Rencontre avec les lauréats de Paris — 14 juin 2017

Cryptanalyse d'Enigma

Razvan Barbulescu

Table des matières

Permutation

Definition

Soit n un entier positif. Une permutation de l'ensemble $\{1, \ldots, n\}$ est une façon de réarranger les nombres de 1 à n. Plus formélement une permutation est une application de $\{1, \ldots, n\}$ dans lui-même.

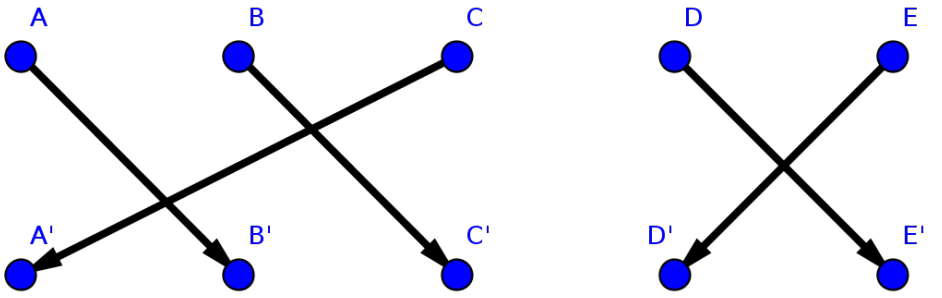
Example

On écrit

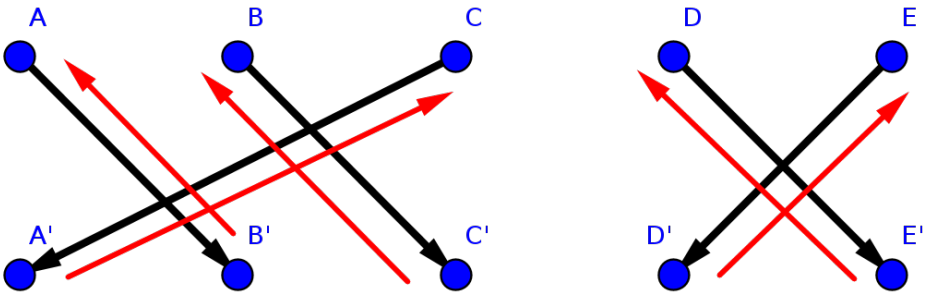
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

pour désigner la permutation qui envoie 1 sur 2, 2 sur 3, 3 sur 1 et échange 4 et 5. Dans la suite on l'appelle σ.

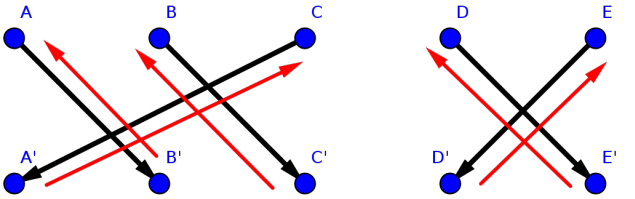
Permutation inverse : definition

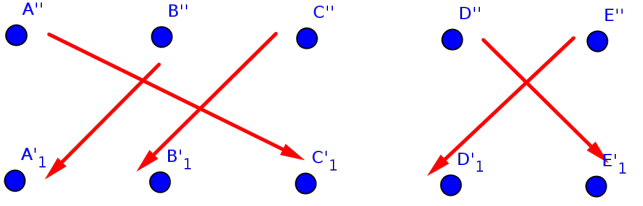


Permutation inverse : definition



Permutation inverse : definition





Permutation inverse : calcul et propriété

Calcul

1. On échange les deux lignes de la permutation.
2. On trie les colonnes pour que la nouvelle ligne soit en ordre croissant.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Permutation inverse : calcul et propriété

Calcul

1. On échange les deux lignes de la permutation.
2. On trie les colonnes pour que la nouvelle ligne soit en ordre croissant.

$$\begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Permutation inverse : calcul et propriété

Calcul

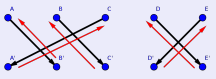
1. On échange les deux lignes de la permutation.
2. On trie les colonnes pour que la nouvelle ligne soit en ordre croissant.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

Théorème

1. Appliquer une permuation puis son inverse revient à laisser la liste $1, \ldots, n$ inchangée (permutation identité).
2. Appliquer la permutation inverse puis la permutation revient à à laisser la liste $1, \ldots, n$ inchangée (permutation identité).

Démonstration



Il s'agit de suivre une flêche noir puis une flêche rouge dans le premier cas et une flêche rouge puis une flêche noir dans le deuxième cas.

Orbites d'une permutation

Example

Si on répète la permutation de l'exemple 1 fois, 2 fois, etc. alors le nombre 1 arrive successivement dans les positions

$$2, 3, 1, 2, 3, 1, 2, 3, 1, \ldots.$$

De même le nombre 4 arrive successivemnt dans les positions $5, 4, 5, 4, \ldots$.

Definition

- L'orbite d'un nombre i par une permutation donnée est la liste de ses valeurs avant de revenir sur soi-même.
- Le motif de décompositon d'une permutation est la liste des longueurs de ses orbites triée par ordre croissant.

Example

Les orbites de σ sont $\{(123), (45)\}$ donc son motif de décomposition est $(2, 3)$.

Table des matières

Histoire

- 1923 Scherbius : commercialise la machine pour 30000 euros pour le secret industriel ; échec finnancier.
- 1926 : la marine allemande achète Enigma.
- 1931 : ministère français de défense paie une taupe au sein des services secrets Allemands et obtient les plans d'Enigma
- 1933 : les mathématiciens polonais cassent les codes, mais Enigma est modfiée régulièrement
- 1940 : les mathématiciens anglais dirigés par Alain Turing cassent les versions successives d'Enigma, à l'aide de l'ordinateur Colossus.

Utilisation d'Enigma

Utilisation

1. Une personne tape le message claire sur le clavier, en laissant passer une seconde après chaque lettre.
2. Une deuxième personne lit la lettre qu'affiche la machine et la note sur un bout de papier, de façon qu'elle obtient le texte chiffré.

Maths from the talk
"Alan Turing and the Enigma Machine"
James Grime

1 The Enigma Machine

By the beginning of the 20th century it had become possible, and necessary, to mechanise encryption. In 1918 a German engineer named Arthur Scherbius patented the Enigma Machine. Originally it was sold to banks, military companies and other organisations who needed to send secret information. By the mid-1920s the German military started to use the Enigma Machine, with some differences from the commercial version of the machine. Enigma was used by the German military throughout World War II, therefore breaking the enigma cipher became a top priority, first by the Polish, then later by the British and Americans.

The Enigma Machine was an electro-mechanical machine, about the size of a typewriter, made with steel casing inside a wooden box. On the outside you will see two sets of letters which were the keyboard (input) and lamps (output). To encode a message using the keyboard, the message would then be encrypted letter by letter. The lamps would light up, so paper the encrypted letter would light up on keyboard. The encrypted message would then be written down by the operator and would be transmitted by radio. The machine itself did not transmit.

Essentially, the Enigma Machine is just a large circuit. When you type in a letter on the Enigma Machine it completes a circuit and lights up a letter on the lampboard.

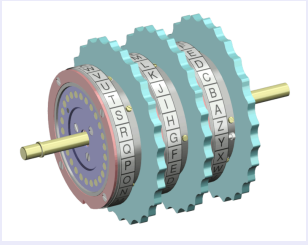
The Enigma Machine has five components.

- Rotors 1, 2 and 3. Inside each rotor is a criss-cross of wires, connecting each letter to another in the manner of a general substitution cipher.

1

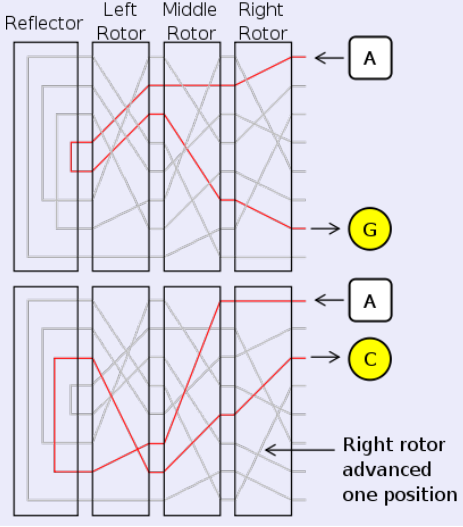
3. Le message est émis par la radio et réceptionné par une autre unité.
4. Deux autres personnes déchiffre le message avec une machine Enigma identique, réglée avec les mêmes paramètres.

Règlages d'Enigma

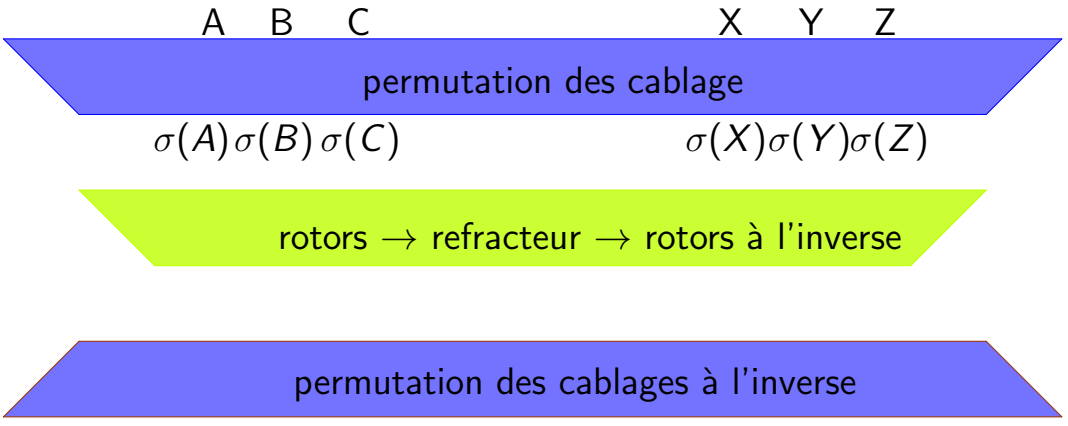


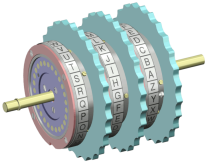
La clé secrète :

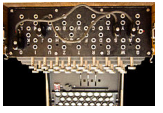
- certaines paires de lettres sont échangées en branchant des cables ;
- les 3 rotors sont mis dans une certaine position déterminée par 3 lettres.



Enigma schématisée







Quand on appuie sur une touche étiquetée de A à Z

on allume une ampoule étiquetée de A à Z. Pour savoir quelle lettre s'allume il faut suivre les cables :

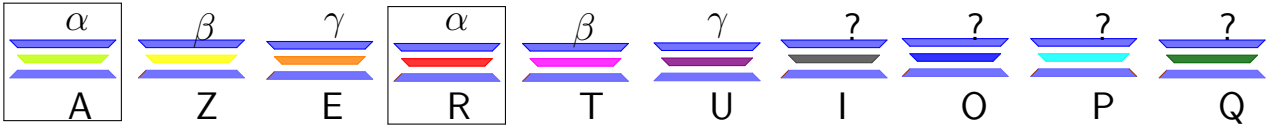
1. on passe par un des cables brachés sur la partie frontale de la machine
2. on traverse les rotors une fois
3. on passe par des cables fixes au fond de la machine
4. on traverse les rotors une deuxième fois, en sens inverse
5. on passe de nouveau par les cables branchés dans la partie avant, mais en sens inverse.

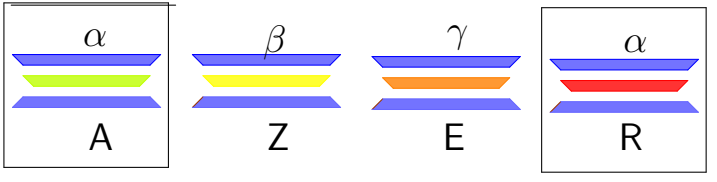
Table des matières

Idée des mathématiciens polonais

Protocole des militaires allemands

- Chaque jour à minuit on régle toutes les machines Enigma de manière identique.
- Chaque message commence par un groupe de la forme $\alpha\beta\gamma\alpha\beta\gamma$ chiffré avec Enigma remise au réglage du jour et continue avec le message proprement-dit chiffré avec $\alpha\beta\gamma$.

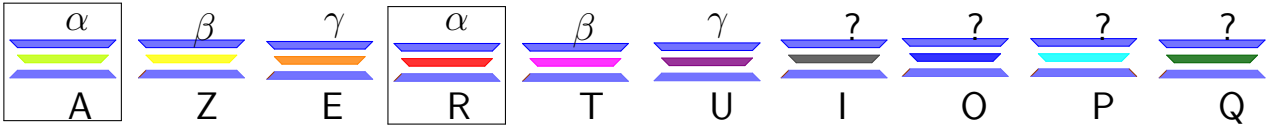


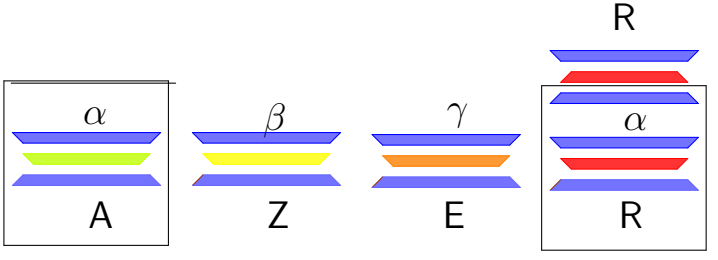


Idée des mathématiciens polonais

Protocole des militaires allemands

- Chaque jour à minuit on régle toutes les machines Enigma de manière identique.
- Chaque message commence par un groupe de la forme $\alpha\beta\gamma\alpha\beta\gamma$ chiffré avec Enigma remise au réglage du jour et continue avec le message proprement-dit chiffré avec $\alpha\beta\gamma$.

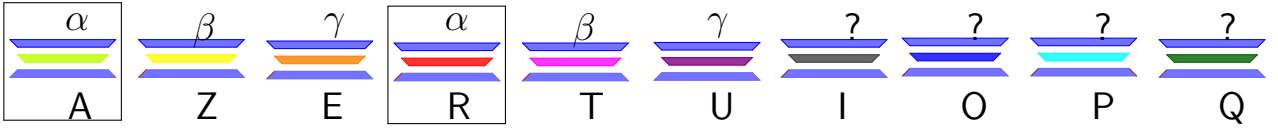


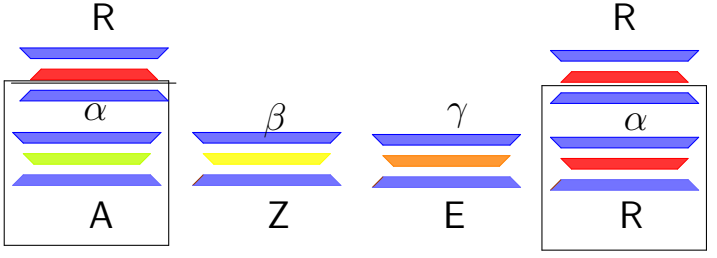


Idée des mathématiciens polonais

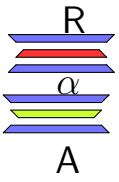
Protocole des militaires allemands

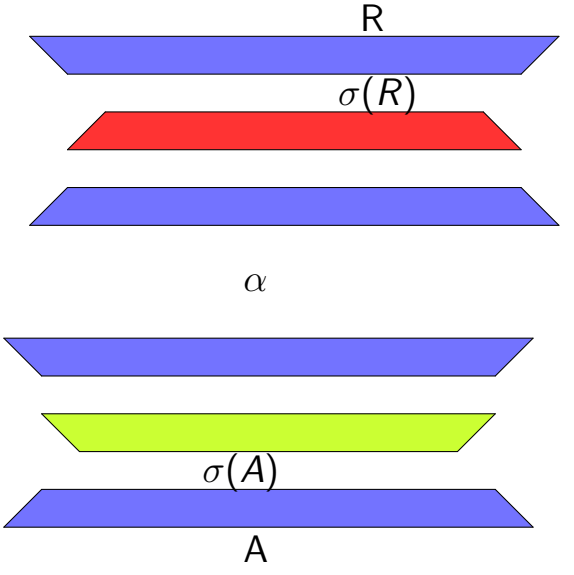
- Chaque jour à minuit on régle toutes les machines Enigma de manière identique.
- Chaque message commence par un groupe de la forme $\alpha\beta\gamma\alpha\beta\gamma$ chiffré avec Enigma remise au réglage du jour et continue avec le message proprement-dit chiffré avec $\alpha\beta\gamma$.





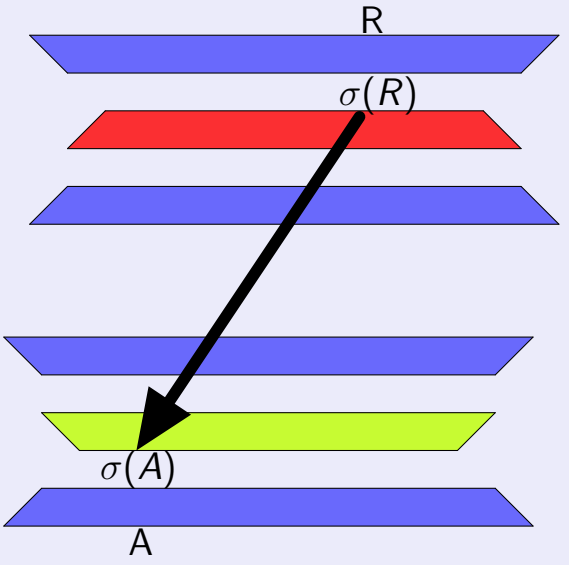
Deux Enigma bout-à-bout

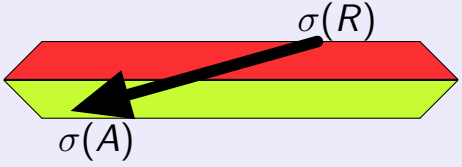




Chaque message intercepté

L'effet de la permutation bleue et celui de son inverse s'annulent





Chaque jour les Allemands envoyaient ≈ 200 messages

Un message donne $\sigma(R) \mapsto \sigma(A)$, un autre $\sigma(B) \mapsto \sigma(T)$ etc. On connait donc la taille des orbites de la permutation rouge-verte.

Méthode

Remarque importante

On connait la taille des orbites de la permutation correspondant aux rotors suivie par la permutation des rotors après l'encodage de 3 lettres à l'inverse.

Methode pour craquer Enigma

1. calculer la charactéristique de la permutation (vert-rouge) ;
2. enumérer les $26^3 = 17576$ réglages des rotors et garder la liste de ceux pour lesquels la permutation verte-rouge a la caractéristique recherchée (très faible nombre, on peut supposer qu'on a trouvé la position des rotors).
3. on teste toutes les 230230 possiblités des cablages, en gardant ceullement celle qui donne une phrase en allemand.

C'est rapide car on utilise des machines et car

on fait $17576 + 230230 = 247806$ essais au lieu de $17576 \cdot 230230 = 4046522480$ essais.

Table des matières

Erreur des Allemands

Envoyer un message prévisible

- Certains soldats émetteur commençaient la journée en réglant la machine et, fiers de leur bon travail, envoyaient le message "Rien à signaler".
- Beaucoup d'unités envoyaient le rapport météo : "wetter bericht". Les mots devignés s'appellent "cribs".

Question

Il suffit de tester toutes les positions des rotors et toutes les positions des cablages et de garder celle qui correspond.

Erreur des Allemands

Envoyer un message prévisible

- Certains soldats émetteur commençaient la journée en réglant la machine et, fiers de leur bon travail, envoyaient le message "Rien à signaler".
- Beaucoup d'unités envoyaient le rapport météo : "wetter bericht". Les mots devignés s'appellent "cribs".

Question

Il suffit de tester toutes les positions des rotors et toutes les positions des cablages et de garder celle qui correspond.

Solution

Turing est l'inventeur de l'ordinatuer pour avoir publié une construction mathématique appelée aujourd'hui "machine de Turing". Il a supervisé la construction du premier ordinateur utilisé pour résoudre un grand problème. C'était pour casser Enigma...

Si les Allemands faisaient cette erreur les Anglais cassaient le code en 20 minutes.

Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

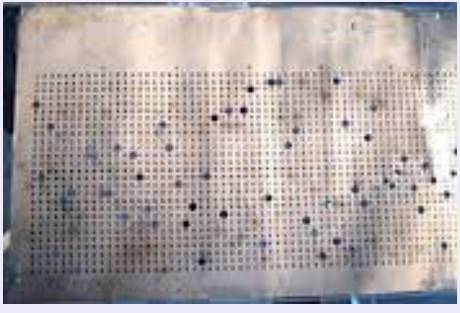
Les banburismes

A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f
r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

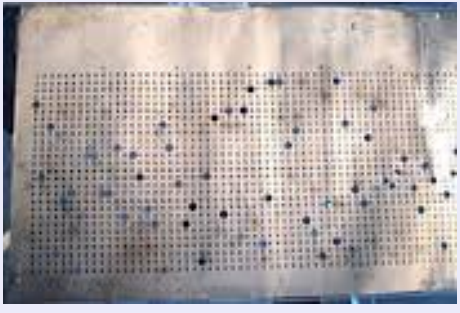
Les banburismes

A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f
r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

Les banburismes

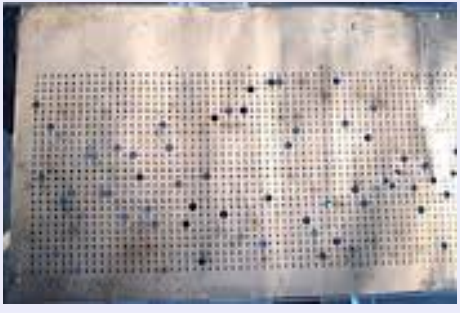
A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f

r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

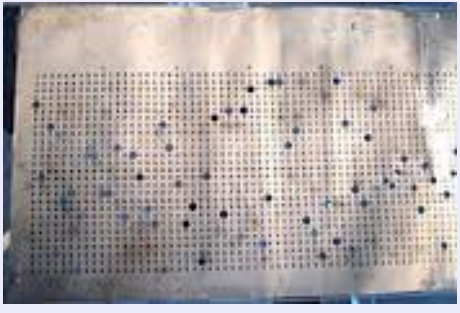
Les banburismes

A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f
r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

Les banburismes

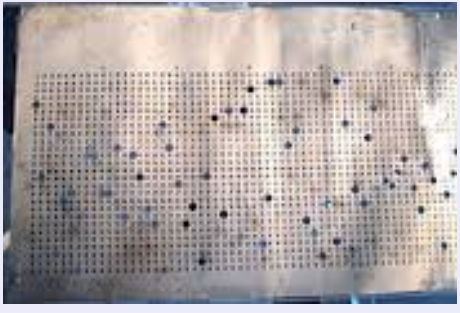
A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f

r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

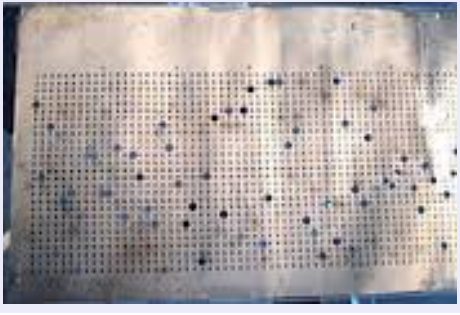
Les banburismes

A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f
r a p p o r t m e t e o

Les Banburismes

Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Les banburismes

Où placer le crib "rapport météo"

Disons qu'on a reçu le message chiffré "sxwyroamptpzomhe". Chaque position possible prend 20 minutes à tester, donc on peut tester seulement 72 positions avant que les Allemands changent le réglage des Enigma.

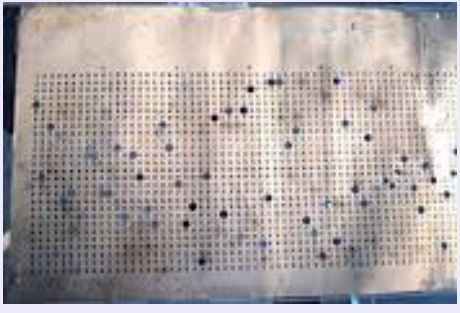
Les banburismes

A cause de la manière dont Enigma est construite une lettre n'est jamais chiffrée par elle même.

s x w y r o a d p t p z o m h e f

Les Banburismes

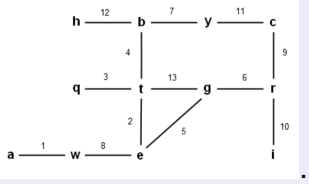
Pour cela on utilisait des bandes de papier produites à Banbury, que l'on faisait glisser.



Le génie de Turing

Idée d'algorithmique

1. Plutôt que de passer beaucoup de temps sur chaque possibilité, on se prépare en extrayant des informations dans ce qu'on appelle "menu" :



2. Pour chaque possibilité on écrit des calcul sur le brouillon. On ne les gète pas mais on les utilise pour les possibilités suivantes.

   La bombe est un ensemble de copies d'Enigma qui testent en parallèle des possibilités. Turing a branché les diffrérentes copies entre elles de façon a échanger les informations de leur "brouillon".