Université de Toulon
UFR : Sciences et techniques

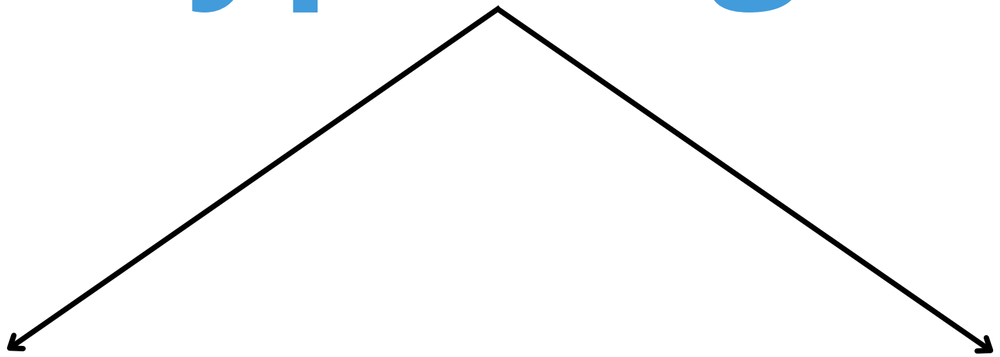
Projet Personnel de Recherche

CRYPTOLOGIE

Présenté par : Coupeaux Bastien

Tuteur : Robert Jean-Marc

Cryptologie



Cryptographie

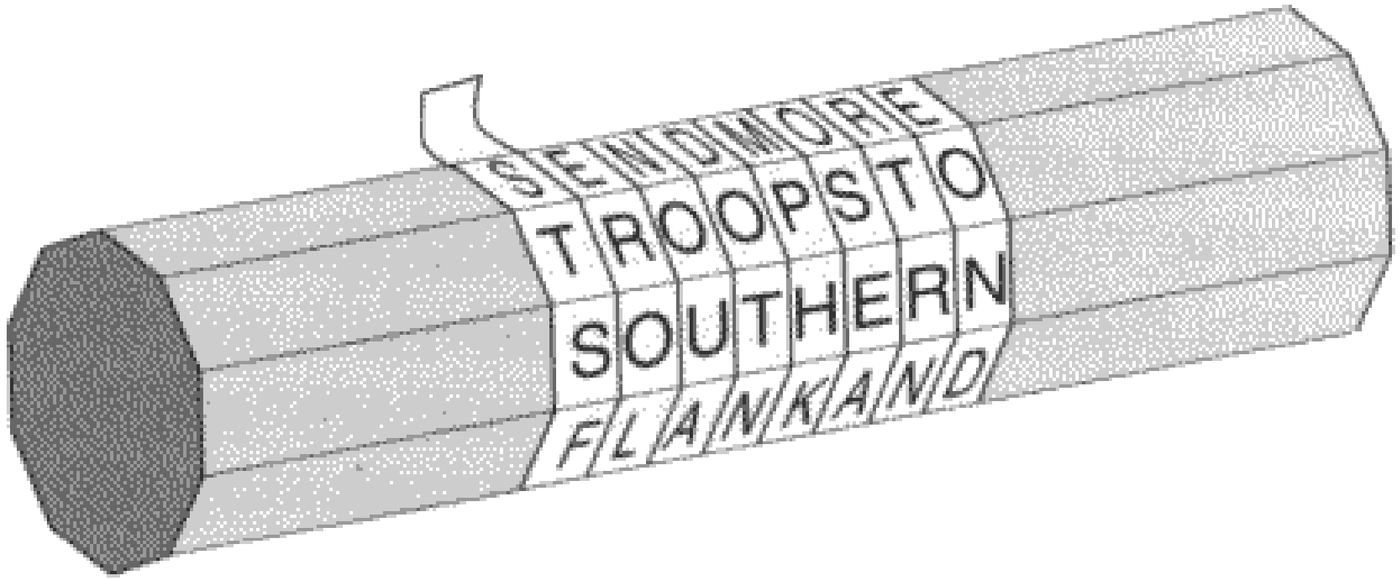
=

Définition et étude

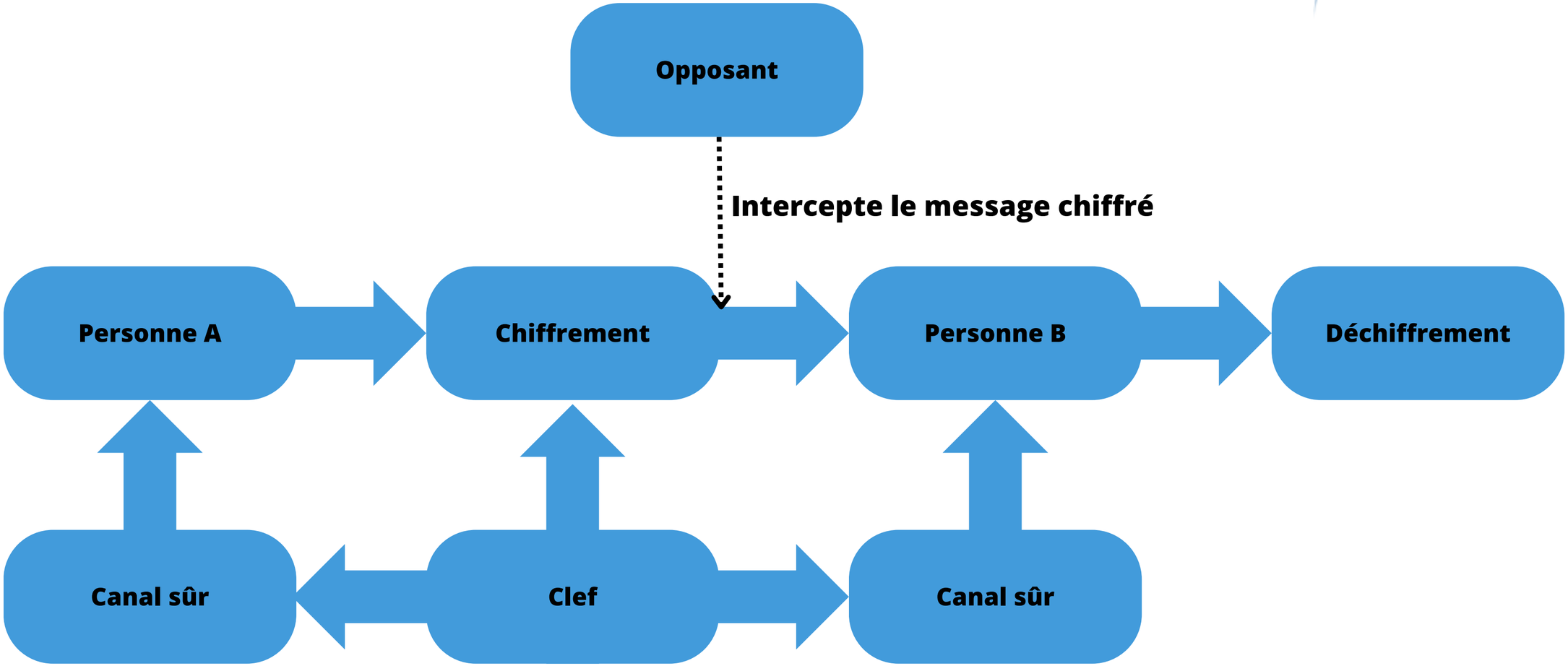
Cryptanalyse

=

Validation et trouver une faille



Deneuville, Jean-Christophe. (2016). Contributions à la cryptographie post-quantique.


Opposant
Intercepte le message chiffré
Personne A
Chiffrement
Personne B
Déchiffrement
Canal sûr
Clef
Canal sûr

Un exemple de chiffrement : le chiffrement par décalage

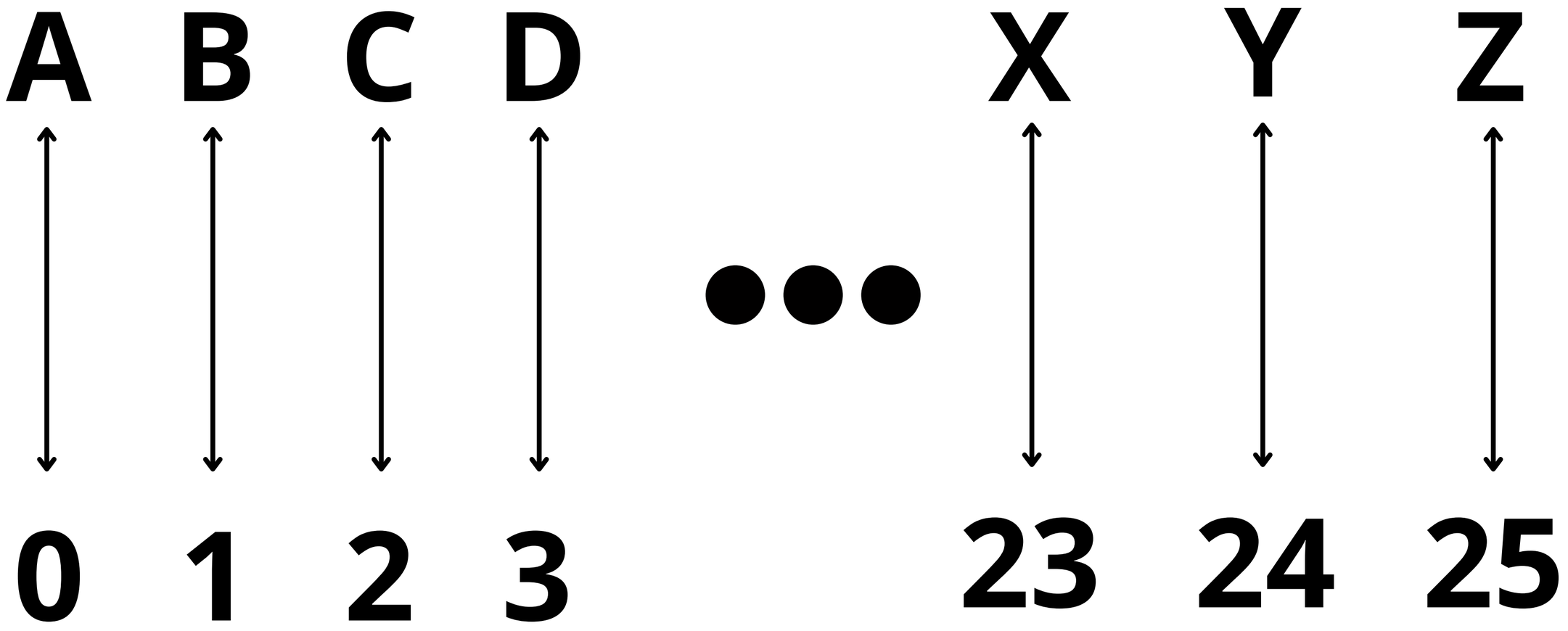
Définition : Congruence

Soient X et Y deux entiers et soit n, un entier positif. On dit que X est congru à Y modulo n si les restes de X et de Y lors de leurs division par n sont identiques.

Exemple : $3 \equiv 5\ [2]$ car :

- $3 = 2 \times 1 + 1$
- $5 = 2 \times 2 + 1$

ENCODAGE



Mot choisi : KIWI

K ⟷ 10 ; I ⟷ 8 ; W ⟷ 22

Clef choisie : 2

KIWI ⟶ MKYK

TABLE	DE	VÉRITÉ
A	B	A $\oplus$ B
1	1	0
1	0	1

Conclusion et Bilan

- **Codage chiffrement de Vigenère , par subsitution, ... et leurs déchiffrements**
- **Étude de théories et concepts cryptologiques comme la théorie de Shannon**