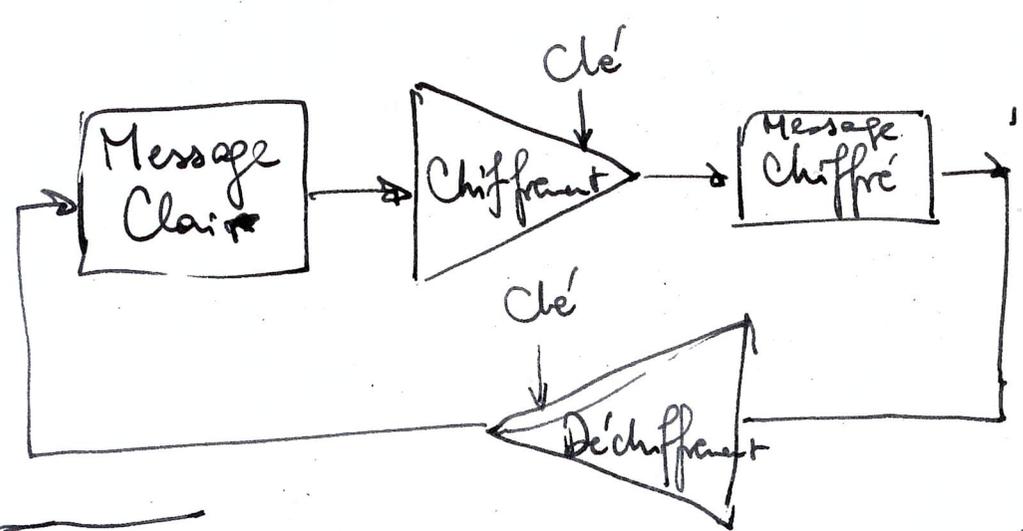


Le cryptographie : techniques de cryptage.



Le cryptosystème = ensemble ~~des clés de messages clairs poss~~
 de clés K
 de messages clairs possibles M
 de messages chiffrés possible C
 associé à un algorithme de chiffrement $E: K \times M \rightarrow C$
 et un procédé de déchiffrement $D: K \times C \rightarrow M$

On suppose que $\forall m \in M \exists$ paire de clé chif. & déchif. ;
 (k_D, k_E)

$$D(k_D, E(k_E, m)) = m$$

Principe de Kerckhoffs : la sécurité d'un cryptosystème ne doit pas reposer sur la non divulgation de la fn de cryptage mais uniquement sur la non divulgation de la clé.
Maxime de Shannon : l'adversaire connaît le syst.

→ Chiffrement symétrique: $k = k_E = k_D$ (secret)

* faiblesse: interception lors de la transmission!

→ Chiffrement asymétrique: $k_E \neq k_D$ (clé publique)

* force: k_E connu, k_D secret ne circule pas!

→ Substitution monoalphabétique:

Chiffrement de César ∈ famille des chiffres de subs.

Problème 1: Chiffrement

1. Permutations quelconques: nb. de clés possibles = $n!$ (26!)

2. Simple décalage: nb. de clés = 26

3. → ~~étaler~~ Principe:

$L \rightarrow 12 \rightarrow$ matrice (E) \rightarrow $\begin{pmatrix} nb \\ ch \end{pmatrix} \rightarrow \begin{pmatrix} lettre \\ ch \end{pmatrix}$

4.

Problème 2: Déchiffrement

1. Trans. inverse du chiffrement de César est le remplacement d'une lettre par celle qui se trouve à la position "-3". Par ex: D est remplacé par A

- Pb1
1. Combien de cle's potentielles ?
 2. Simple décalage → nb de cle's ?
 3. Chiffrement César
 4. Permutation quelconque.

donner la fⁿ $\text{ascii}(x)$

$x = \text{"message"}$ $\text{ascii} \Rightarrow \text{code}$
 $x = \text{code}$ $\text{ascii} \Rightarrow \text{"message"}$

$i < \text{length}(\text{tabAscii})$

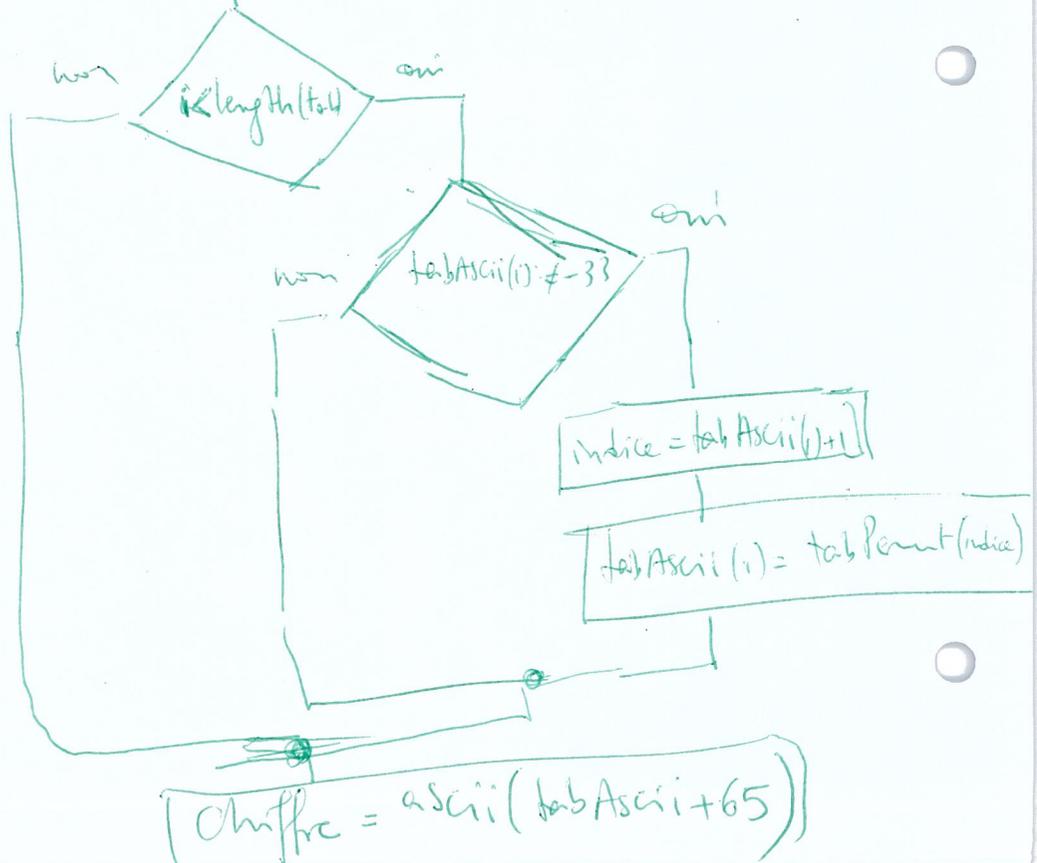
fonction chiffre (tabPermut, mess)
 ↳ [0, 25]

$\text{tabAscii} = \text{ascii}(\text{mess})$

transformation du message en une suite de code

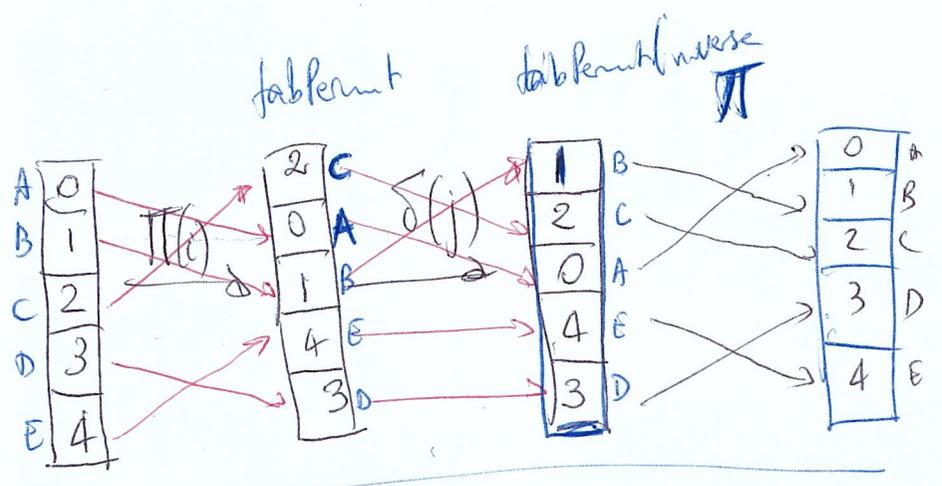
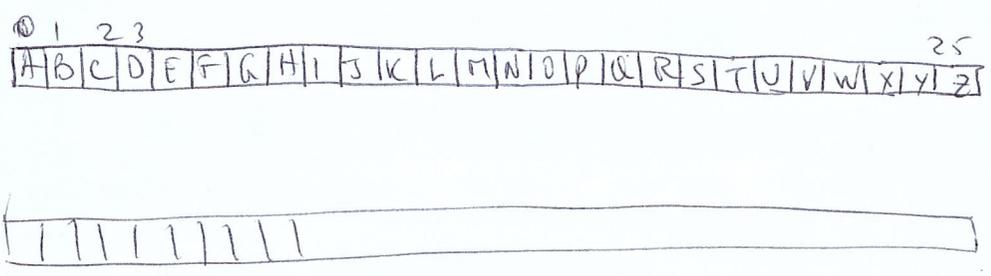
$\text{tabAscii} = \text{tabAscii} - 65$

On retire 65 code de "A" ainsi on a [0, 25] dans tabAscii.



• Ecrire les fonctions avec le message et la clé en paramètres. (pour le 'er')

• Chiffrement monoalphabet:
arguments (tab_permut, message).



A → C → B

BABADE
ACACFD
BA

A	
B	←
C	←
D	
E	