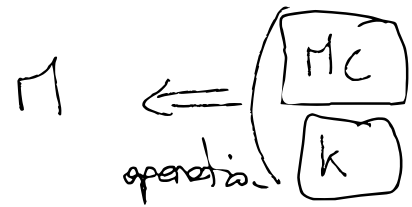
Codage d'un message

Message M
Clé K
⟹ opération → Message Codé MC



Le système de Vernam

Alphabet A (par exemple : A, B, ... Z : ASCII 127 (7bits)) 0 – 127

Message = "Pierre" → "PIERRE"
→ "Pierre"

Clé de Vernam

Longueur est la longueur du message
Et le vocabulaire de la clé et le vocabulaire de l'alphabet du message

Et les éléments de la clé sont générés aléatoirement

Exemple

M = "PIERRE"

K = "AZBATF"

A	B	C	D	...	Z
0	1	2	3		25

26 symboles

M' = "15 8 4 17 17 4"

K = "0 25 1 0 19 5"

⊕ addition modulaire 26

(8+25) mod 26

MC = "15 7 5 17 10 9"

MC' = "P H F R K J"

MC = "PMFRKJ" est reçu par le receveur sur un canal

K = "AZBATF" est reçue par le receveur sur un autre canal

Le receveur va décoder le message.

MC' = "15 7 5 17 10 9"

K = "0 25 1 0 19 5"

$\oplus^{-1}$

15 + 0 mod 26
7 + 25 mod 26
5 + 1 mod 26

M = "~~18 6~~ ~~17~~

8 ← 26 − (7 − 25) → −18

M = "15 8 4 17 17 4"

2 [15 − 0 → 15
[5 − 1 → 4
[17 − 0 → 17
17 26 − (10 − 19) → −9
[9 − 5 → 4

MC' − K → ≥ 0 ok
→ < 0 26 − (MC' − K)

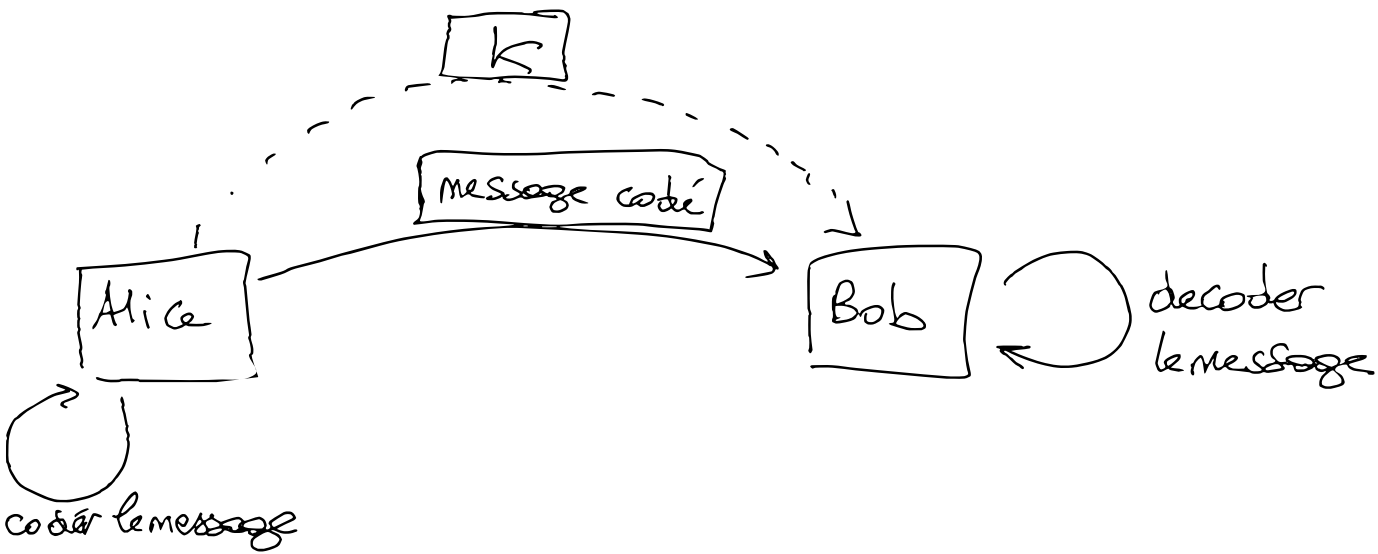
M = "15 8 4 17 17 4"

① Générer une clé

↳ générer un fichier (qui contiendra la clé)

- On a besoin de la longueur du message] entier
- Vocabulaire] ensemble de symboles] entier qui correspond à la taille de mon A B.

① correspondance en lettres de l'alphabet et l'entier lui correspondant



(2)

J'ai à ma disposition un fichier dans lequel est la clé

- fichier qui contient le message
- fichier qui contient la clé

- un fichier qui contient le message codé. (en sortie)