Vis ma vie
Mathématiques

Enseignant
Arnaud Bannier

Découverte d'Enigma

Année 2020–2021

esiea

Objectifs de la cryptographie

Objectifs de la cryptographie

Douglas

Tigibus

Objectifs de la cryptographie

p

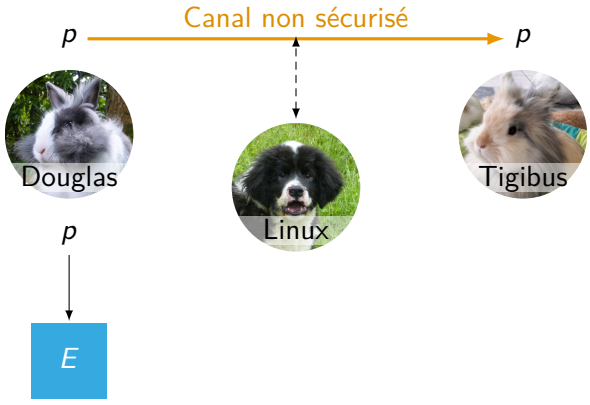
Douglas

Tigibus

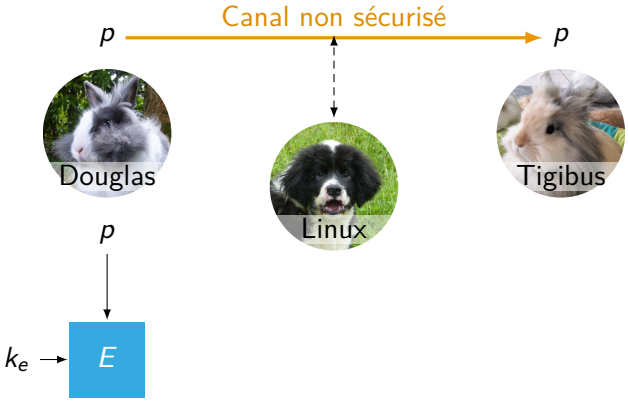
Objectifs de la cryptographie

Objectifs de la cryptographie

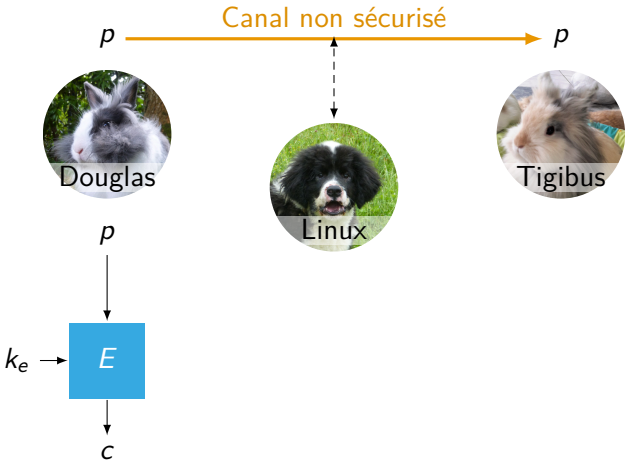
Objectifs de la cryptographie



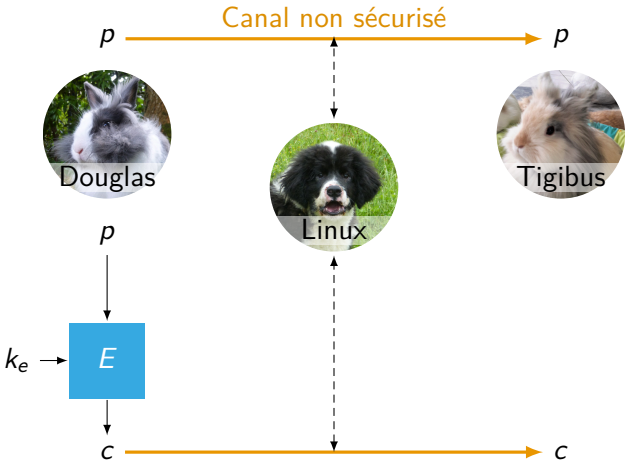
Objectifs de la cryptographie



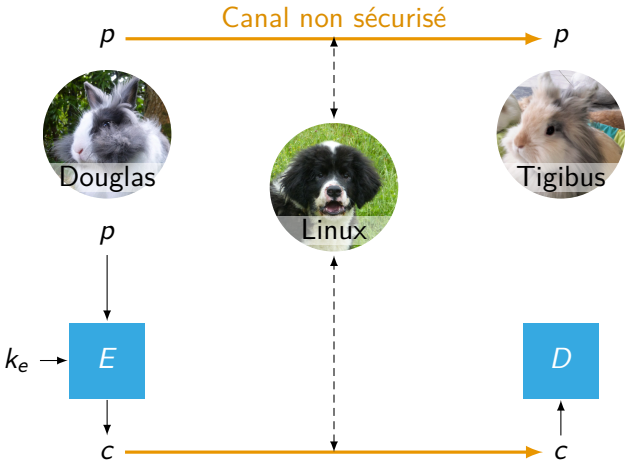
Objectifs de la cryptographie



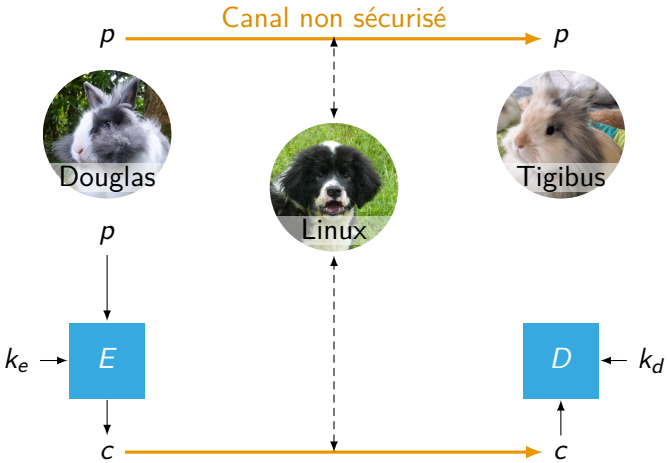
Objectifs de la cryptographie



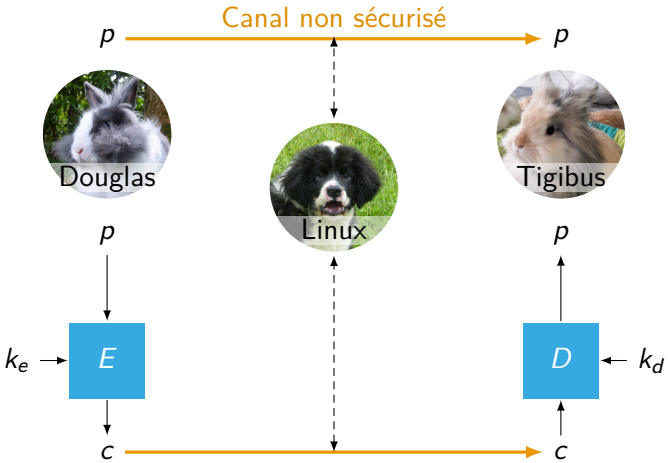
Objectifs de la cryptographie



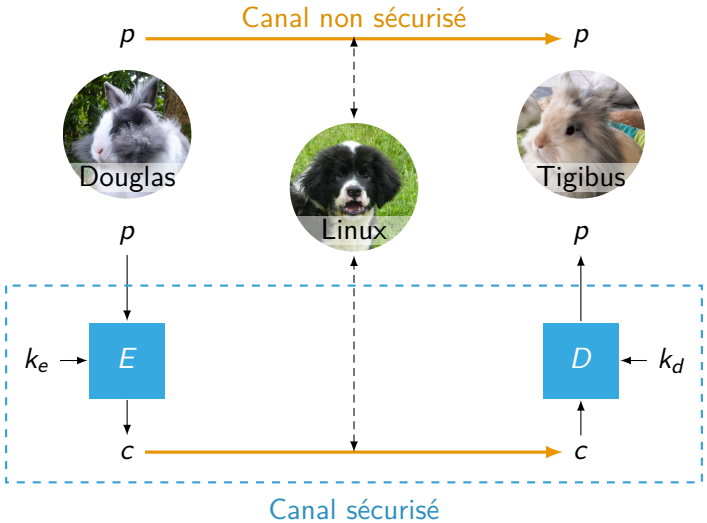
Objectifs de la cryptographie



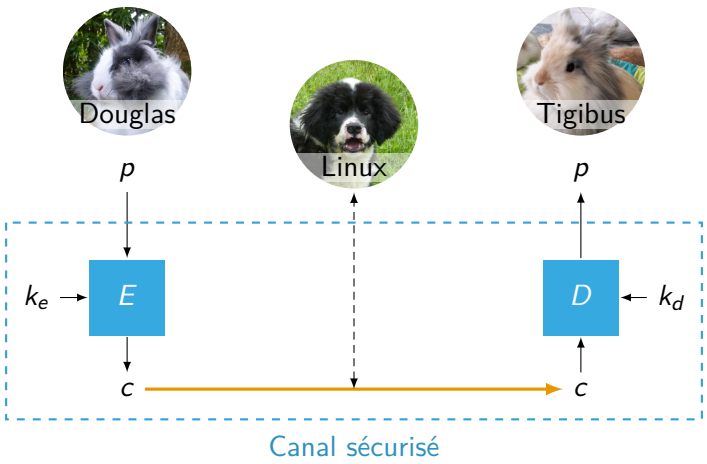
Objectifs de la cryptographie



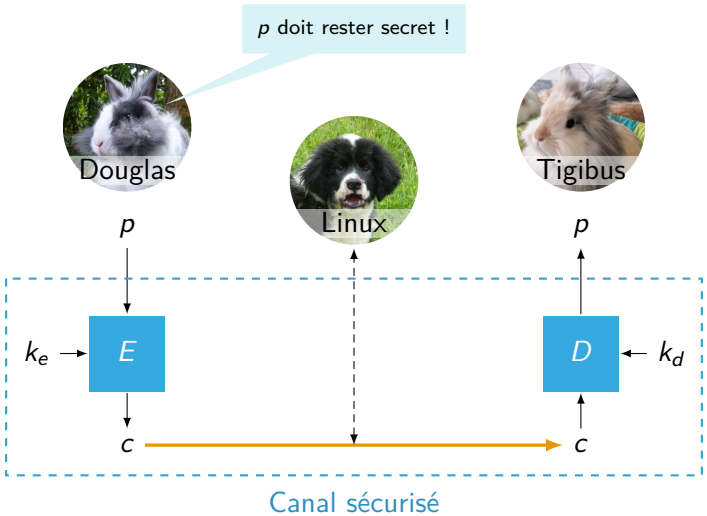
Objectifs de la cryptographie



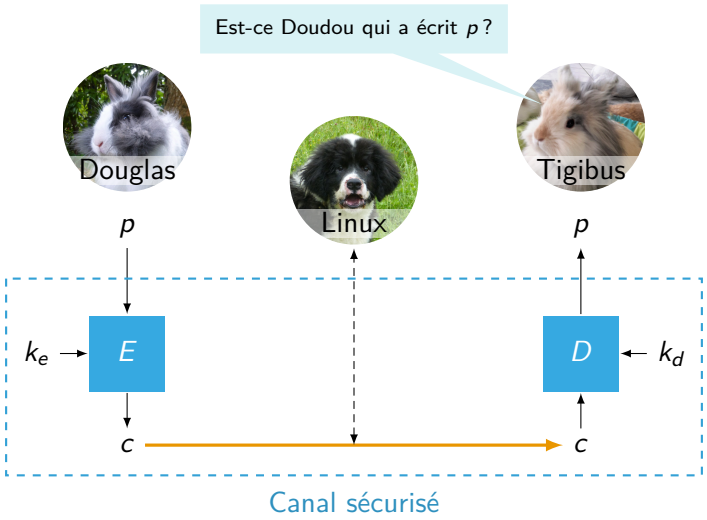
Objectifs de la cryptographie



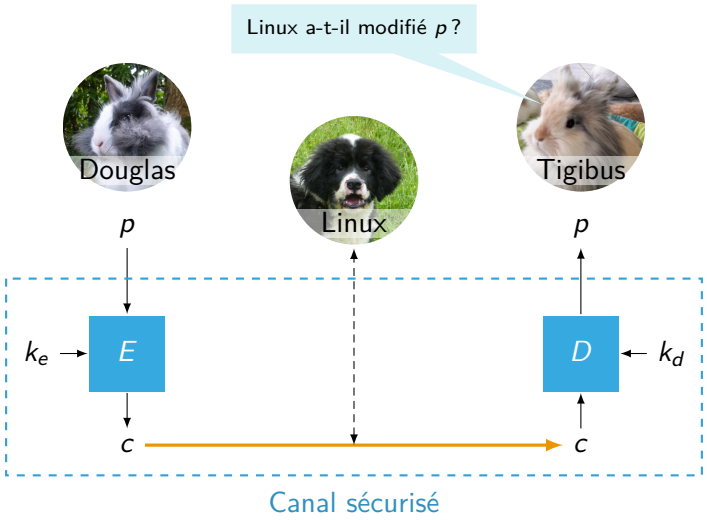
Objectifs de la cryptographie



Objectifs de la cryptographie



Objectifs de la cryptographie



Objectifs de la cryptographie

Confidentialité.
Un adversaire écoutant la communication ne peut obtenir aucune information sur son contenu.

Objectifs de la cryptographie

Confidentialité.
Un adversaire écoutant la communication ne peut obtenir aucune information sur son contenu.

Authentification.
Un adversaire ne peut se faire passer pour l'émetteur ou le récepteur.

Objectifs de la cryptographie

Confidentialité.
Un adversaire écoutant la communication ne peut obtenir aucune information sur son contenu.

Authentification.
Un adversaire ne peut se faire passer pour l'émetteur ou le récepteur.

Intégrité.
Un adversaire ne peut modifier le contenu d'une conversation sans que le destinataire légitime ne puisse s'en apercevoir.

Objectifs de la cryptographie

Confidentialité.
Un adversaire écoutant la communication ne peut obtenir aucune information sur son contenu.

Authentification.
Un adversaire ne peut se faire passer pour l'émetteur ou le récepteur.

Intégrité.
Un adversaire ne peut modifier le contenu d'une conversation sans que le destinataire légitime ne puisse s'en apercevoir.

Non répudiation.
L'émetteur ne doit pas pouvoir nier ultérieurement l'envoi d'un message.

Historique.

- Machine de chiffrement électromécanique
- Brevetée en 1918 par Arthur Scherbius

Historique.

- Machine de chiffrement électromécanique
- Brevetée en 1918 par Arthur Scherbius
- Utilisée par les Allemands pendant la 2^{e} guerre mondiale

Enigma

Historique.

- Machine de chiffrement électromécanique
- Brevetée en 1918 par Arthur Scherbius
- Utilisée par les Allemands pendant la 2^{e} guerre mondiale
- Cassée par les britanniques, dont Alan Turing, à l'aide de « bombes électromécaniques »

Enigma

Historique.

- Machine de chiffrement électromécanique
- Brevetée en 1918 par Arthur Scherbius
- Utilisée par les Allemands pendant la 2^{e} guerre mondiale
- Cassée par les britanniques, dont Alan Turing, à l'aide de « bombes électromécaniques »
- Le décryptage des messages aurait écourté la guerre de 2 ans

Historique.

- Machine de chiffrement électromécanique
- Brevetée en 1918 par Arthur Scherbius
- Utilisée par les Allemands pendant la 2^{e} guerre mondiale
- Cassée par les britanniques, dont Alan Turing, à l'aide de « bombes électromécaniques »
- Le décryptage des messages aurait écourté la guerre de 2 ans

Comment fonctionne-t-elle ?
Pourquoi a-t-elle été si difficile à casser ?

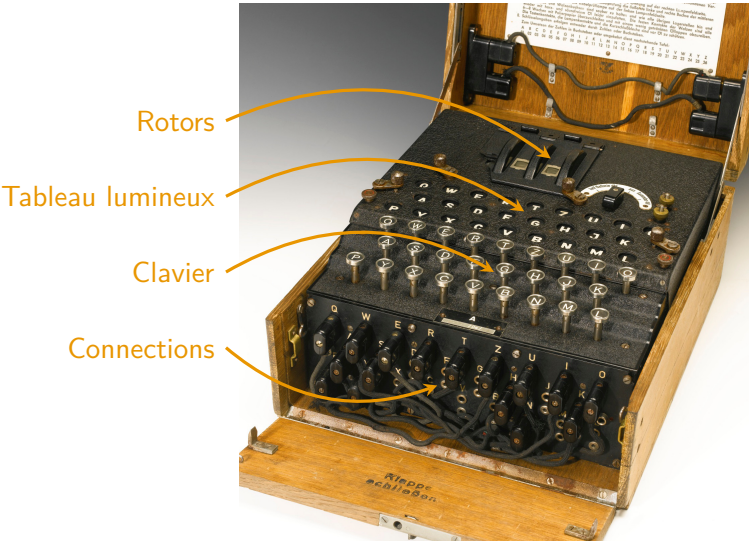
Vue d'ensemble

Vue d'ensemble

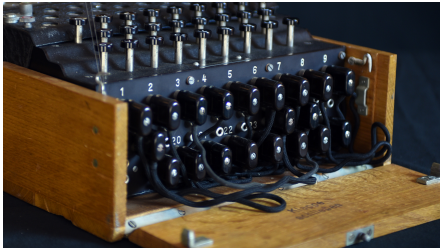
Vue d'ensemble

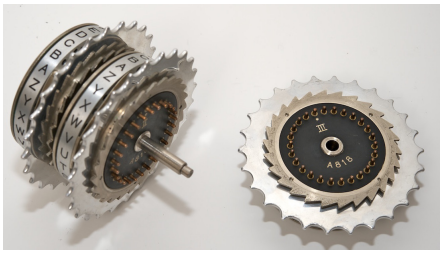
Vue d'ensemble

Vue d'ensemble

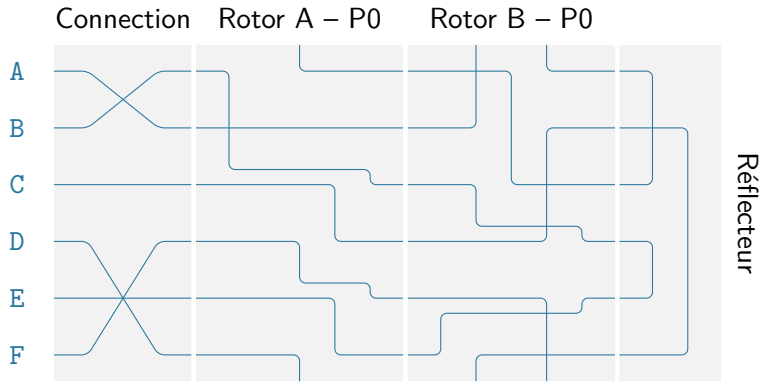


Rotors et tableau de connections





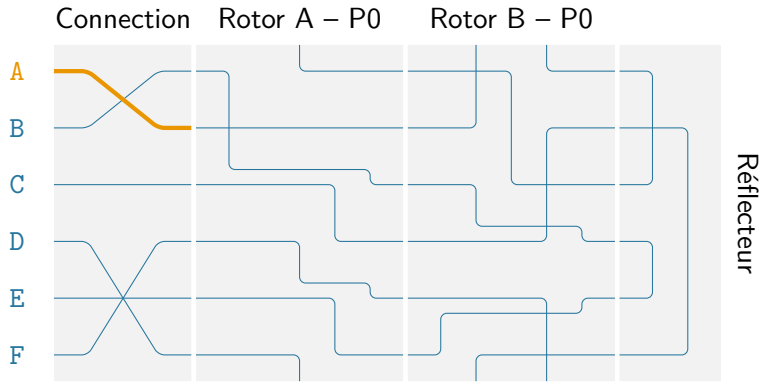
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

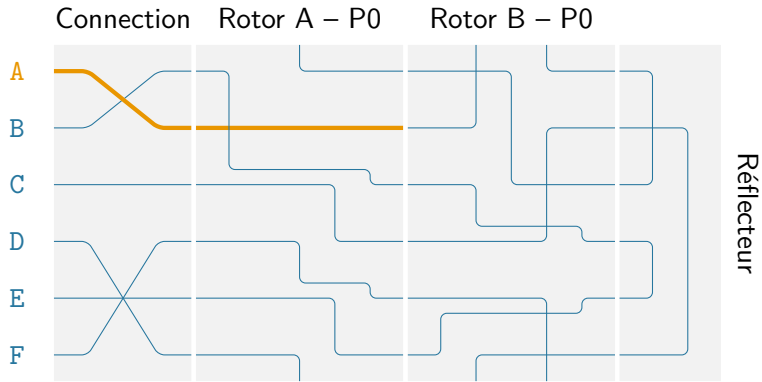
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

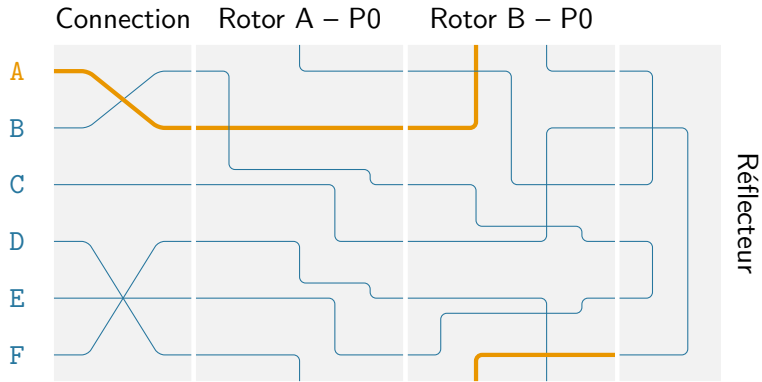
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

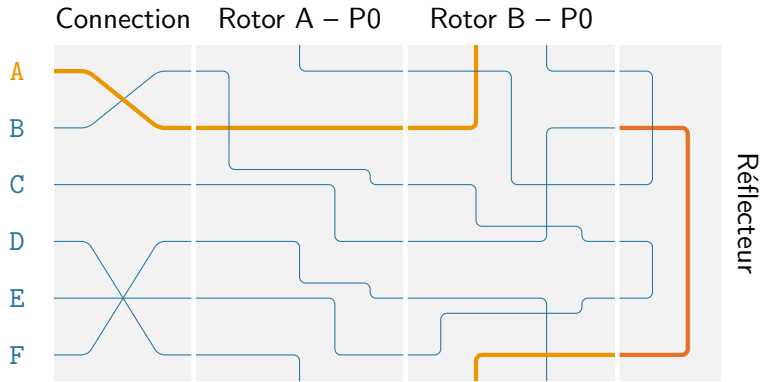
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

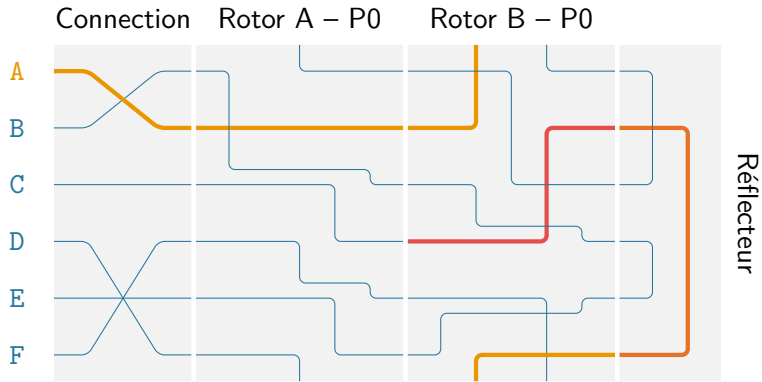
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

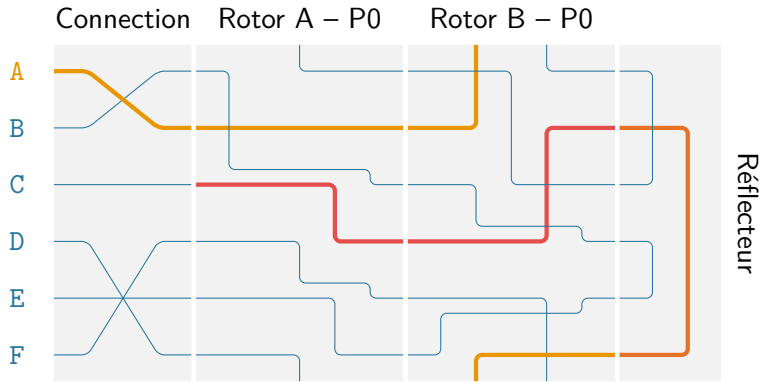
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré :

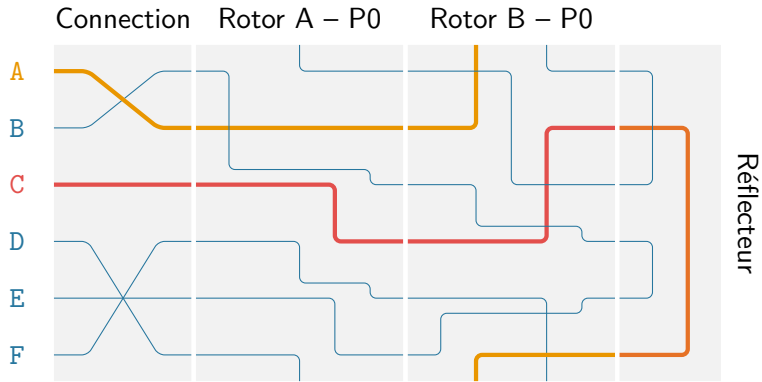
Exemple de chiffrement



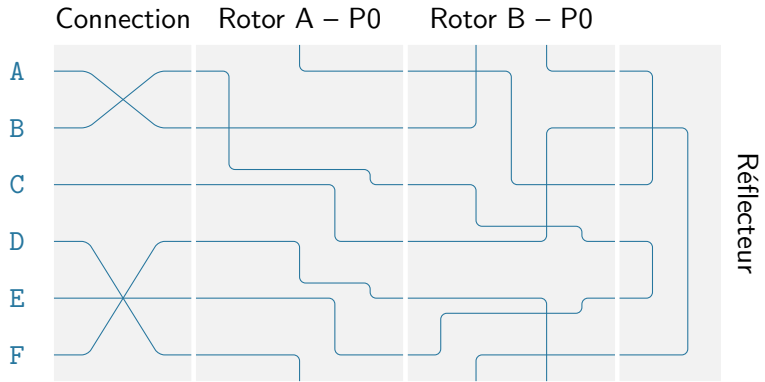
Clair : A A A B B B C C C

Chiffré :

Exemple de chiffrement



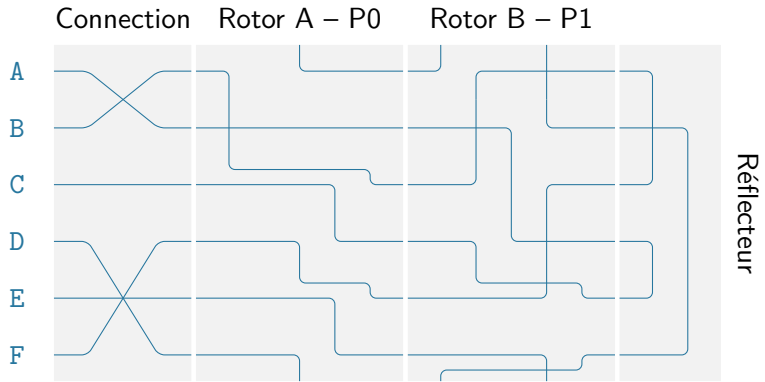
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C

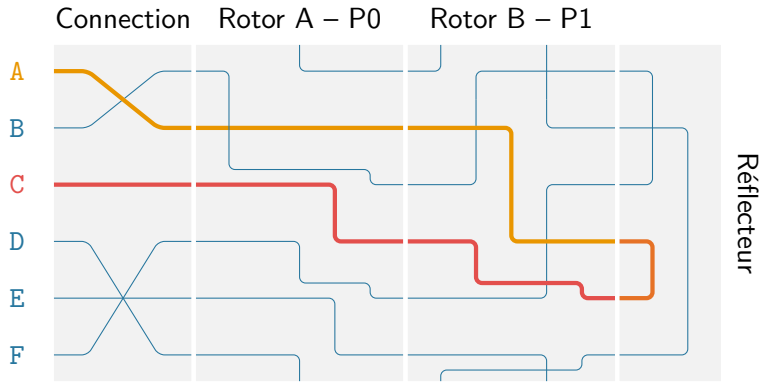
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C

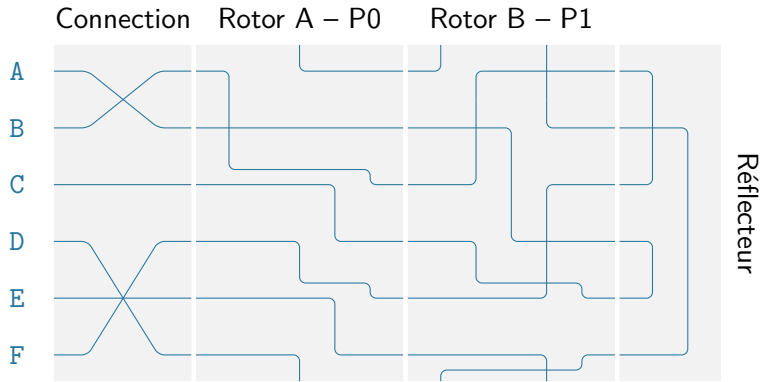
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C

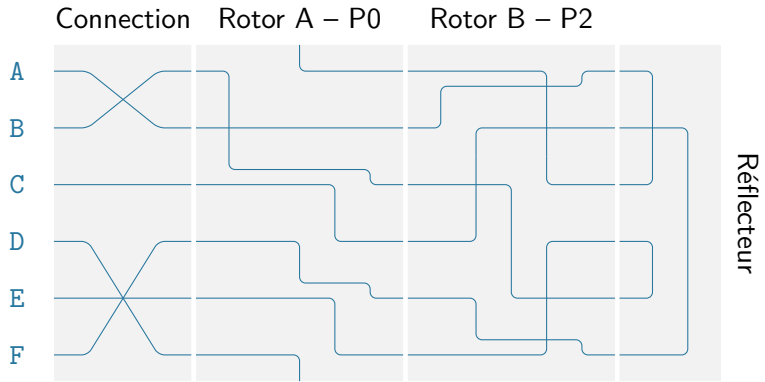
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C

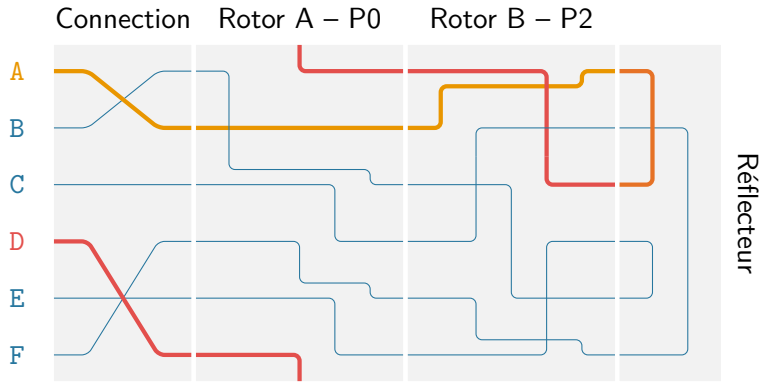
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C

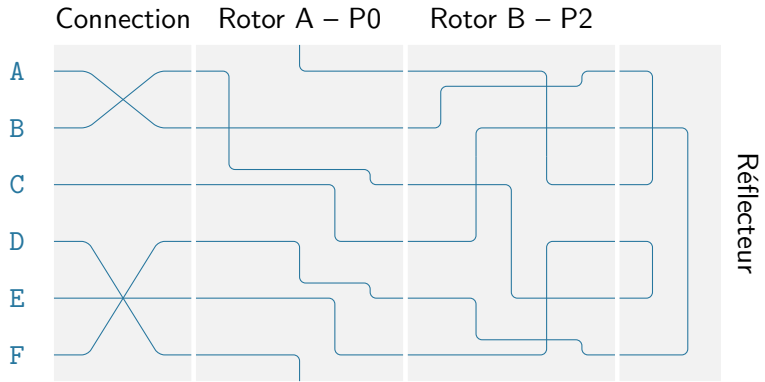
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C D

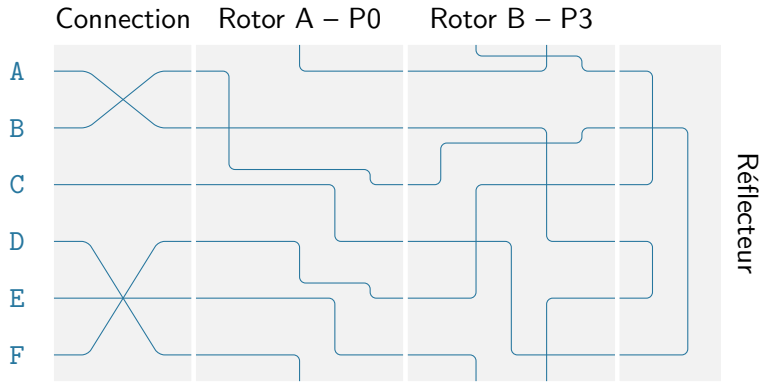
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C D

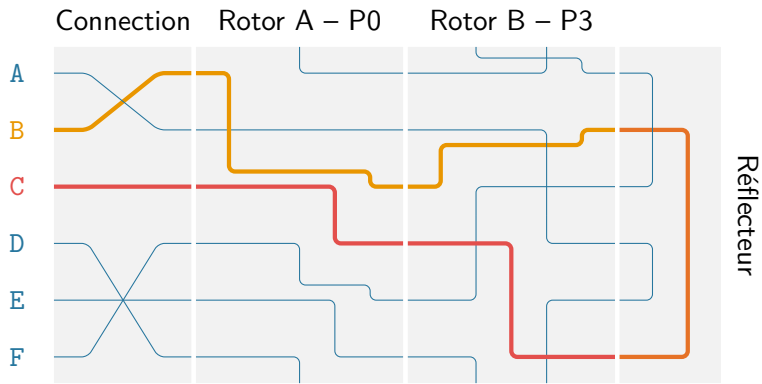
Exemple de chiffrement



Clair : A A A B B B C C C

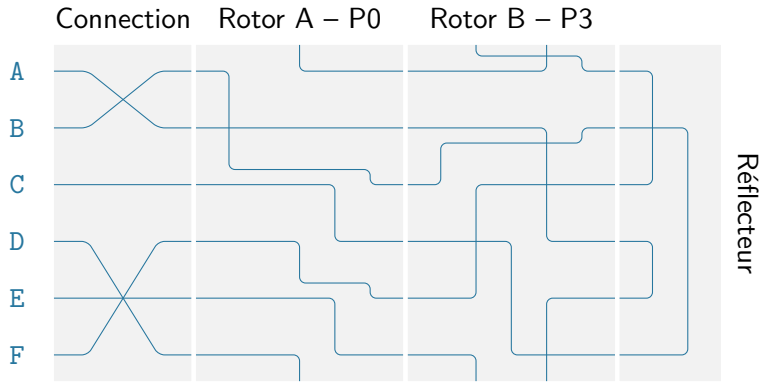
Chiffré : C C D

Exemple de chiffrement



Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C					

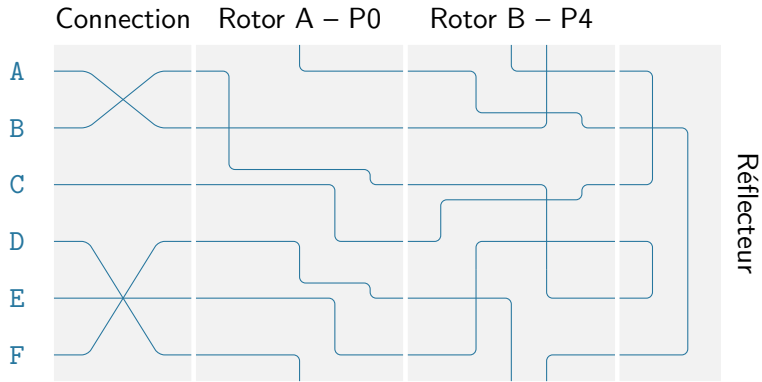
Exemple de chiffrement



Clair : A A A B B B C C C

Chiffré : C C D C

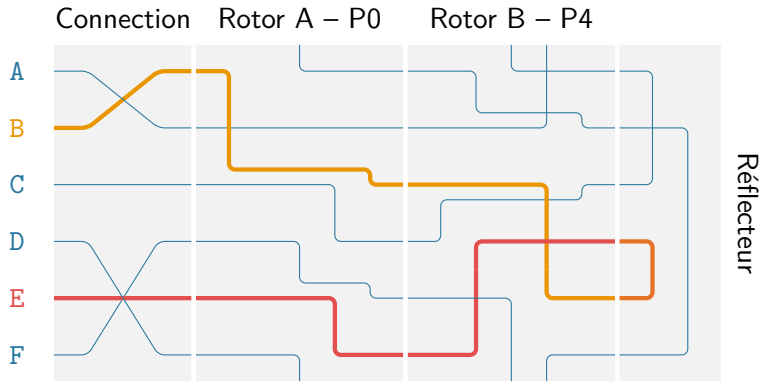
Exemple de chiffrement



Clair : A A A B B B C C C

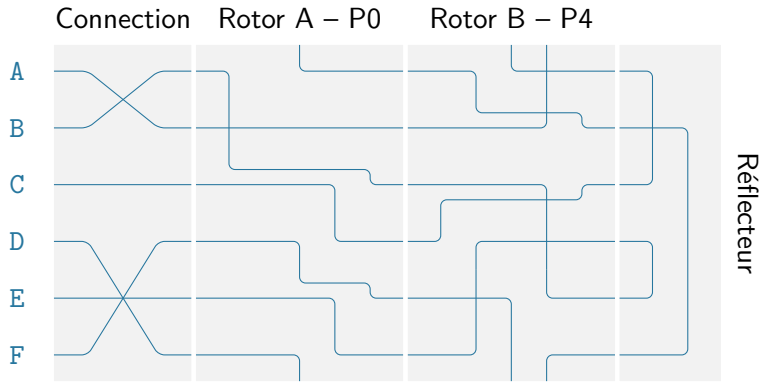
Chiffré : C C D C

Exemple de chiffrement



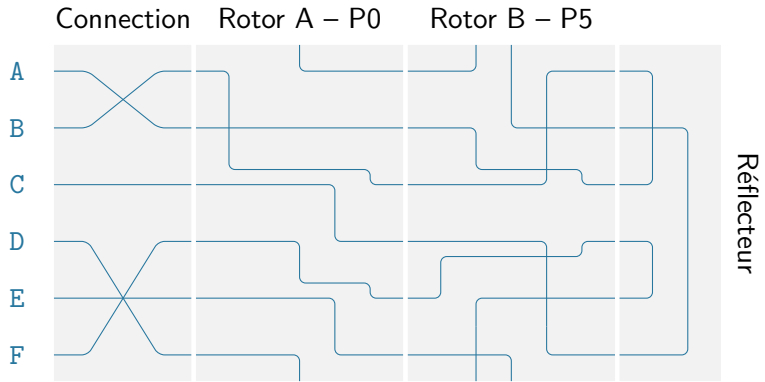
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E				

Exemple de chiffrement



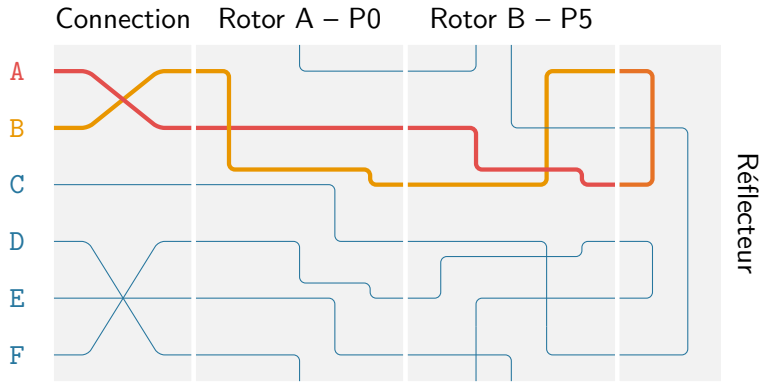
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E				

Exemple de chiffrement



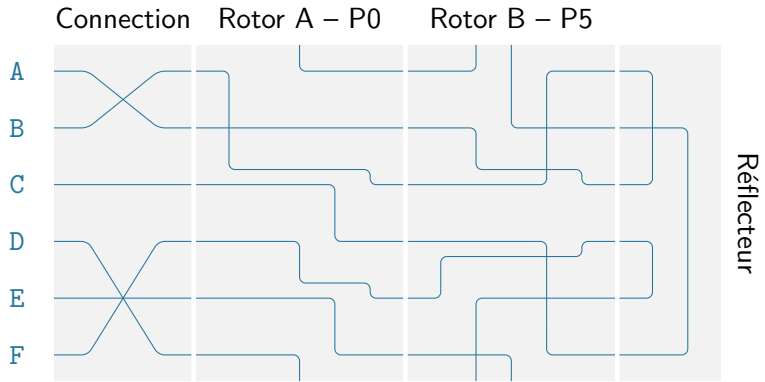
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E				

Exemple de chiffrement



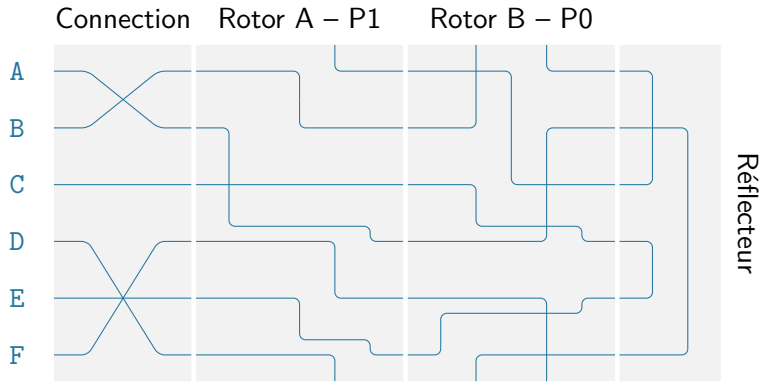
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A			

Exemple de chiffrement



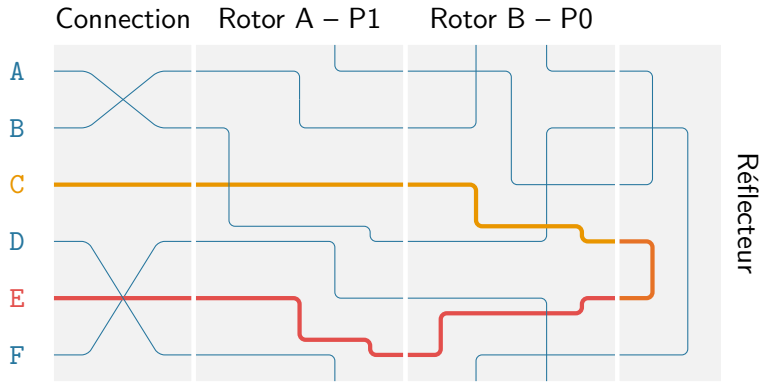
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A			

Exemple de chiffrement



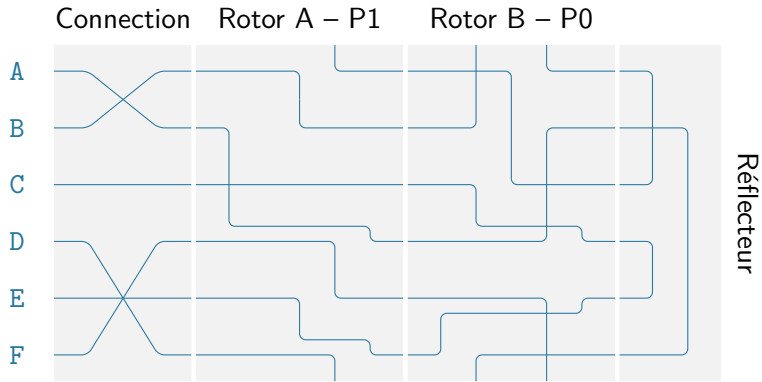
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A			

Exemple de chiffrement



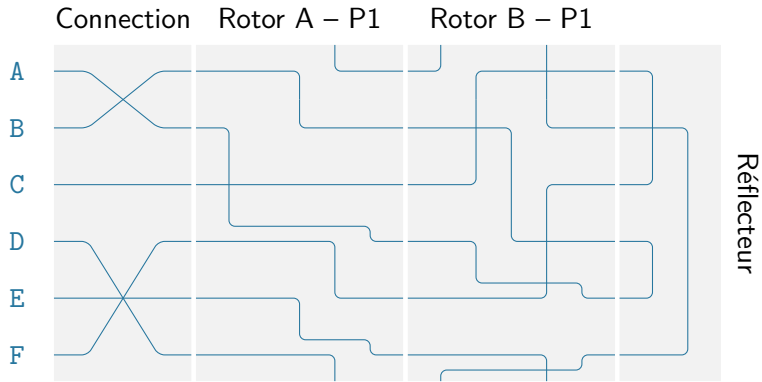
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E		

Exemple de chiffrement



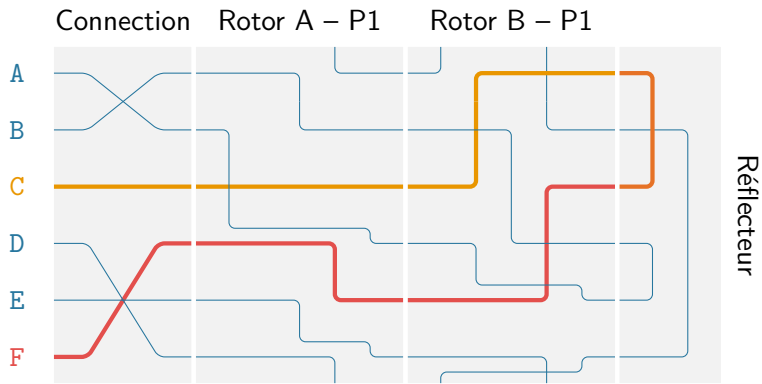
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E		

Exemple de chiffrement



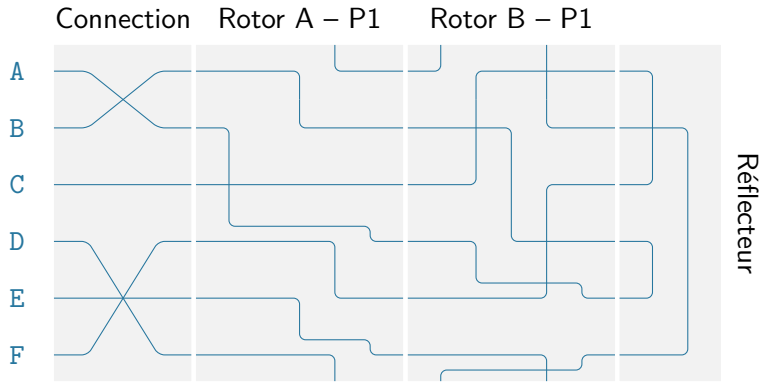
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E		

Exemple de chiffrement



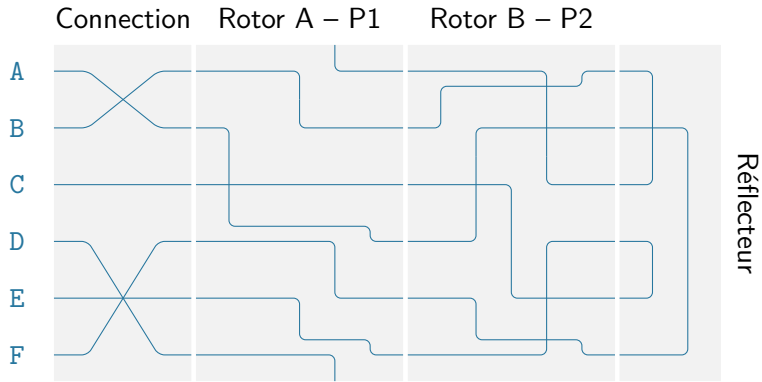
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E	F	

Exemple de chiffrement



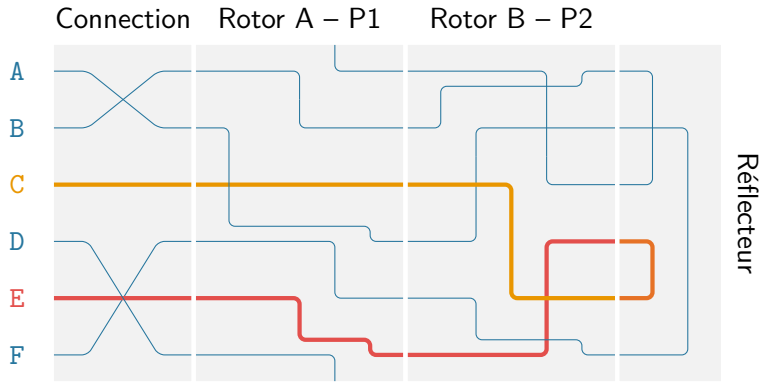
Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E	F	

Exemple de chiffrement



Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E	F	

Exemple de chiffrement



Clair :	A	A	A	B	B	B	C	C	C
Chiffré :	C	C	D	C	E	A	E	F	E

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

$\Rightarrow$ $5 \times 4 \times 3$ possibilités

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

$\Rightarrow$ $5 \times 4 \times 3$ possibilités

Positions initiales des rotors.

- 26 choix pour le premier
- 26 pour le second
- 26 pour le dernier

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

$\Rightarrow$ $5 \times 4 \times 3$ possibilités

Positions initiales des rotors.

- 26 choix pour le premier
- 26 pour le second
- 26 pour le dernier

$\Rightarrow$ $26^3 = 17576$ possibilités

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

$\Rightarrow 5 \times 4 \times 3$ possibilités

Positions initiales des rotors.

- 26 choix pour le premier
- 26 pour le second
- 26 pour le dernier

$\Rightarrow 26^3 = 17576$ possibilités

Tableau de connections.

- 1^{er} câble : $26 \times 25 / 2$
- 2^{e} câble : $24 \times 23 / 2$
- ...
- 10^{e} câble : $8 \times 7 / 2$

Nombre de configurations

Choix des rotors.

- 5 choix pour le premier
- 4 pour le second
- 3 pour le dernier

$\Rightarrow 5 \times 4 \times 3$ possibilités

Positions initiales des rotors.

- 26 choix pour le premier
- 26 pour le second
- 26 pour le dernier

$\Rightarrow 26^3 = 17576$ possibilités

Tableau de connections.

- 1^{er} câble : $26 \times 25 / 2$
- 2^{e} câble : $24 \times 23 / 2$
- ...
- 10^{e} câble : $8 \times 7 / 2$

Tableau de connections.

Le tout divisé par 10! puisque l'ordre ne compte pas !

$$\frac{26!}{6! \times 10! \times 2^{10}} \text{ possibilités}$$

Nombre de configurations

Bilan

158 962 555 217 826 360 000 $\approx 2^{67}$ configurations possibles

Nombre de configurations

Bilan

158 962 555 217 826 360 000 $\approx 2^{67}$ configurations possibles

Exemple. Sur mon portable :

- 2^{30} opérations $\approx 1,5$ s

Nombre de configurations

Bilan

158 962 555 217 826 360 000 $\approx 2^{67}$ configurations possibles

Exemple. Sur mon portable :

- 2^{30} opérations $\approx 1,5$ s
- 2^{55} opérations ≈ 1 an

Nombre de configurations

Bilan

158 962 555 217 826 360 000 $\approx 2^{67}$ configurations possibles

Exemple. Sur mon portable :

- 2^{30} opérations $\approx 1,5$ s
- 2^{55} opérations ≈ 1 an
- 2^{67} opérations ≈ 4000 ans

Nombre de configurations

Bilan

158 962 555 217 826 360 000 $\approx 2^{67}$ configurations possibles

Exemple. Sur mon portable :

- 2^{30} opérations $\approx 1,5$ s
- 2^{55} opérations ≈ 1 an
- 2^{67} opérations ≈ 4000 ans

Un déchiffrement avec Enigma requiert plusieurs opérations ...

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même
- On fait alors des hypothèses sur la configuration

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même
- On fait alors des hypothèses sur la configuration
- Puis on essaye de trouver une contradiction

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même
- On fait alors des hypothèses sur la configuration
- Puis on essaye de trouver une contradiction

Exemple.

- On suppose que le premier rotor est en position 0

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même
- On fait alors des hypothèses sur la configuration
- Puis on essaye de trouver une contradiction

Exemple.

- On suppose que le premier rotor est en position 0
- Si on trouve une contradiction

Alors comment a-t-elle été cassée ?

Des propriétés réduisant l'espace de recherche.

- Exemple : une lettre ne peut être chiffrée en elle-même
- On fait alors des hypothèses sur la configuration
- Puis on essaye de trouver une contradiction

Exemple.

- On suppose que le premier rotor est en position 0
- Si on trouve une contradiction
  - on élimine $\frac{1}{26}$ des configurations
  - soit 6 113 944 431 454 860 000 configurations

Questions

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Sur mon portable.

- 2^{30} op ≈ 1.5 s

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Sur mon portable.

- 2^{30} op ≈ 1.5 s
- 2^{55} op ≈ 1 an

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Sur mon portable.

- 2^{30} op ≈ 1.5 s
- 2^{55} op ≈ 1 an
- 2^{89} op $\approx$ age de l'univers

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Sur mon portable.

- 2^{30} op ≈ 1.5 s
- 2^{55} op ≈ 1 an
- 2^{89} op $\approx$ age de l'univers
- 2^{128} op $\approx 10^{12} \times$ age de l'univers

Bonus : les ordres de grandeur en cryptologie

Quelques nombres en puissance de 2.

- Une année : $60^2 \times 24 \times 365 \approx 2^{25}$ secondes
- Age de l'univers : $13.8 \times 10^9 \approx 2^{34}$ années
- Nombre d'atomes sur terre : $10^{50} \approx 2^{166}$
- Nombre d'atomes dans l'univers (observable) : $10^{80} \approx 2^{266}$

Sur mon portable.

- 2^{30} op $\approx$ 1.5 s
- 2^{55} op $\approx$ 1 an
- 2^{89} op $\approx$ age de l'univers
- 2^{128} op $\approx 10^{12} \times$ age de l'univers

Tailles de clés actuelles.

- 128 bits
- 196 bits
- 256 bits