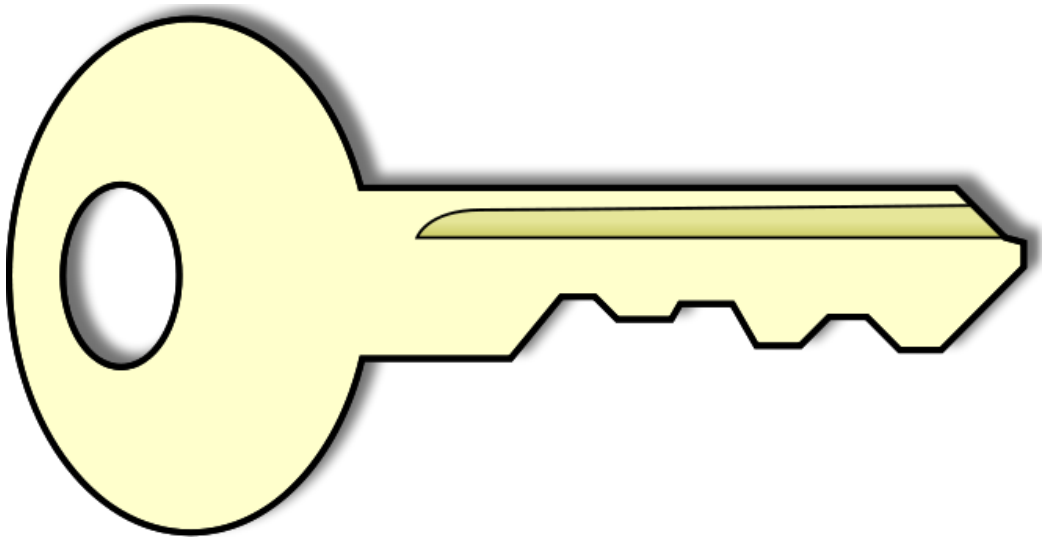
A l'attaque des codes secrets



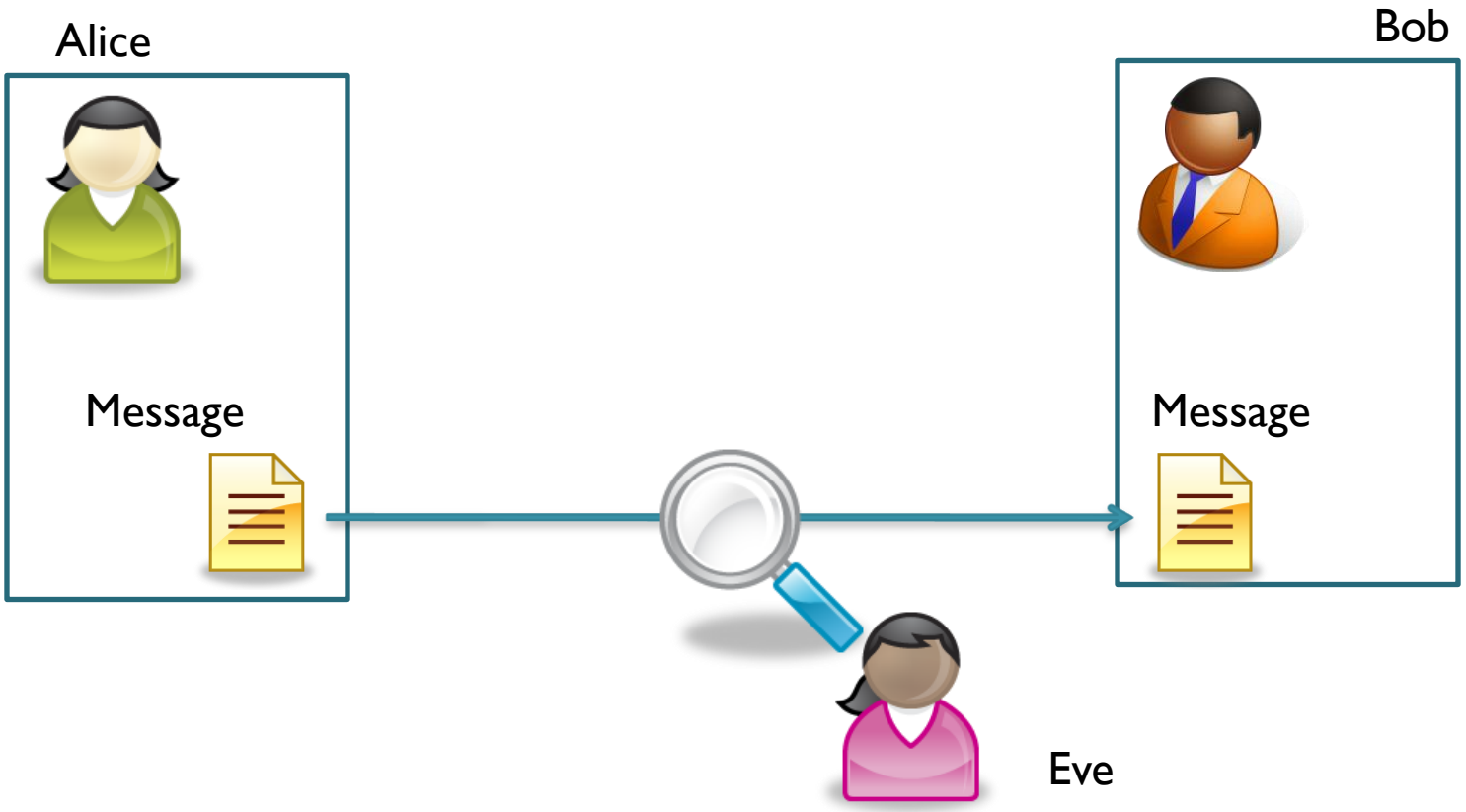
Fête de la science 2008

INRIA Rhône-Alpes

Mathieu Cunche, Mate Soos, Aurélien Francillon, Thomas Roche

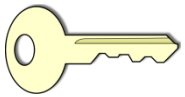
Comment transmettre un message secret ?

- Alice veut envoyer un message à Bob
- Eve veut connaître le contenu du message

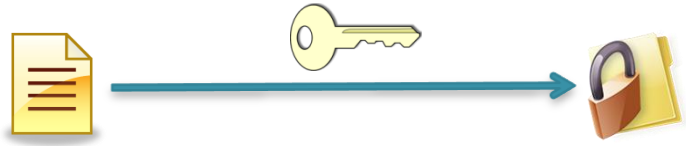


Comment transmettre un message secret ?

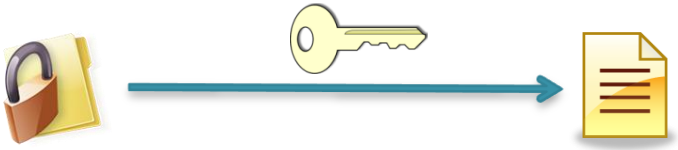
- Utiliser un système de chiffrement (ou chiffre)
  - Alice et Bob choisissent une clef



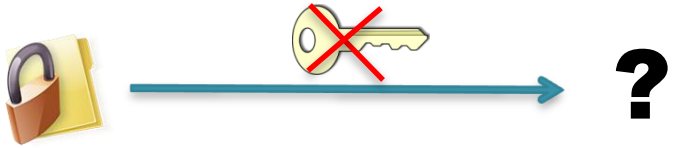
  - Alice utilise la clef pour chiffrer le message



  - Bob déchiffre le message avec la clef



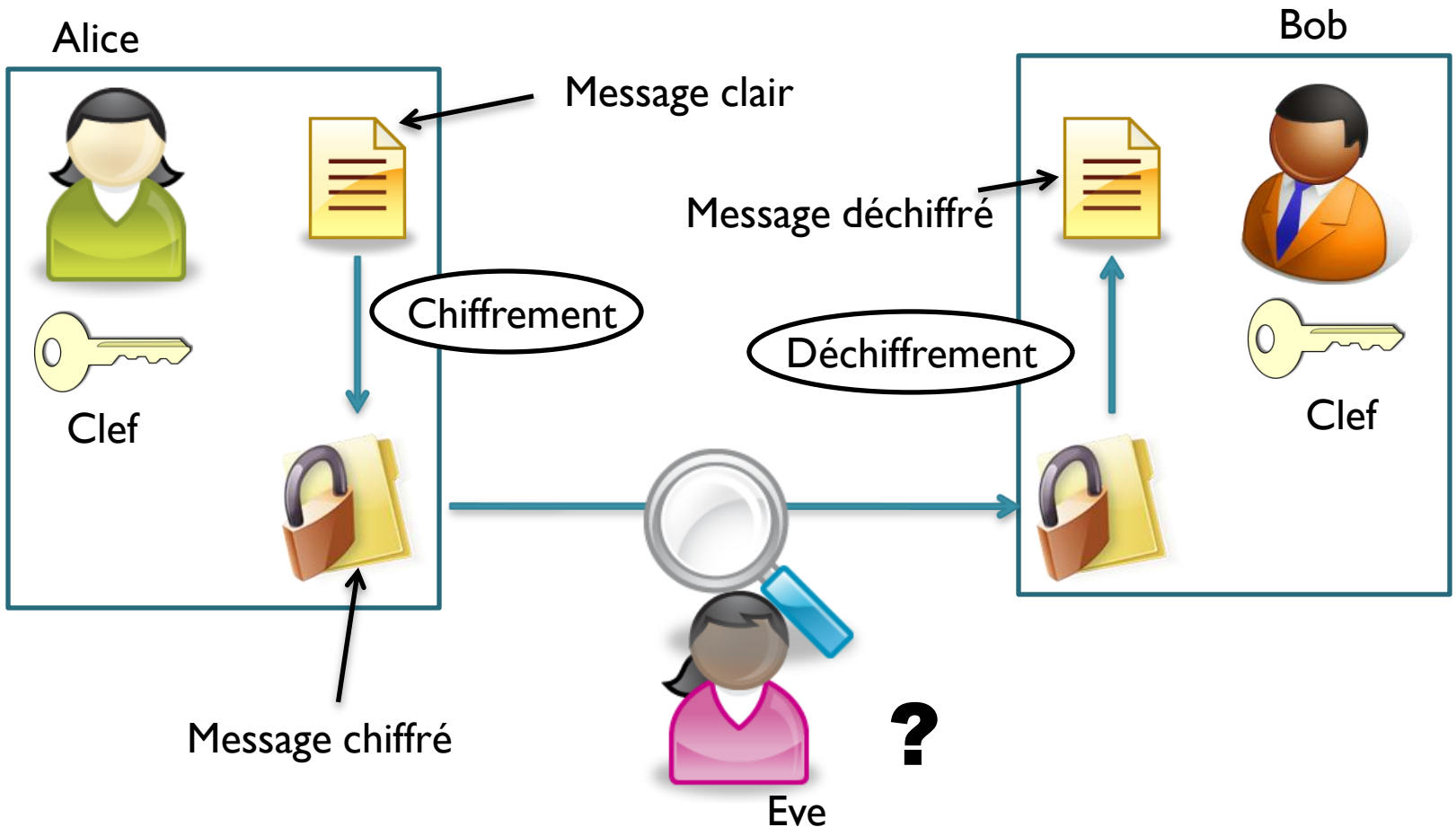
  - Eve ne peut pas déchiffrer le message sans la clef



  - Mais elle peut tenter de décrypter le message (très difficile voir impossible, si le chiffre est bien fait)

Comment transmettre un message secret ?

- Grâce au chiffrement le message n'est pas dévoilé

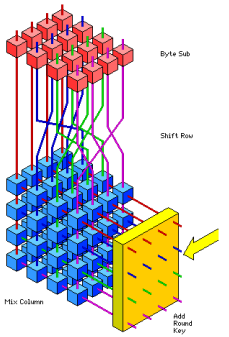


Un peu d'histoire

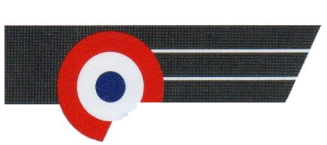
- Chiffre de Cesar (-40 av J-C)
  - 25 clefs possibles

- Enigma (2eme guerre mondiale)
  - 10^16 clefs possibles

- Advanced Encryption Standard (2000)
  - 10^38 clefs possibles



Qui utilise les codes secrets?

- Les diplomates 
- Les militaires 
- Les agents secrets 

Qui utilise les codes secrets?

- Nous !!
  - Téléphone portables

  - Cartes à puce

  - Sites internet sécurisés

  - Etc …

Le chiffre de Cesar

- Décalage de l'alphabet

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

Chiffrement ↓

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

Alphabet décalé de 3 positions vers la gauche

Déchiffrement ↓

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

- Clef = nombre de positions dont on a décalé

➢ Expérience: chiffrement et déchiffrement avec le chiffre de césar

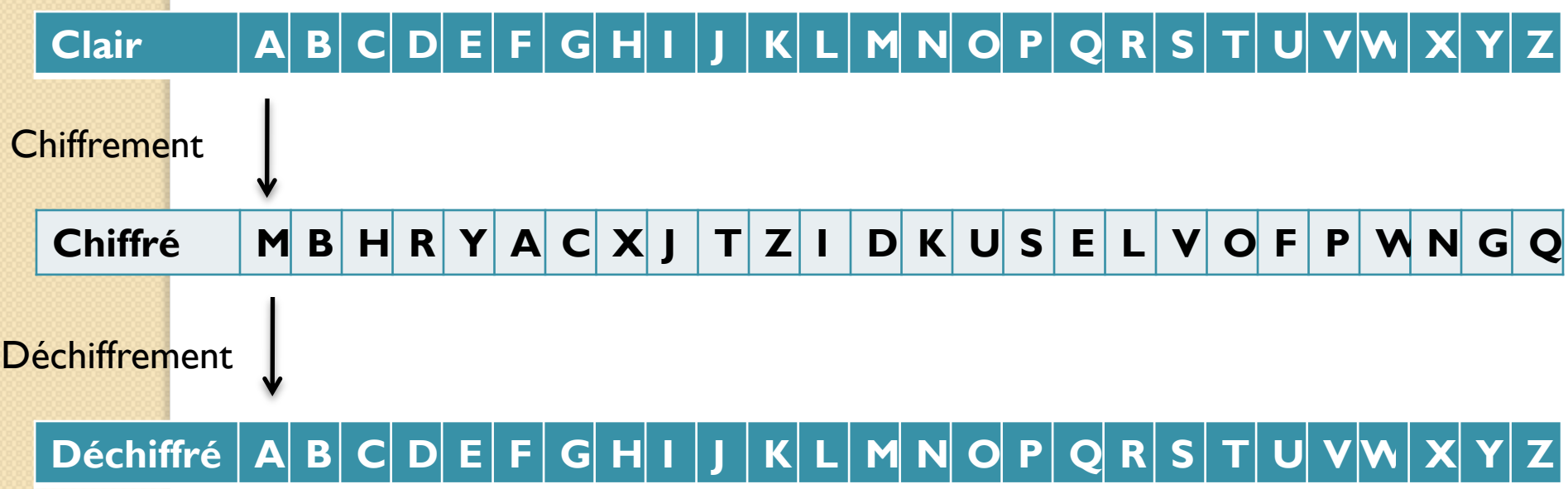
Casser le chiffre de César

- But: retrouver le nombre de décalages
- Nombre de clefs possibles = 25
  - On essaye toutes les clefs (attaque par force brute)
    - On déchiffre avec chaque clef
    - Si on reconnait un texte en francais on a gagné
    - Sinon on essaye une autre clef
  - 25 essais au maximum ☺

➢ Expérience: cassage du chiffre de César par attaque force brut

Chiffre à alphabet mélangé

- Permutation: mélange des lettres de l'alphabet



- Clef = permutation de l'alphabet

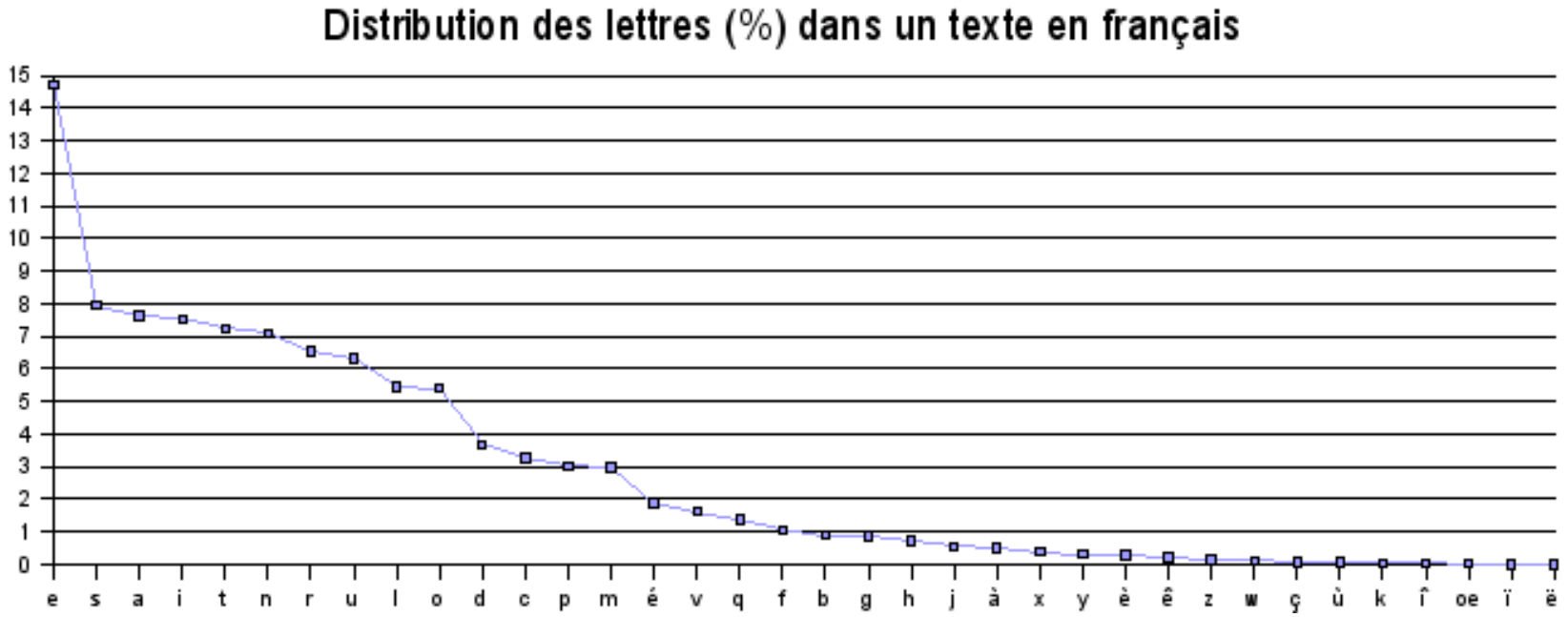
➢ Expérience: cassage du chiffre à alphabet mélangé par attaque force brute

Casser le chiffre à alphabet mélangé: par force brute

- But: retrouver la permutation de l'alphabet
- Essayer toutes les clefs possibles ?
  - Il existe 10^25 alphabets mélangés différents
  - Trop long de tous les essayer
  - A titre de comparaison: dans un livre il y a 10^24 atomes
  - Il faut être plus malin …

Fréquence des lettres dans un texte

- Dans un texte en français:
  - La lettre ***e*** est celle que l'on retrouve le plus souvent, c'est ensuite la lettre ***s,*** puis la lettre ***a,*** etc
  - Pour chaque lettre de l'alphabet on peut estimer le nombre de fois qu'elle va apparaitre



Casser le chiffre à alphabet mélangé: par analyse fréquentielle

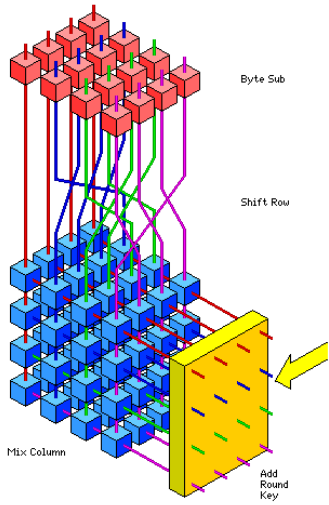
- Compter le nombre de fois que chaque lettre apparait dans le texte chiffré

Lettre du chiffré	Y	M	V	J	K	O	L	F
Nombre d'apparitions	3023	1354	1235	1210	1195	1003	986	923

- La lettre **y** apparait le plus souvent:
  - il y a de fortes chances que **y** remplace ***e*** dans le chiffré

➢ Expérience: cassage du chiffre à alphabet mélangé par attaque de lettre probable

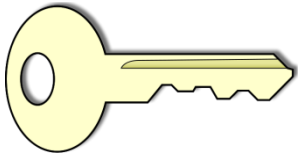
Les chiffres d'aujourd'hui



- Utilisent des permutations, des substitutions
- Les attaques fréquentielles ne suffisent plus pour les casser
- Pour les casser il faut utiliser des méthodes de cryptanalyse beaucoup plus complexes

L'étude des codes secrets

- Les cryptographes ont créés les chiffres
- Les cryptanalystes cherchent des faiblesses pour casser les codes secrets
- Les cryptologues: cryptographes et cryptanalystes à la fois
  - Pour construire un chiffre résistant aux attaques, il faut connaître ces attaques



Conclusion

- Le but d'un code secret est d'assurer la confidentialité des messages
- Grâce à des outils appropriés il est parfois possible de casser la protection
- L'étude des codes secrets est un domaine de recherche très dynamique
- Les chercheurs de l'INRIA travaillent à construire les codes secrets de demain

Sources

- Wikipedia
- La guerre des Gaules:
  - http://bcs.fltr.ucl.ac.be/CAES/BGI.html
- Outils en lignes:
  - http://planete.inrialpes.fr/~soos/fete_science/

Un peu de vocabulaire

- Chiffrer:
  - Coder à l'aide d'une clef un message clair en un message chiffré
- Déchiffrer:
  - Décoder à l'aide de la clef un message chiffré pour récupérer le message clair
- Décrypter:
  - Décoder un message chiffré sans connaitre la clef