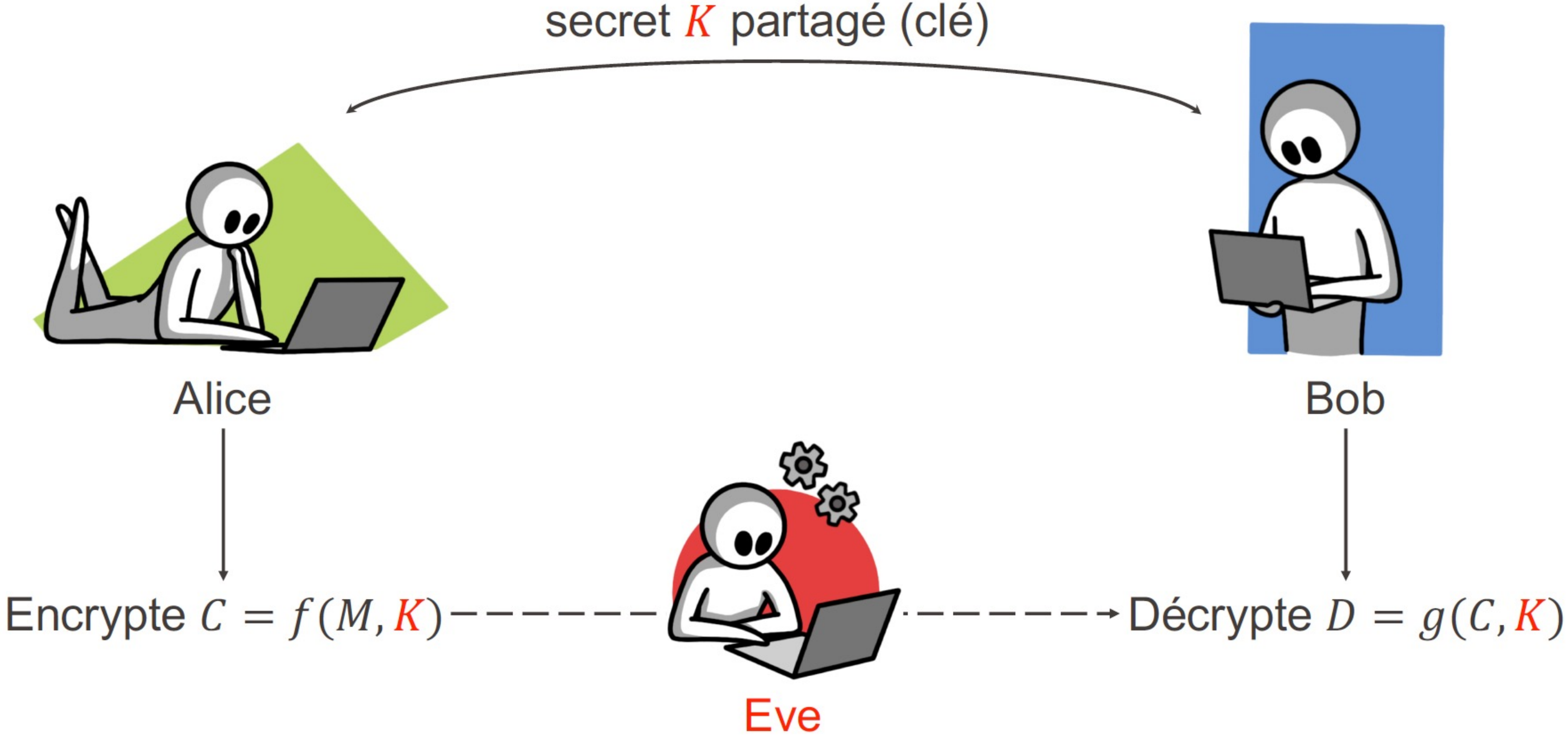
Cryptographie à clé secrète: un peu d'histoire

Cours Turing – Semaine 7

Scénario



Eve intercepte C mais ne sait pas trop quoi en faire sans la clé K…

Préliminaire: additions modulo 26 sur l'alphabet

$$\begin{array}{ccccccccc} A & B & C & D & E & F & G & \ldots \text{ (26 symboles) } \ldots & Z \\ | & | & | & | & | & | & & & | \\ 0 & 1 & 2 & 3 & 4 & 5 & & & 25 \end{array}$$

$$\begin{array}{cccc} A + B = B, & C + D = F, & \ldots, & Y + Z = X \\ 0 + 1 = 1 & 2 + 3 = 5 & & 24 + 25 = 49\ (-26) = 23 \end{array}$$

$$A - B = Z$$

$$0 - 1 = -1\ (+26) = 25$$

Chiffre de César

clé = une lettre (p.ex C = 2)

M = "BONJOUR"

+C (chiffrement)

C = "DQPLQWT"

message chiffré

déchiffrement : −C ou +Y

(−2) (+24)

D = "BONJOUR"

Grave problème

Eve peut tester les 26 clés pour retrouver le message

Chiffre par substitution (monoalphabétique)

A	B	C	D	E	F	...
R	A	D	G	K	F	...

Secret partagé

$\longrightarrow 26!$ possibilités $\simeq 4 \cdot 10^{26}$

$M =$ "BONJOUR" $\longrightarrow$ $C =$ "_ _ _ _"

Chiffre par substitution: décryptage

analyse des fréquences:

Malgré le nombre pour chiffrer le message, le système n'est pas sûr

Chiffre de Vigenère

clé = un mot (ex: CHAT)

« BONJOUR COMMENT VAS TU »

\+ CHATCHA TCHATCH ATC HA

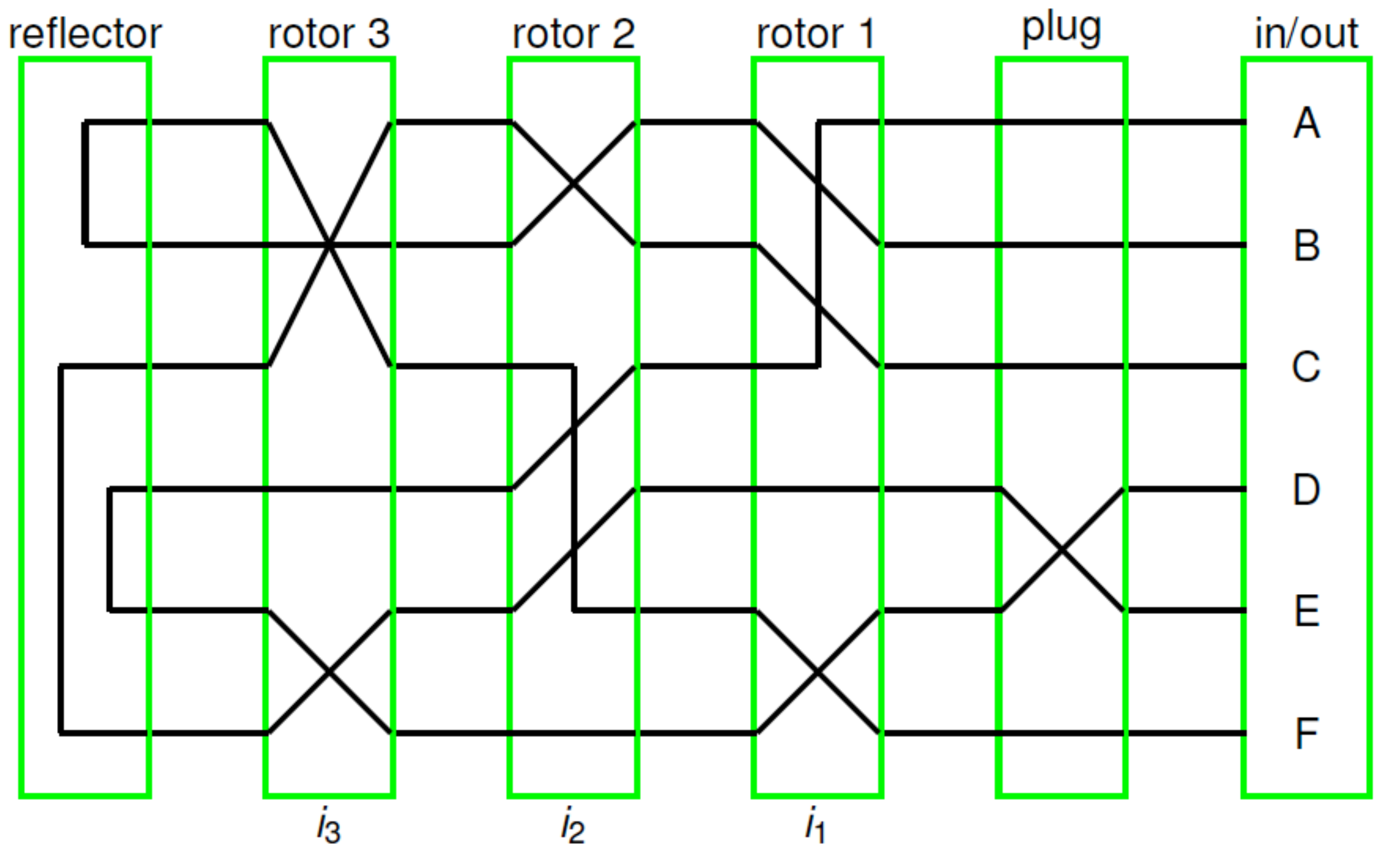
DVN - - - - - - -

Combien de mots possibles avec des mots de k lettres ?

$$\underbrace{26 \cdot 26 \cdot 26 \cdot 26 \cdots 26}_{k \text{ fois}} = 26^k$$

Enigma

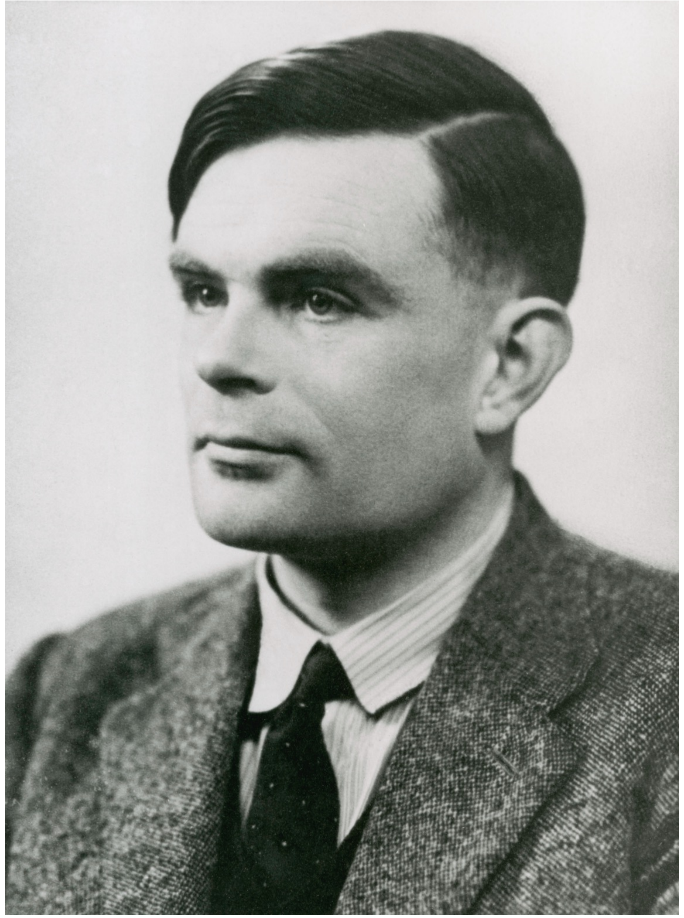
Enigma



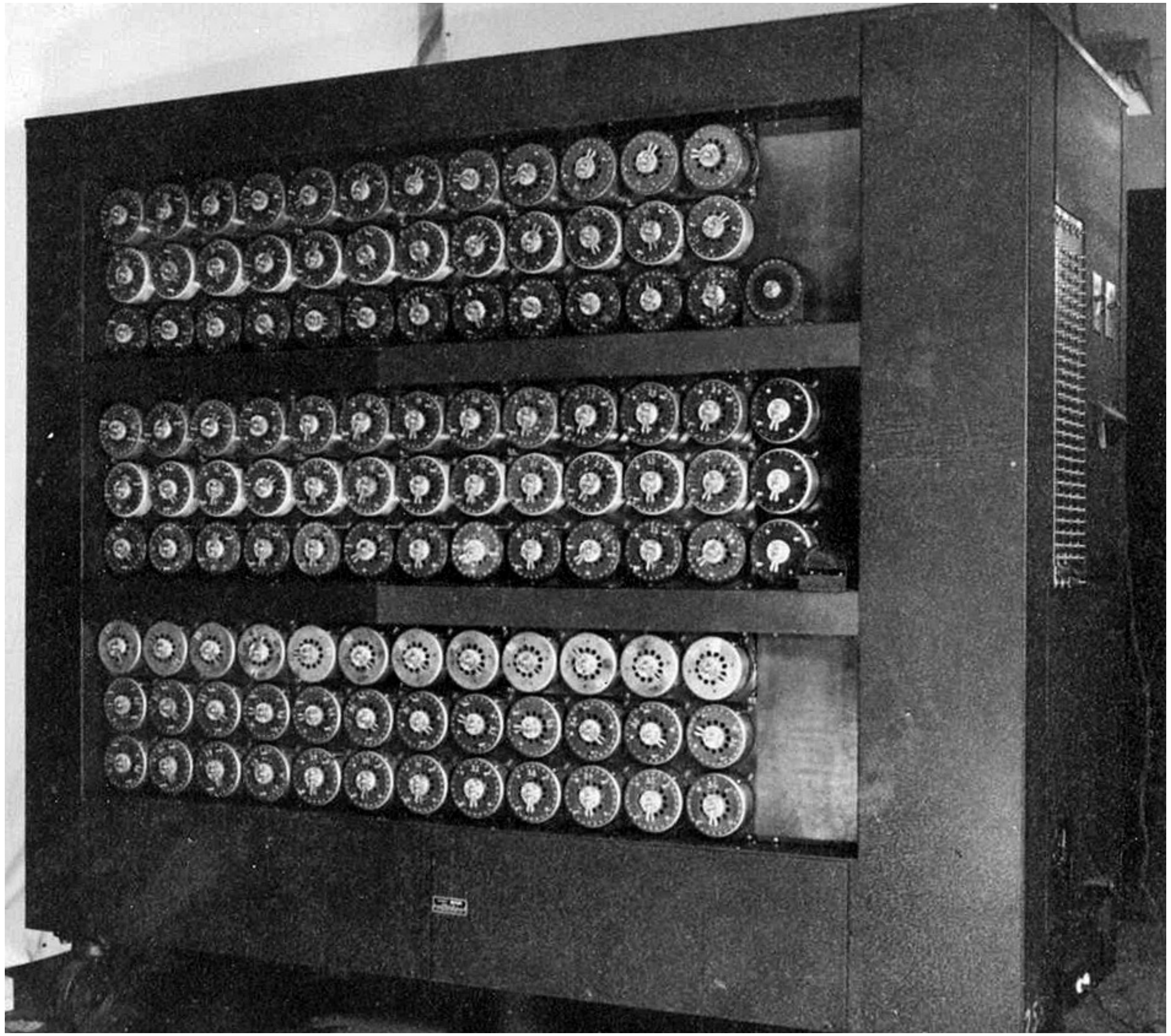
Enigma

https://www.101computing.net/enigma-machine-emulator/

Alan Turing - Bletchley Park



La "bombe"



Principes de Kerckhoffs

Exercice 1

A utiliser :

code ASCII

- ord et chr : ord('A') = 65 chr(65) = 'A'
- opération modulo : a % b = reste de la division entière de a par b
  exemple : 127 % 5 = 2
- distance entre deux listes de fréquences : … $\sum_{i=0}^{25} |freq\_th[i] - freq\_emp[i]|$

Exercice 2

"AZTZZBBCDEFJKZ..."

$\underline{k=3}$

A utiliser :

- indice de coïncidence : $\boxed{IC = \sum_{i=A}^{Z} \frac{n_i(n_i-1)}{n(n-1)}}$

texte aléatoire : ~0.03

texte français : ~0.075

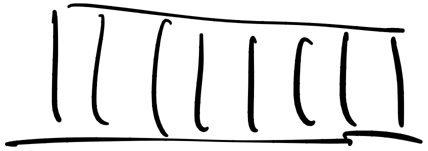
exemple de texte : "AAAABBBCCCDDE"

$n_A = 4, n_B = 3, n_C = 3, n_D = 2, n_E = 1, n = 13$

$$IC = \frac{4\cdot 3}{13\cdot 12} + \frac{3\cdot 2}{13\cdot 12} + \frac{3\cdot 2}{13\cdot 12} + \frac{2\cdot 1}{13\cdot 12} + \frac{1\cdot 0}{13\cdot 12}$$

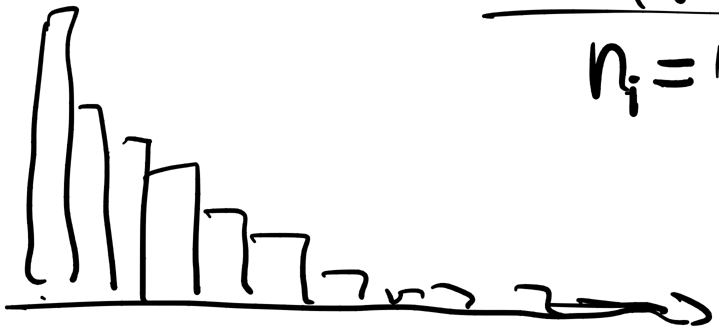
$$= \frac{12+6+6+2+0}{156} = \frac{26}{156} = 0{,}1\overline{6}$$

al:



$n_i = n_j$

fr:



e

$n_e > n_z$