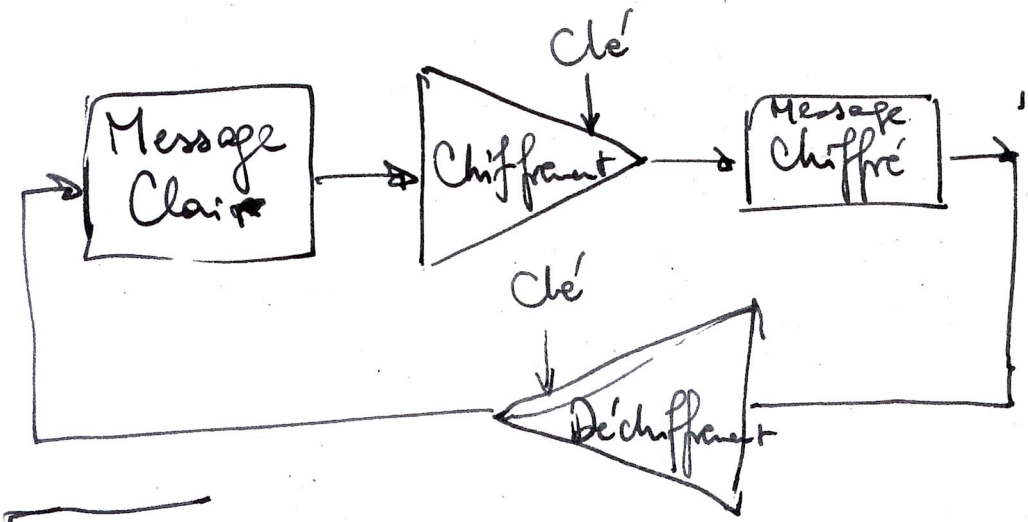
La cryptographie : technique de cryptage.



Le cryptosystème = ensemble
- de clés $\mathcal{K}$
- de messages clairs possibles $\mathcal{M}$
- de messages chiffrés possible $\mathcal{C}$

associé à un algorithme de chiffrage $\mathcal{E} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
et un procédé de déchiffrage $\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

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

$$\mathcal{D}(k_D, \mathcal{E}(k_E, m)) = m$$

Principe de Kerckhoffs : la sécurité d'un cryptosystème ne doit pas reposer sur la non divulgation de la fct 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 assymétrique : $k_E \neq k_D$ (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. → Principe :

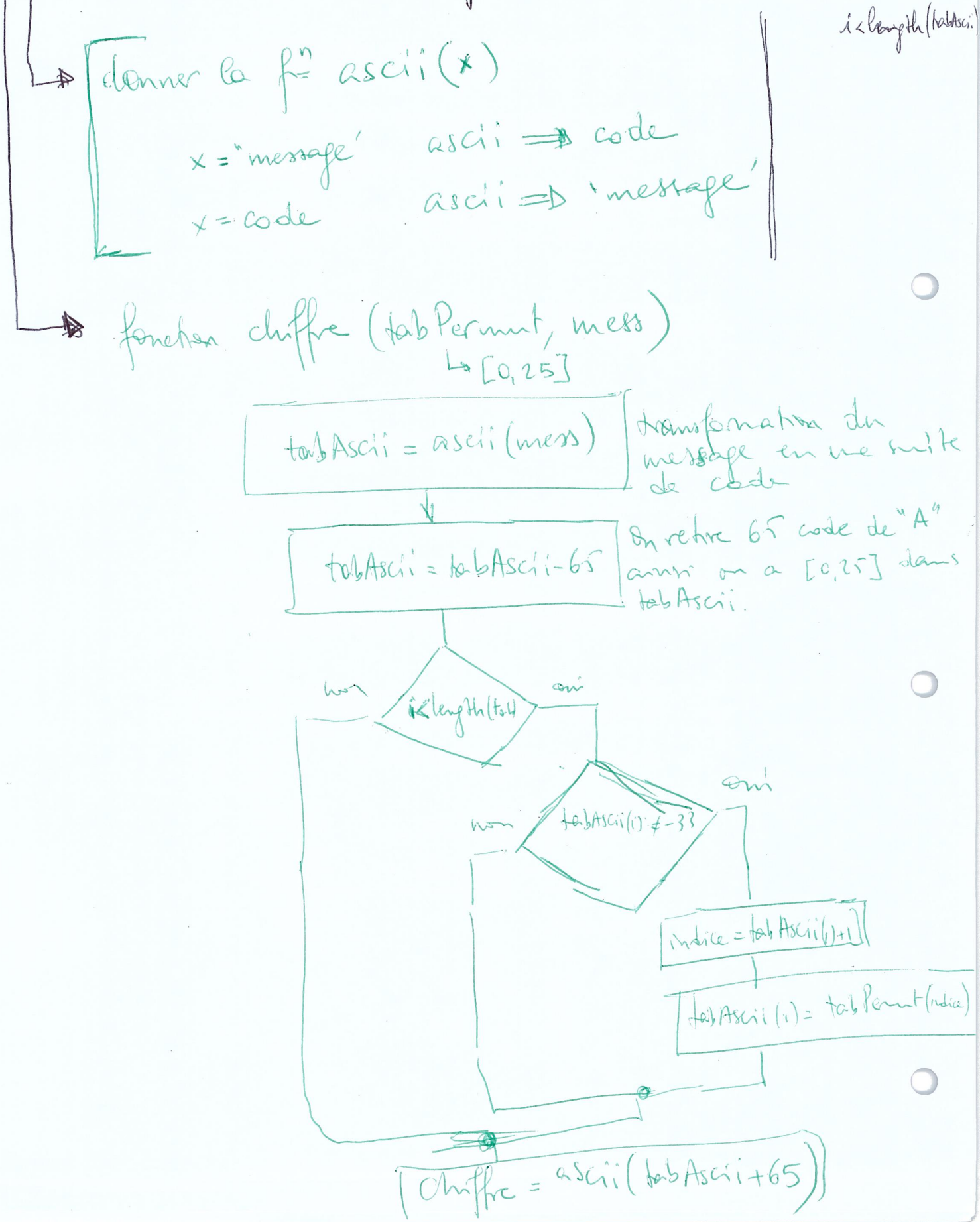
$$L \to 12 \to \text{matrice } (E) \to (nb_{Ch}) \to (lettre_{Ch})$$

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

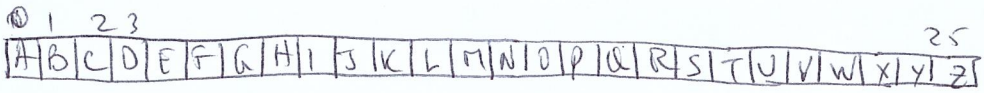
Pb1 : 1. Combien de clés potentielles ?
2. Simple décalage → nb de clés ?
3. Chiffrement César
4. Permutation quelconque.

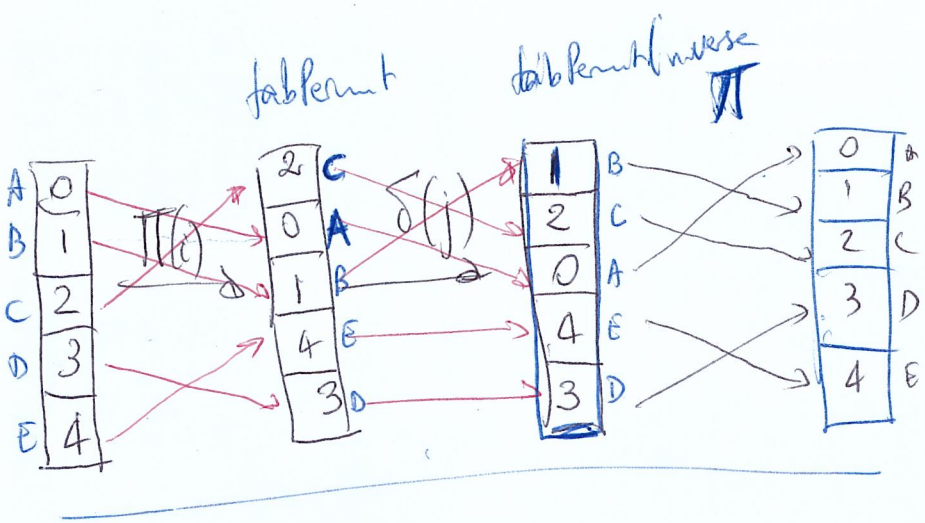


; Ecrire les fonctions avec le message et la clé en paramètres. (pour César)

° Chiffrement monoalphabet :

arguments (tabPermut, message).





A → C → B

BABADE
ACACED
BA