IUT ANNECY
UNIVERSITÉ SAVOIE MONT BLANC

Cryptographie et sécurité

Cours 1: cryptographie symétrique

Mickaël Bettinelli
(mickael.bettinelli@univ-smb.fr)

Slides par Mickaël Bettinelli et Nhan Duc Nguyen (université de Oulu)

Prérequis et objectifs

Connaissances nécessaire pour ce cours:

- Faire des opérations avec les modulos

Connaissances et compétences à acquérir à la fin du cours

- Comprendre les congruences
- Faire des opérations sur un ensemble $\mathbb{Z}/n\mathbb{Z}$
- Fonctionnement général du chiffrement symétrique
- Fonctionnement des chiffrements par bloc et par flot
- Capacité à réutiliser les chiffrements vus dans ce chapitre

Cours interactif

1. Connectez vous au quizz
2. Choisissez votre pseudo (= nom de famille + prénom)
3. Répondez aux questions
4. Chaque bonne réponse vous rapporte des points
5. Un classement des participants est effectué à la fin du questionnaire
6. Chaque étudiant recevra un bonus de point sur sa moyenne proportionnel à son score dans le questionnaire (max ⅓)

Connectez vous avec votre téléphone sur:

https://quizizz.com/

Game code:

Sommaire

- Pourquoi la cryptographie ?
- Vue d'ensemble
- Arithmétique modulaire
  - Relation de congruence
  - $\mathbb{Z}/n\mathbb{Z}$
- Quelques chiffrements historiques
- Les chiffrements modernes
  - Par flot
  - Par bloc
  - Quelques exemples
- En résumé

Les menaces


IOT SECURITY RISKS
01 INDUSTRY
There is already an account of a hacked German steel mill, which caused massive damage to the facility.
02 CARS
Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.
03 VIDEO CAMERAS
The wireless networks used for transferring video signals can be insecure.
04 CYBER-WARFARE
It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.
05 POWER GRIDS
Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.
06 BUILDINGS
As more buildings become more connected, the risk for exploits increases.
07 CITIES
Few cities engage in regular cybersecurity testing, and many have weak security controls in place.
08 MEDICAL DEVICES
The security used in many medical devices and hospitals lags behind that used in many other industries.
09 AIR TRAVEL
Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.
10 RETAIL
In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.
CAMERAS CAN BE EXPLOITED
Even video cameras, which are intended to improve security, can be hacked.
CONNECTIVITY OFFERS NEW RISKS
As cars and industrial facilities become increasingly connected to the cloud, security risks increase.
ATTACKS LIKELY UNDER-REPORTED
It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.
AIRPLANES CAN BE HACKED
Software vulnerabilities have been identified in several commercial aircraft.
Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.
MALWARE DESIGNED FOR WARFARE
POWER GRIDS ARE VULNERABLE
The utility and building industries are increasingly vulnerable to software attacks and software bugs that can cripple infrastructure.
NEW RISKS FOR CITIES AND BUILDINGS
HOSPITALS ARE ALREADY TARGETS
There are already examples of hospitals that have been shut down by ransomeware attacks. Many medical devices are also insecure.

Les menaces

- Le message ne doit pas être compréhensible de tous
- Il ne doit pas avoir été modifié entre l’envoie et la réception
- Il doit être envoyé à la bonne personne, et on doit pouvoir être certain que l'émetteur est bien celui que l’on pense
- L’émetteur ne doit pas pouvoir réfuter avoir envoyé un message

Les services de la cryptographie

- Confidentialité: le message n’est pas lisible par tout le monde
- Intégrité: le message n’est pas modifiable par un tier
- Authentification: l’émetteur et le récepteur sont clairement identifiés
- Non-répudiation: l’émetteur ne peut réfuter avoir envoyé le message

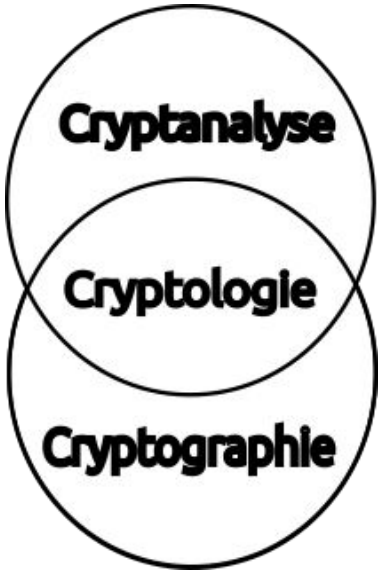
Introduction

Quelques définitions:

- **Cryptographie**: *ensemble de méthodes pour sécuriser l'information et les communications numériques.*

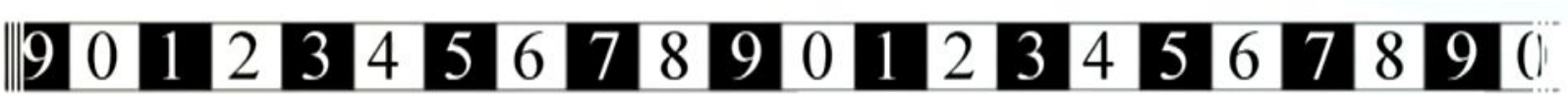
- **Cryptanalyse**: *consiste à casser ces méthodes les méthodes de cryptographie.*

- **Cryptologie**: *Cryptographie + Cryptanalyse.*



Relation de congruence

Introduction

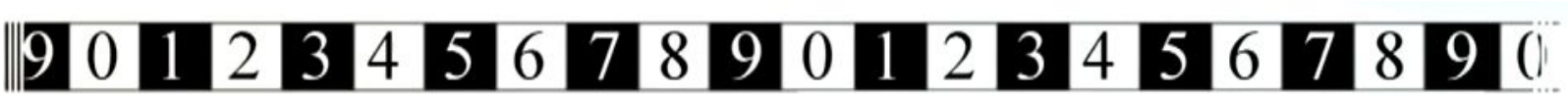


Représentation en bande:

- Lors d'une addition, le "surplus" retourne au début de la bande
- Exemples:
  - $\dot{7} + \dot{7} = \dot{4}$
  - $\dot{9} + \dot{3} = \dot{2}$

Relation de congruence

Relation de congruence



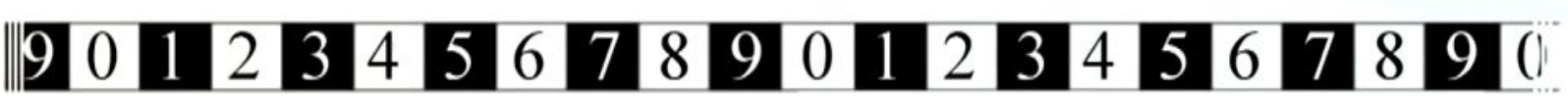
Si deux chiffres ***a*** et ***b*** sont sur la même case, on dit qu'ils sont congru modulo 10

Exemple:

- 2 et 12 sont congrus modulo 10
- 7 et 17 sont congrus modulo 10

Relation de congruence

Relation de congruence



Si deux chiffres ***a*** et ***b*** sont sur la même case, on dit qu'ils sont congru modulo 10

Cela signifie que:

- ***a*** et ***b*** ont le même chiffre
- ***a*** et ***b*** ont le même reste dans la division par 10
- ***a*** - ***b*** est un multiple de 10

On le note: a ≡ b [10]

Relation de congruence

Théorème.

Soit $n \in \mathbb{N}$, $n > 1$. Soient a et $b \in \mathbb{Z}$, on dit que a et b sont congrus modulo n lorsque $a - b$ est multiple de n.

On note alors $a \equiv b\ [n]$

Autrement dit:

$\exists\ k \in \mathbb{Z},\ a = b + kn$

Exemple: pour $17 \equiv 11\ [3]$, 17(a) = 11(b) + 2(k) * 3(n)

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$

Exemples.

- $10 \equiv 10\ [3]$

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$

Exemples.

- $10 \equiv 10\ [3]$
- $6 \equiv 3\ [3]$ et $9 \equiv 6\ [3] \Rightarrow 9 \equiv 3\ [3]$

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow aa' \equiv bb'\ [n]$

Exemples.

- $10 \equiv 10\ [3]$
- $6 \equiv 3\ [3]$ et $9 \equiv 6\ [3] \Rightarrow 9 \equiv 3\ [3]$
- $15 \equiv 10\ [5]$ et $5 \equiv 10\ [5] \Rightarrow 75 \equiv 100\ [5]$

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow aa' \equiv bb'\ [n]$
- $a \equiv b\ [n]$ si et seulement si $b \equiv a\ [n]$

Exemples.

- $10 \equiv 10\ [3]$
- $6 \equiv 3\ [3]$ et $9 \equiv 6\ [3] \Rightarrow 9 \equiv 3\ [3]$
- $15 \equiv 10\ [5]$ et $5 \equiv 10\ [5] \Rightarrow 75 \equiv 100\ [5]$
- $8 \equiv 6\ [2]$ si et seulement si $6 \equiv 8\ [2]$

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow aa' \equiv bb'\ [n]$
- $a \equiv b\ [n]$ si et seulement si $b \equiv a\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow a + a' \equiv b + b'\ [n]$

Exemples.

- $10 \equiv 10\ [3]$
- $6 \equiv 3\ [3]$ et $9 \equiv 6\ [3] \Rightarrow 9 \equiv 3\ [3]$
- $15 \equiv 10\ [5]$ et $5 \equiv 10\ [5] \Rightarrow 75 \equiv 100\ [5]$
- $8 \equiv 6\ [2]$ si et seulement si $6 \equiv 8\ [2]$
- $8 \equiv 2\ [2]$ et $10 \equiv 4\ [2] \Rightarrow 18 \equiv 6\ [2]$

Relation de congruence

Théorème.

Soient a et $b \in \mathbb{Z}$, Les principales propriétés des congruences sont:

- $a \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow aa' \equiv bb'\ [n]$
- $a \equiv b\ [n]$ si et seulement si $b \equiv a\ [n]$
- $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow a + a' \equiv b + b'\ [n]$
- $a \equiv b\ [n]$ et $k \in \mathbb{N} \Rightarrow a^k \equiv b^k\ [n]$

Exemples.

- $10 \equiv 10\ [3]$
- $6 \equiv 3\ [3]$ et $9 \equiv 6\ [3] \Rightarrow 9 \equiv 3\ [3]$
- $15 \equiv 10\ [5]$ et $5 \equiv 10\ [5] \Rightarrow 75 \equiv 100\ [5]$
- $8 \equiv 6\ [2]$ si et seulement si $6 \equiv 8\ [2]$
- $8 \equiv 2\ [2]$ et $10 \equiv 4\ [2] \Rightarrow 18 \equiv 6\ [2]$
- $4 \equiv 2\ [2]$ et $k = 2 \Rightarrow 4^2 \equiv 2^2\ [2]$

Introduction d’une activité

Activité *1, 2, Tous*:

- Réfléchissez individuellement à ces questions pendant - **3mn**
- Comparez vos réponses avec l’un de vos voisins, convainquez-le que vous avez raison ! - **3mn**
- Mise en commun des réponses, des binômes sont interrogés - **2mn**

Quelques exemples

Vrai ou Faux ?

- $19 \equiv 23\ [2]$
- $488 \equiv 68\ [6]$
- $8 \equiv -3\ [11]$
- $14 + 33 \equiv 23\ [12]$
- $8 * 15 \equiv -1\ [11]$
- $11 * 16 \equiv 4\ [12]$
- $6 * 26 \equiv 7\ [20]$

Activité *1, 2, Tous*:

- Réfléchissez individuellement à ces questions pendant - **3mn**
- Comparez vos réponses avec l'un de vos voisins, convainquez-le que vous avez raison ! - **3mn**
- Mise en commun des réponses, des binômes sont interrogés - **2mn**

Quelques exemples

Vrai ou Faux ?

- $19 \equiv 23\ [2]$ ——--> Vrai
- $488 \equiv 68\ [6]$
- $8 \equiv -3\ [11]$
- $14 + 33 \equiv 23\ [12]$
- $8 * 15 \equiv -1\ [11]$
- $11 * 16 \equiv 4\ [12]$
- $6 * 26 \equiv 7\ [20]$

Quelques exemples

Vrai ou Faux ?

- *19* ≡ *23* [*2*] ——--> Vrai
- *488* ≡ *68* [*6*] ——--> Vrai
- *8* ≡ *-3* [*11*]
- 14 + 33 ≡ *23* [*12*]
- 8 * 15 ≡ *-1* [*11*]
- 11 * 16 ≡ *4* [*12*]
- 6 * 26 ≡ *7* [*20*]

Quelques exemples

Vrai ou Faux ?

- $19 \equiv 23\ [2]$ ——--> Vrai
- $488 \equiv 68\ [6]$ ——--> Vrai
- $8 \equiv -3\ [11]$ ——--> Vrai
- $14 + 33 \equiv 23\ [12]$
- $8 * 15 \equiv -1\ [11]$
- $11 * 16 \equiv 4\ [12]$
- $6 * 26 \equiv 7\ [20]$

Quelques exemples

Vrai ou Faux ?

- $19 \equiv 23\ [2]$ ——--> Vrai
- $488 \equiv 68\ [6]$ ——--> Vrai
- $8 \equiv -3\ [11]$ ——--> Vrai
- $14 + 33 \equiv 23\ [12]$ ——--> Vrai
- $8 * 15 \equiv -1\ [11]$
- $11 * 16 \equiv 4\ [12]$
- $6 * 26 \equiv 7\ [20]$

Quelques exemples

Vrai ou Faux ?

- *19* ≡ *23* [*2*] ——--> Vrai
- *488* ≡ *68* [*6*] ——--> Vrai
- *8* ≡ *-3* [*11*] ——--> Vrai
- 14 + 33 ≡ *23* [*12*] ——--> Vrai
- 8 * 15 ≡ *-1* [*11*] ——--> Vrai
- 11 * 16 ≡ *4* [*12*]
- 6 * 26 ≡ *7* [*20*]

Quelques exemples

Vrai ou Faux ?

- *19* ≡ *23* [*2*] ——--> Vrai
- *488* ≡ *68* [*6*] ——--> Vrai
- *8* ≡ *-3* [*11*] ——--> Vrai
- 14 + 33 ≡ *23* [*12*] ——--> Vrai
- 8 * 15 ≡ *-1* [*11*] ——--> Vrai
- 11 * 16 ≡ *4* [*12*] ——--> Faux
- 6 * 26 ≡ *7* [*20*]

Quelques exemples

Vrai ou Faux ?

- *19* ≡ *23* [*2*] ——--> Vrai
- *488* ≡ *68* [*6*] ——--> Vrai
- *8* ≡ *-3* [*11*] ——--> Vrai
- 14 + 33 ≡ *23* [*12*] ——--> Vrai
- 8 * 15 ≡ *-1* [*11*] ——--> Vrai
- 11 * 16 ≡ *4* [*12*] ——--> Faux
- 6 * 26 ≡ *7* [*20*] ——--> Faux

$\mathbb{Z}/n\mathbb{Z}$

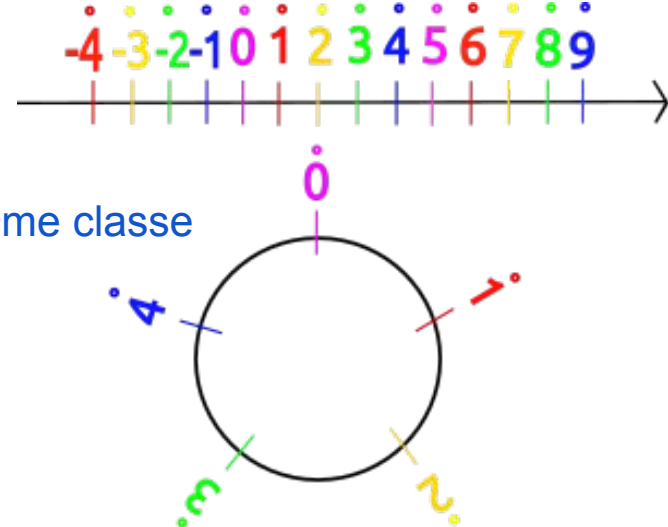
Théorème.

Soit $n \in \mathbb{N}$, $n > 1$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n.

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n - 1\}$ où $\dot{a}$ est l'ensemble des entiers congrus à a modulo n.

Exemple pour $\mathbb{Z}/5\mathbb{Z}$:

Tous les chiffres de même couleur appartiennent à la même classe

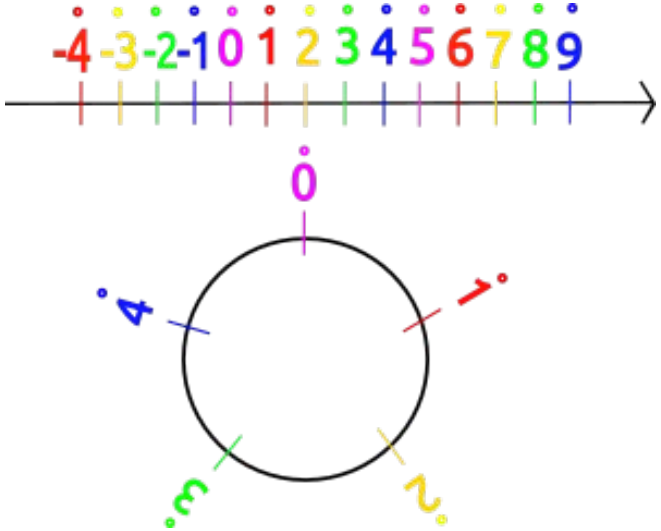


Additions et multiplications

Théorème.

Dans $\mathbb{Z}/n\mathbb{Z}$, si $x \dot{=} a$ et $y \dot{=} b$ alors $x \dot{+} y = a \dot{+} b$

Ceci est également vrai pour la multiplication !



Exemple sur $\mathbb{Z}/5\mathbb{Z}$:

- $\dot{3} + \dot{1} = \dot{4}$
- $\dot{8} + \dot{11} = \dot{19} = \dot{4}$
- $\dot{2} * \dot{2} = \dot{4}$
- $\dot{12} * \dot{3} = \dot{1}$

Exponentiation modulaire

En particulier avec l'algorithme RSA, on a souvent besoin de calculer des exponentiation modulaire tel que:

- $b^e \pmod m$ où b, e, m sont des entiers naturels.

b est appelé la base, e l'exposant et m le module.

→ Le calcul peut être très coûteux en mémoire, des algorithmes peuvent aider à le réaliser

Exemple. Calculer $c \equiv 4^7 \pmod{497}$

Exponentiation modulaire

Exemple. Calculer $c \equiv 4^7 \pmod{497}$

$4^2 \equiv 16 \pmod{497}$

$(4^2)^2 = 16^2 \equiv 256 \pmod{497}$

$4^5 = 256 * 4 \equiv 1024 \pmod{497} = 30 \pmod{497}$

$4^6 = 30 * 4 \equiv 120 \pmod{497}$

$4^7 = 120 * 4 \equiv 480 \pmod{497}$

$\Rightarrow c = 480$

Exponentiation modulaire

Historique

Quelques méthodes utilisées au fil du temps:

- Le carré de Polybe (-150 av. J-C)
- Chiffrement de César (58 av. J-C)
- La substitution polyalphabétique (1467)
- Le chiffre de Vigenère (1586)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Ces méthodes reposent sur la sécurité par l'obscurité

- Auguste Kerckhoffs (1883): la sécurité ne devrait pas reposer sur le secret de la méthode de chiffrement

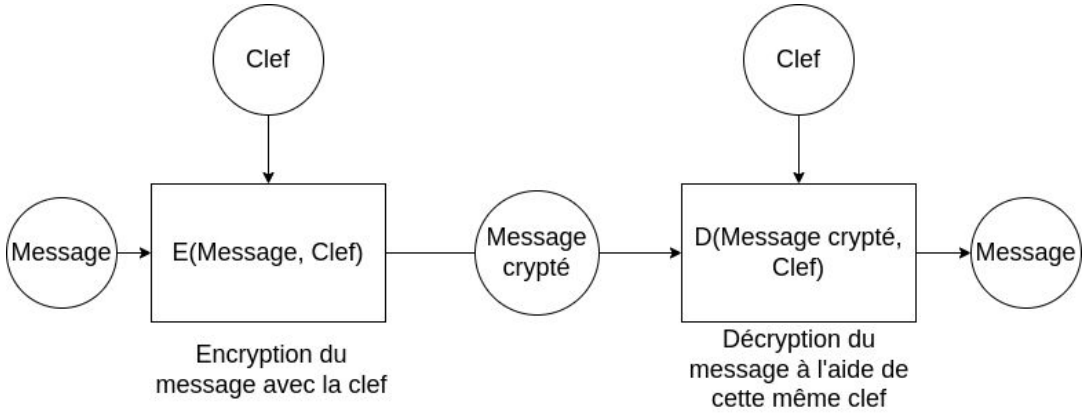
Historique

Les bonnes pratiques:

- Les cryptologues prônent la transparence en matière de processus et de conception des méthodes de cryptographie
- La méthode doit être bien documentée et son fonctionnement transparent
- Elle doit pouvoir être testée et utilisée par le plus grand nombre
- La sécurité passe par le coût computationnel plutôt que la méconnaissance de la méthode de chiffrement

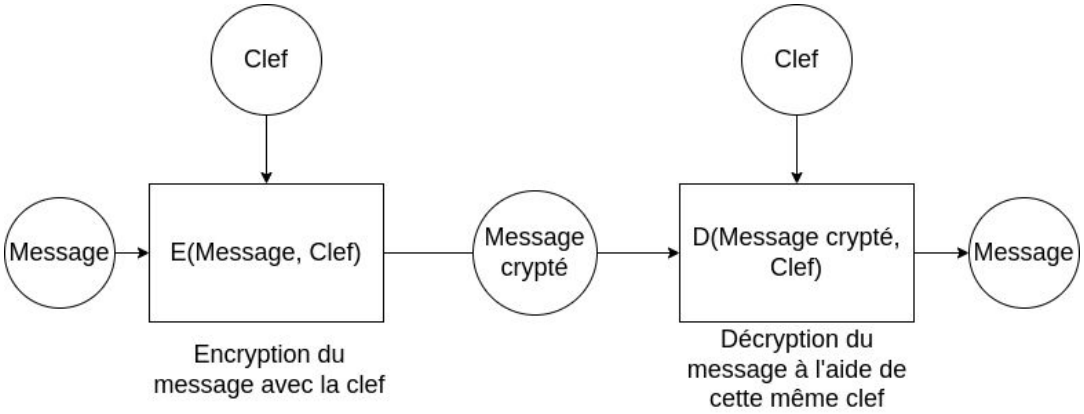
Vue d’ensemble

Système comportant une clef partagée devant être gardée secrète entre l’émetteur et le receveur.



1. L'émetteur crypte un message en utilisant une clef secrète
2. Le receveur le décrypte en utilisant cette même clef

Vue d'ensemble



Les clefs sont généralement entre ***128 bits*** et ***256 bits.***

Les clefs doivent être partagées entre les utilisateurs pour crypter et décrypter les messages.

La cryptologie repose largement sur les mathématiques.

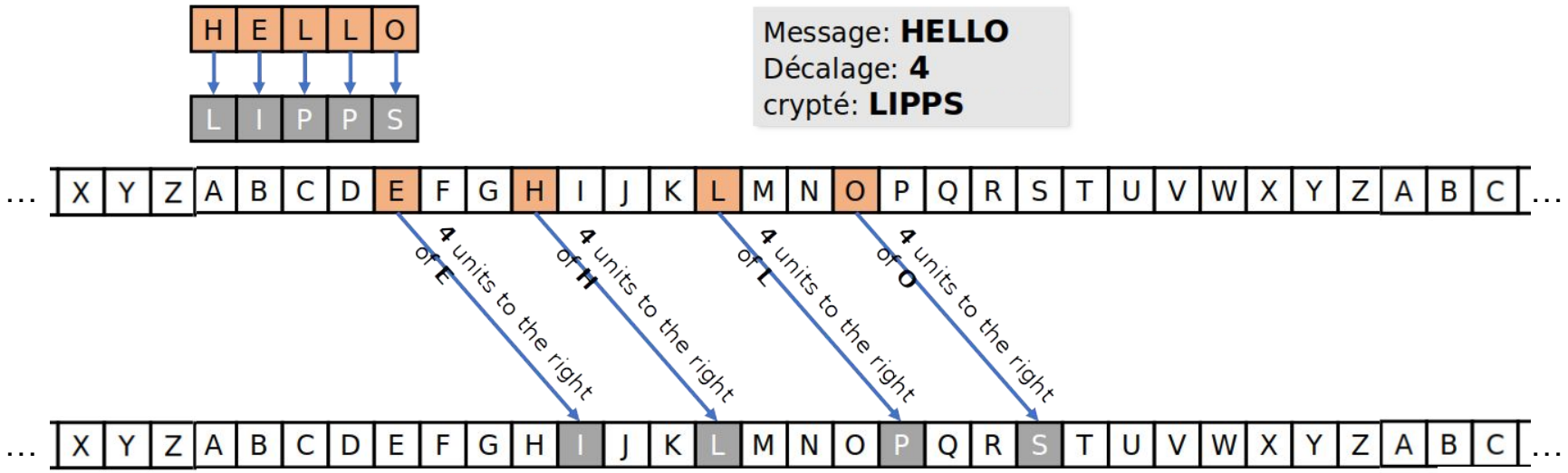
Les premières techniques

Chiffrement César

- Une des techniques les plus simples, inventée par Jules César
- Le message est crypté par un décalage de chaque lettre
- Le décryptage se fait en décalant les lettres dans l’autre sens

Les premières techniques

Chiffrement César



Les premières techniques

Chiffrement César 

Avantage:

- Très simple à comprendre et mettre en oeuvre

Inconvénients:

- Facilement cassable (par exemple par analyse de fréquence)

Les premières techniques

Analyse de fréquence:

- Chercher le **caractère** qui a le plus d'occurrence dans le texte crypté
- Comparer aux **lettres** les plus courantes dans la langue source du message
- Associer le **caractère** le plus courant à la **lettre** la plus courante

Fréquence des caractères[2] sur le corpus de Wikipédia en français

Rang	Caractère	Nombre d'occurrences	Pourcentage
1	e	115 024 205	12.10%
2	a	67 563 628	7.11%
3	i	62 672 992	6.59%
4	s	61 882 785	6.51%
5	n	60 728 196	6.39%
6	r	57 656 209	6.07%
7	t	56 267 109	5.92%
8	o	47 724 400	5.02%
9	l	47 171 247	4.96%
10	u	42 698 875	4.49%

Les premières techniques

Problème possible:

Un chat noir vit un grand garçon. Il avait faim. L'humain avait un hot-dog qui avait un parfum divin. L'animal noir sauta sur l'humain lui arrachant ainsi l'hot-dog. Mais un lapin biscornu sauta du saucisson faisant fuir l'humain. L'animal noir poussa un long cri aigu qui arracha l'animal biscornu du sol mouvant. Tout d'un coup, tout bascula. Un trou noir sauta sur l'hot-dog sourd provoquant un tourbillon d'imagination. La rotation du typhon fit mourir l'hot-dog. L'animal noir hurla pour bannir l'animal biscornu.

Fréquence des caractères[2] sur le corpus de Wikipédia en français

Rang	Caractère	Nombre d'occurrences	Pourcentage	
1	e	115 024 205	12.10%	
2	a	67 563 628	7.11%	
3	i	62 672 992	6.59%	
4	s	61 882 785	6.51%	
5	n	60 728 196	6.39%	
6	r	57 656 209	6.07%	
7	t	56 267 109	5.92%	
8	o	47 724 400	5.02%	
9	l	47 171 247	4.96%	
10	u	42 698 875	4.49%	

Les premières techniques

Chiffre de Vigenère

- La méthode de Vigenère résiste mieux à l'analyse de fréquence
- Elle utilise un mot entier pour décaler les lettres plutôt qu'un simple entier
- La clé est générée à partir d'un mot choisi, plus petite ou égale à la longueur du message. Elle se répète jusqu'à la fin du message à crypter.

Les premières techniques

Chiffre de Vigenère

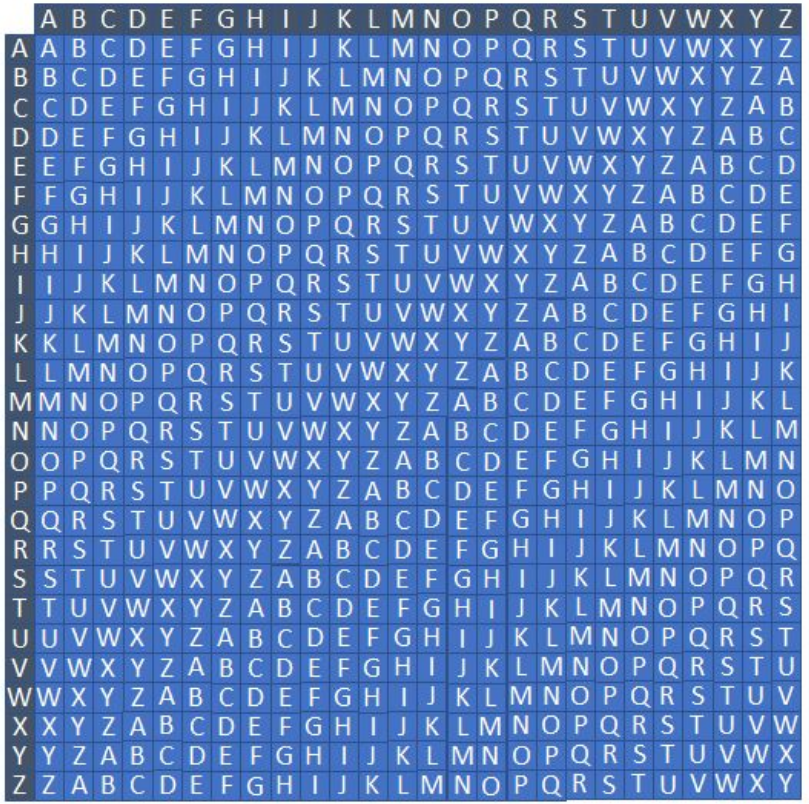
Message: **UNIVERSITY**
Clef: **APPLE**
Clef générée: **APPLEAPPLE**
Message crypté: **UCXGIRHXEC**

U	N	I	V	E	R	S	I	T	Y

cryptage

A	P	P	L	E	A	P	P	L	E

À partir de la table



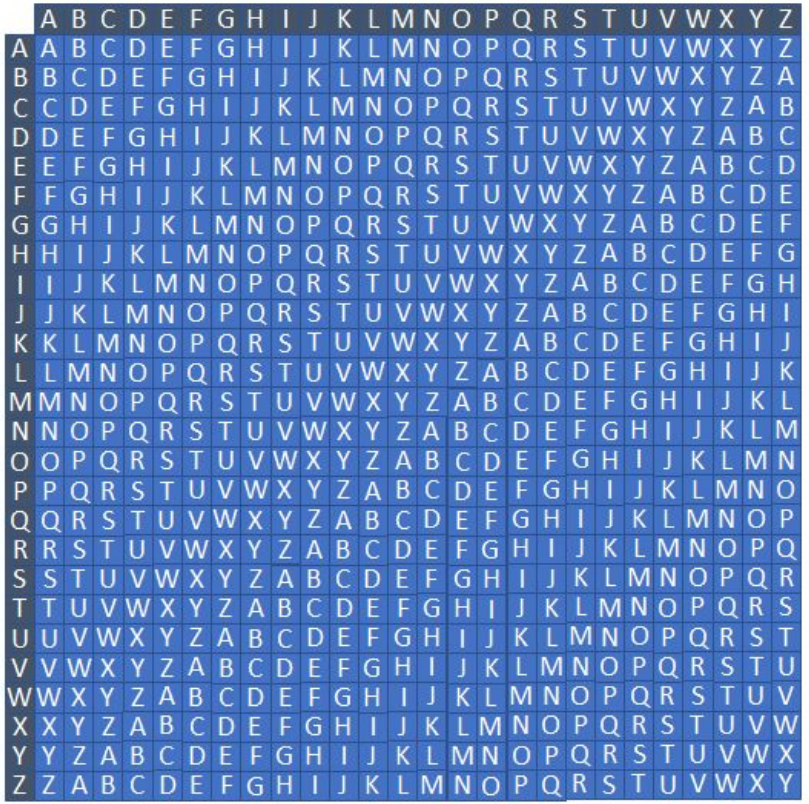
Les premières techniques

Chiffre de Vigenère

Message: **UNIVERSITY**
Clef: **APPLE**
Clef générée: **APPLEAPPLE**
Message crypté: **UCXGIRHXEC**

	U	N	I	V	E	R	S	I	T	Y
cryptage	U	C	X	G	I	R	H	X	E	C
	A	P	P	L	E	A	P	P	L	E

À partir de la table



Les premières techniques

Chiffre de Vigenère

Avantages:

- Plus résistante que celle de César

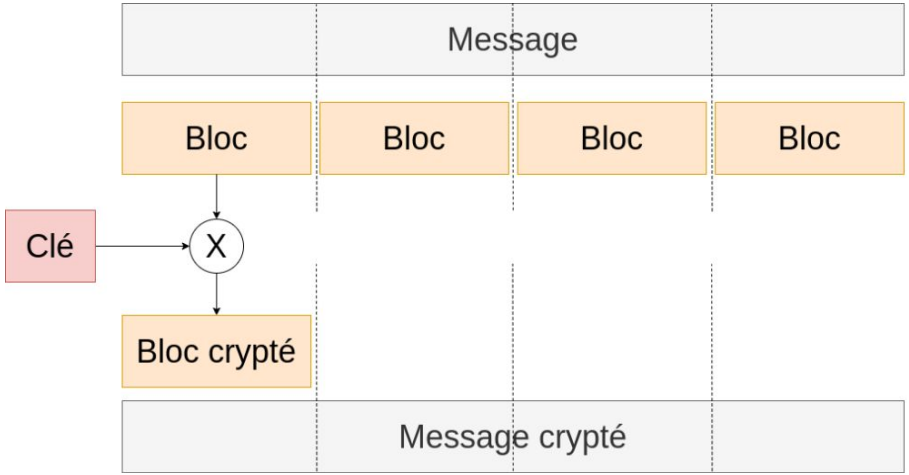
Inconvénients:

- L’analyse de fréquence est tout de même possible si l’on connaît la longueur de la clef

Chiffrement par bloc

Fonctionnement:

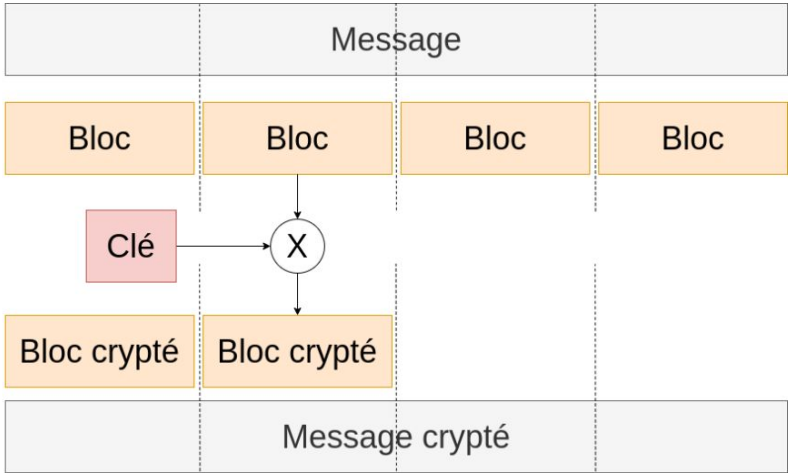
- Création d'une clé de taille fixe
- Division du message en blocs de la taille de la clé
- Chiffrement de chaque bloc avec la clé (par exemple avec un XOR)



Chiffrement par bloc

Fonctionnement:

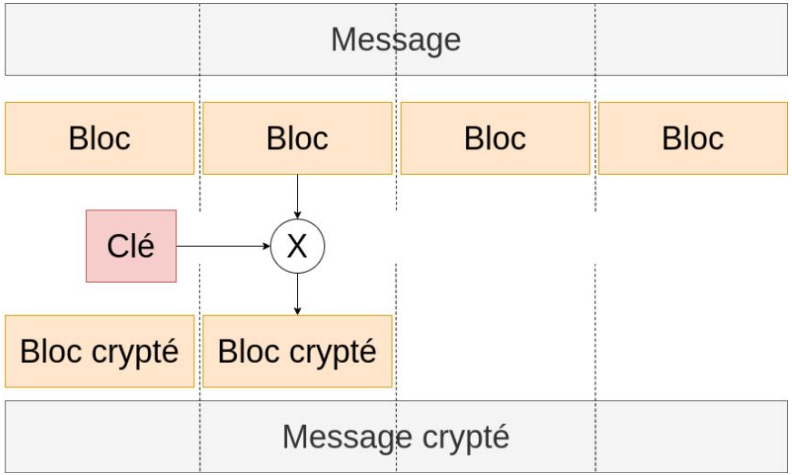
- Création d'une clé de taille fixe
- Division du message en blocs de la taille de la clé
- Chiffrement de chaque bloc avec la clé (par exemple avec un XOR)



Chiffrement par bloc

Inconvénient:

- Il existe des méthodes pour décrypter les chiffrements XOR !
- Certaines opérations peuvent laisser des motifs dans la chaîne chiffrée



Chiffrement par bloc

Chiffrement AES (Advanced Encryption Standard)

- La clef est dérivée en plusieurs versions (10 à 14 selon la taille de la clef)
- Chaque version de la clef chiffre une fois le bloc
- Chaque tour effectue plusieurs opérations matricielles permettant de “mélanger” les bits du message

Chaque opération peut s’inverser de manière à retrouver le message initial.

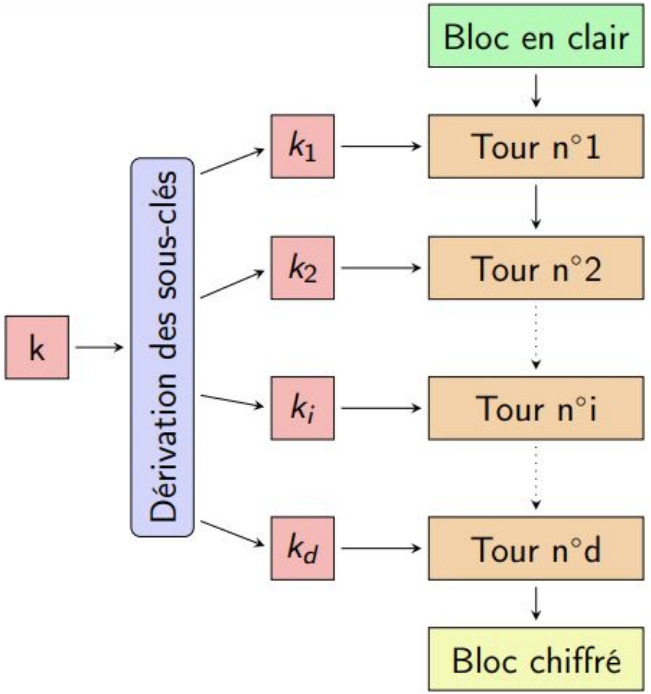


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

- Chiffrement à la volée sans attendre d’avoir tout le message
- Pas de découpage du message
- Chiffrement rapide
- Bien adapté aux applications temps réel

Chiffrement par flot

Fonctionnement:

- Utilisation d'un générateur de nombres pseudo-aléatoires
- Un XOR est opéré sur chaque bit du nombre généré avec un bit du message

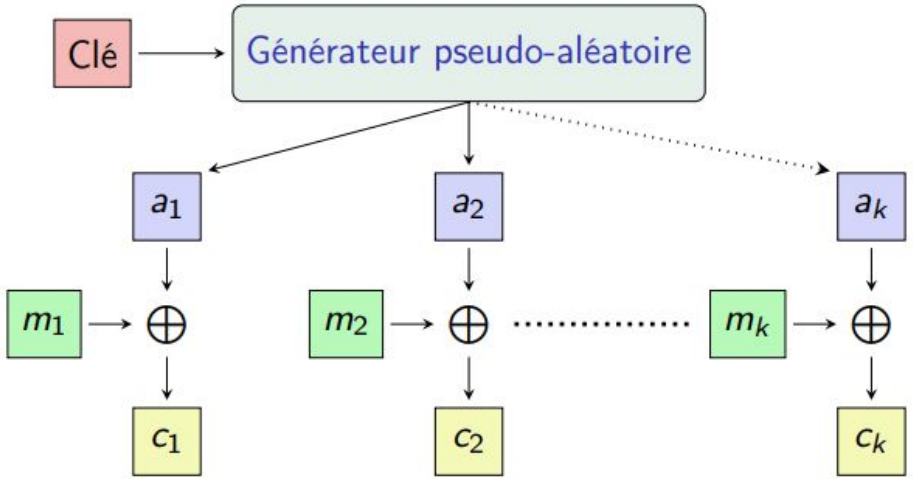


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Inconvénient: pour une même clé, le générateur créera les mêmes nombres pseudo aléatoires.

Peu pratique pour éviter les motifs dans le message crypté.

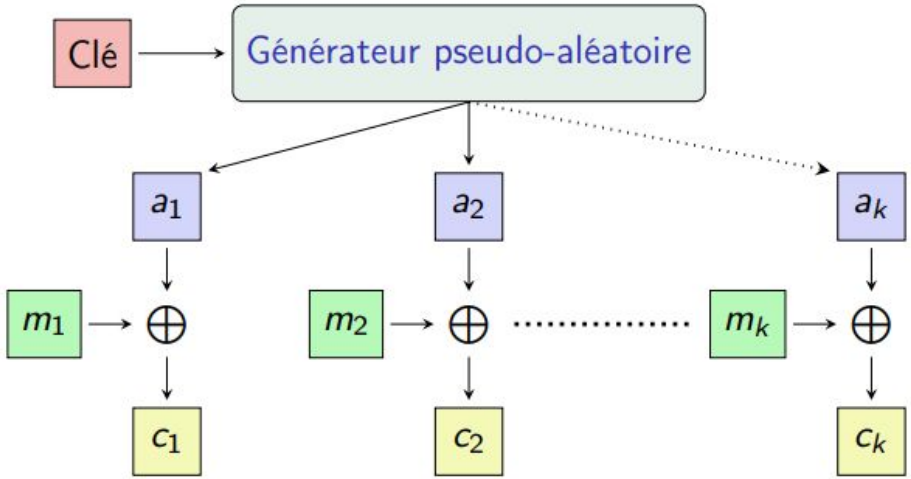


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Pour éviter cela, on ajoute un vecteur d'initialisation qui modifie le comportement du générateur:

VI = bloc de bits combiné avec le premier bloc de données lors d'une opération de chiffrement.

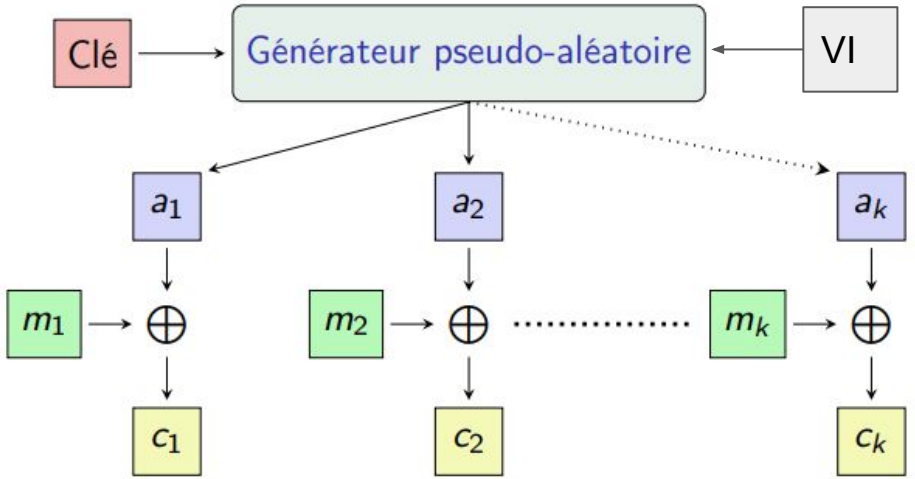


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Chiffre de Vernam

- Algorithme créé en 1917
- Théoriquement incassable
- Difficile à mettre en oeuvre pour les communications via internet

Particularité: la création des clés

- La clé doit être au moins aussi longue que le message
- La clé doit être choisie de manière aléatoire
- Chaque clé ne doit être utilisée qu’une seule fois

Chiffrement par flot

Chiffre de Vernam

Algorithme:

- Vérifier la taille du message
- Créer une clé de la même taille
- Opérer un XOR sur chaque bit du message et de la clé
- Recommencer pour chaque nouveau message

Mess	0	1	0	1	1	1	0	0	1	0
Clé	1	0	1	1	0	0	1	1	1	0
Res	1	1	1	0	1					

En résumé

Par bloc:

- Découpage en bloc
- Chiffrement de chaque bloc pour chiffrer le message complet
- Manque de sécurité si l’opération de chiffrement est trop simple (e.g., XOR): des motifs peuvent être retrouvés

Par flot:

- Pas de découpage en blocs
- Chiffrement rapide
- Pratique pour les applications temps réel (e.g., streaming)

Conclusion sur les chiffrements symétriques

Ces méthodes sont intuitives mais quelques inconvénients nuances leur utilisation:

- La longueur de la clé doit être aussi longue que le message
- Les chiffrement symétriques nécessitent de transmettre la clé
  - très difficile sur internet car la clé peut être interceptée
- Le nombre de clés à transmettre est très grand:
  - Pour N personnes, il faudra transmettre N * (N-1) / 2 clés

Quand utiliser le chiffrement symétrique ?

- Utile pour chiffrer les données de son disque dur

Identifier les apprentissages

Quels sont les concepts à retenir de ce cours ?

Activité *1, 2, Tous*:

- Réfléchissez individuellement à cette question pendant - **3mn**
- Comparez vos idées avec l'un de vos voisins, convainquez-le que vous avez raison ! - **3mn**
- Mise en commun des réponses, des binômes sont interrogés - **2mn**

En résumé

Ce qu'il faut retenir:

- Les congruences
- Les opérations sur $\mathbb{Z}/n\mathbb{Z}$
- Les types de chiffrements symétriques et leur fonctionnement général

Le prochain cours:

- Comment s'échanger des clés privées sur un réseau ?
- Comment communiquer de manière sécurisée ?

Quelques dernières questions sur le quizz

Ressources

https://www.irif.fr/_media/users/ylg/crypto.pdf