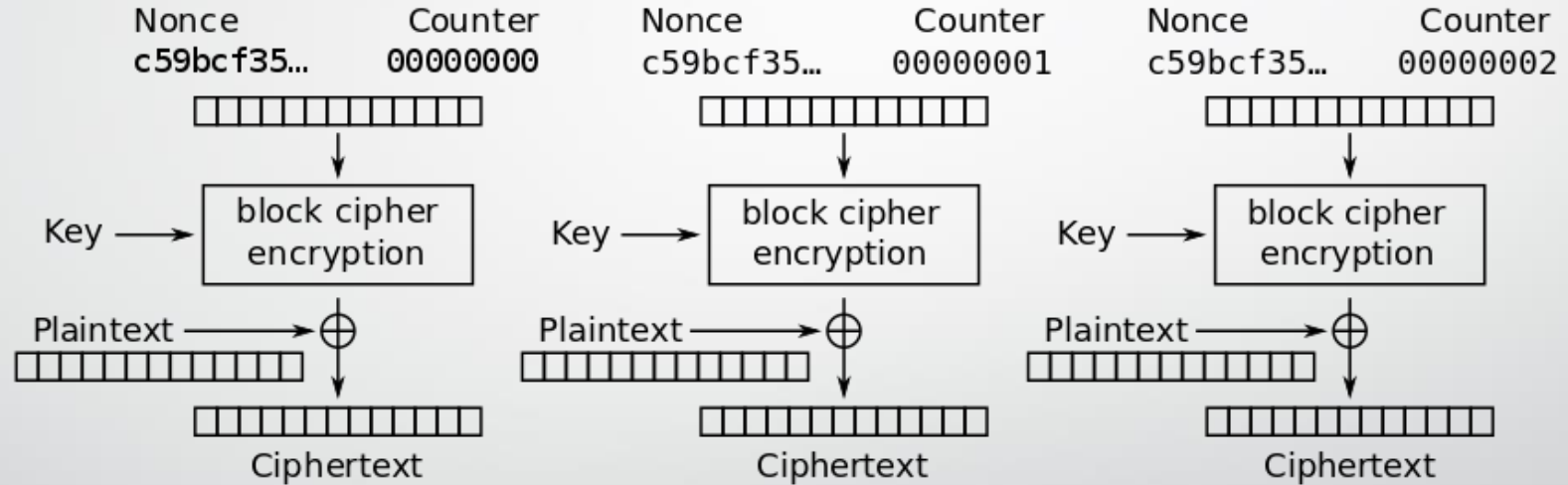


Cipher Block Chaining (CBC) mode encryption

Source : Wikipedia.org

Mieux que ECB, mais moins populaire à cause des attaques contre une utilisation particulière dans le protocole TLS/SSL

Le mode compteur (CTR)

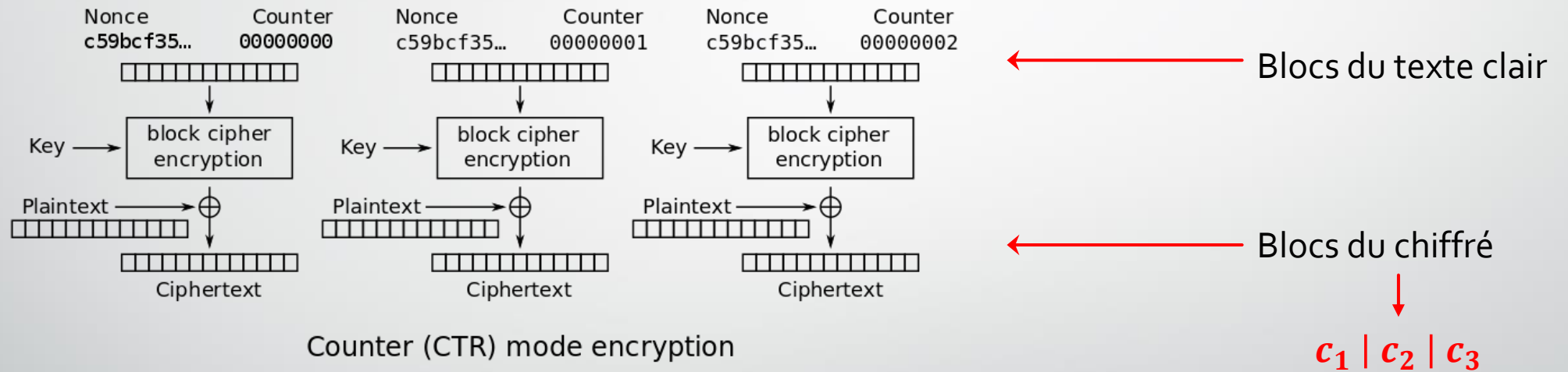


Counter (CTR) mode encryption

Source : Wikipedia.org

Le mode le plus utilisé actuellement est le mode GSM, une variante du mode CTR

Le mode compteur (CTR)



Source : Wikipedia.org

Qu'est-ce que a change par rapport au mode ECB ?