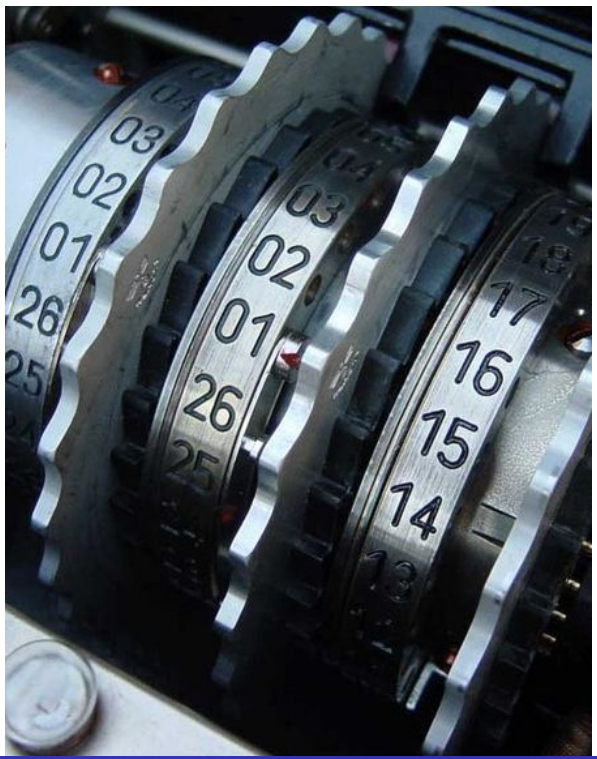
Analyse et implantation de la machine Enigma

Jonathan Amiez Jérôme Dijoux

M1 Informatique
Université Claude Bernard Lyon 1

Composition principale :

- un clavier
- une table de permutations (plugboard)
- des rotors
- une réflecteur



- le tableau de connexions

- permutation de caractères
- jusqu'à $\frac{nb\_caracteres}{2} - 4$ permutations

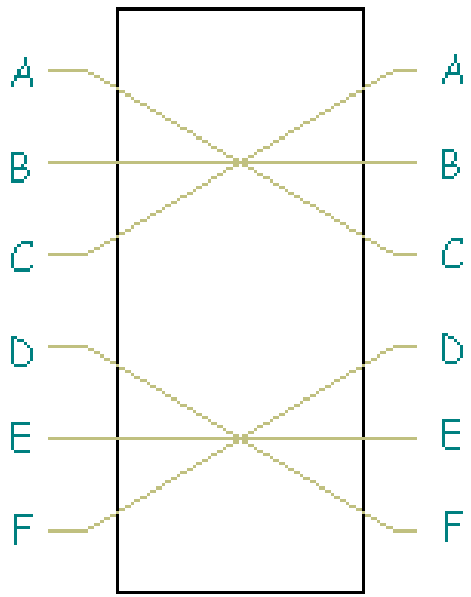
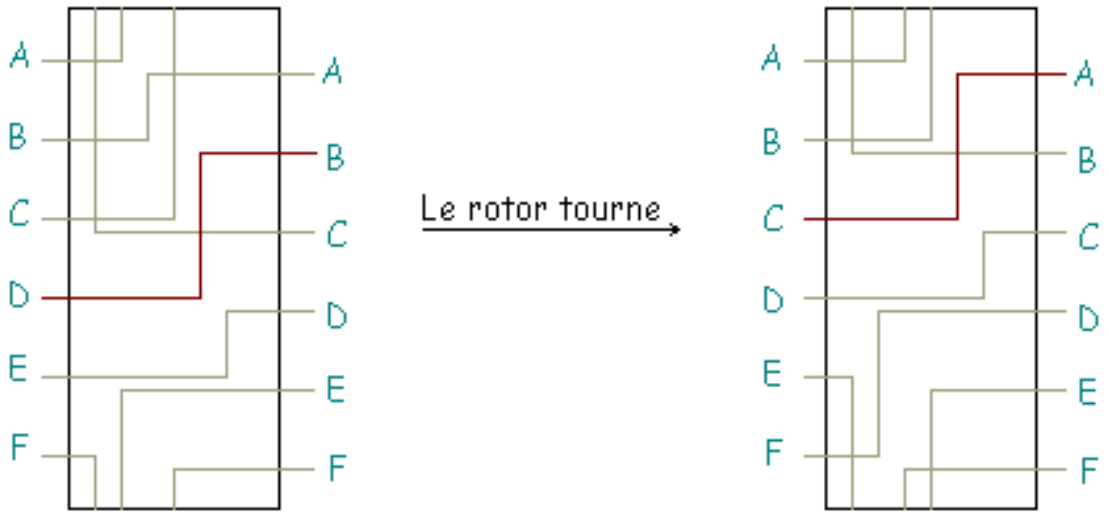


Tableau de connexions

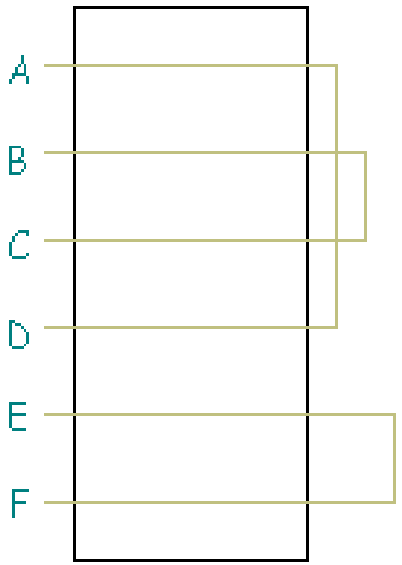
- les rotors

- permutation aléatoire des caractères
- chaque itération génère de nouvelles permutations
- association de 3 à 8 rotors



- le reflecteur

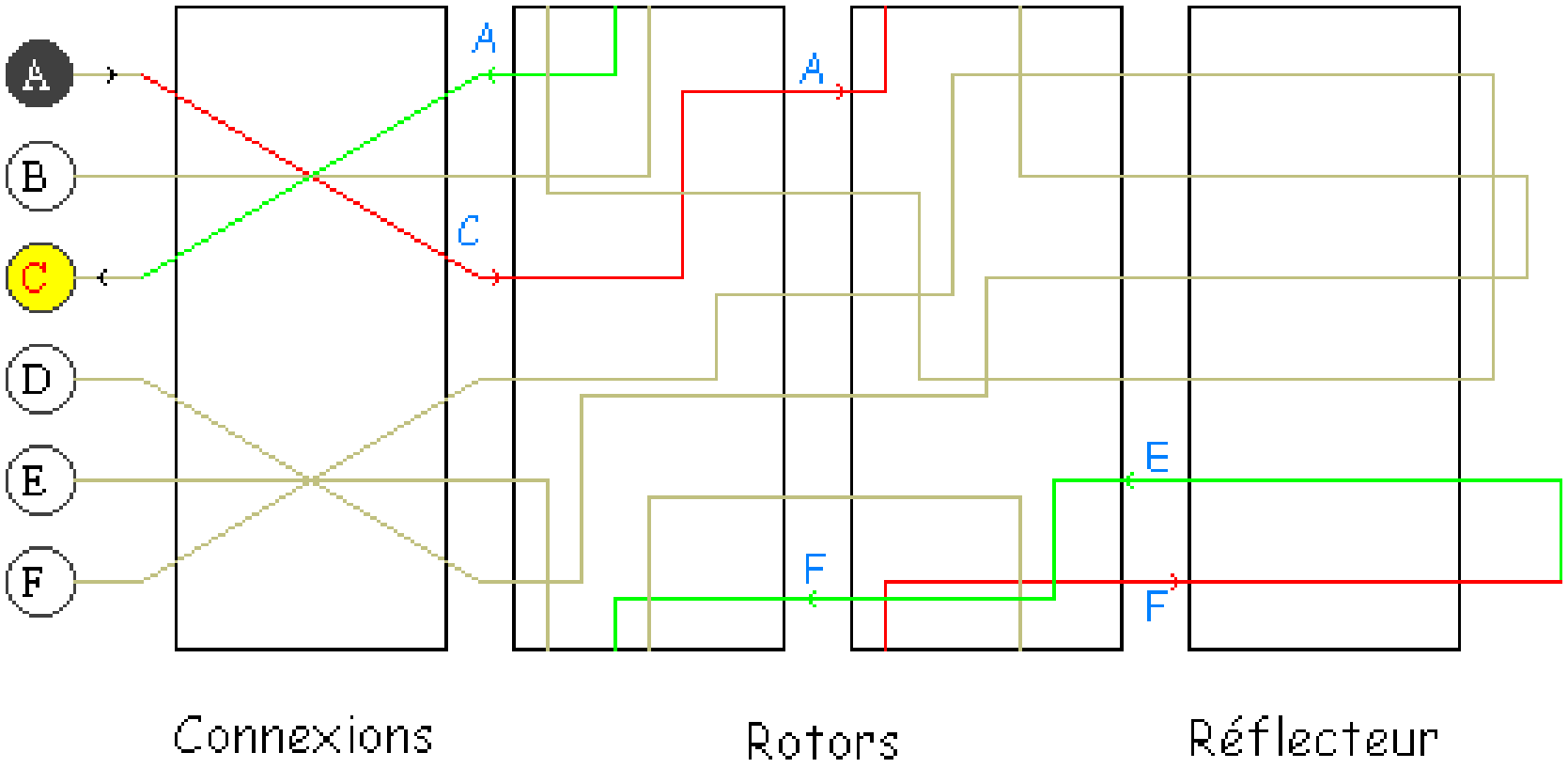
- dernière permutation qui permet de faire le chemin inverse
- permutation de couples d'éléments



A est permuté avec D, B est permuté avec C, et E avec F.

Le réflecteur

- Codage du caractère A en C



- les premières versions de Enigma

- 26^3 positions initiales possibles des rotors
- A_5^3 choix et ordre possible des rotors
- 1.5073827493725^{14} permutations possibles des caractères
- $\approx 2.7939258705 \times 10^{24}$ combinaisons différentes.

- notre version de Enigma

- $94^4 = 78074896$ positions initiales possibles des rotors
- 4 choix de réflecteur possibles
- $A_8^4 = 1680$ choix et ordre possibles des rotors
- $\approx 5.074798513 \times 10^{75}$ permutations de lettres possibles
- $\approx 2.078791373 \times 10^{95}$ combinaisons différentes

Améliorations

- Alphabet de 94 caractères
- 8 rotors
- 4 réflecteurs
- $\longrightarrow 10^{71}\times$ plus de combinaisons !

Clés de configuration

- Chaque élément a une configuration initiale
- La clé décrit ces configurations
- Exemple : A 1573 A/ !V ¡%iz ASml :$\hat{*}$k=o ...

Échange de clés

Problématique

- Robustesse du chiffrage d'Enigma située dans sa configuration
- Nécéssité d'utiliser la même config. pour chiffrer et déchiffrer
- Utilisateurs distants

Échange de clés

Problématique

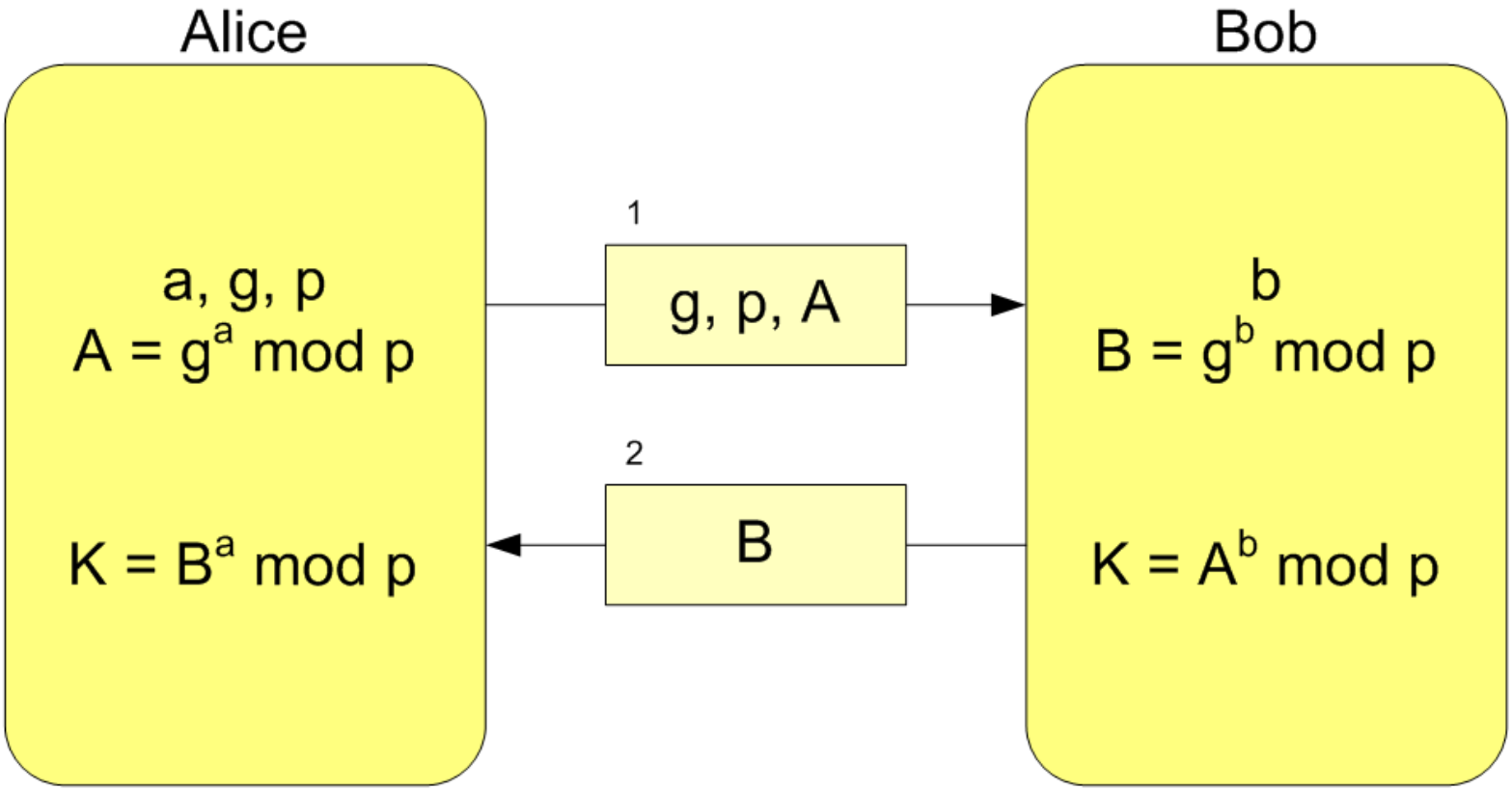
- Robustesse du chiffrage d'Enigma située dans sa configuration
- Nécéssité d'utiliser la même config. pour chiffrer et déchiffrer
- Utilisateurs distants

Solution

- Établir une clé secrète commune aux 2 entités
- $\longrightarrow$ Utiliser l'échange de clé Diffie-Hellman
- Utiliser cette clé pour chiffrer la clé Enigma
- $\longrightarrow$ Implanter un algorithme symétrique

Protocole Diffie-Hellman

Principe



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Algorithme du masque jetable

- Méthode de chiffrage très simple
- Théoriquement impossible à casser sous certaines conditions

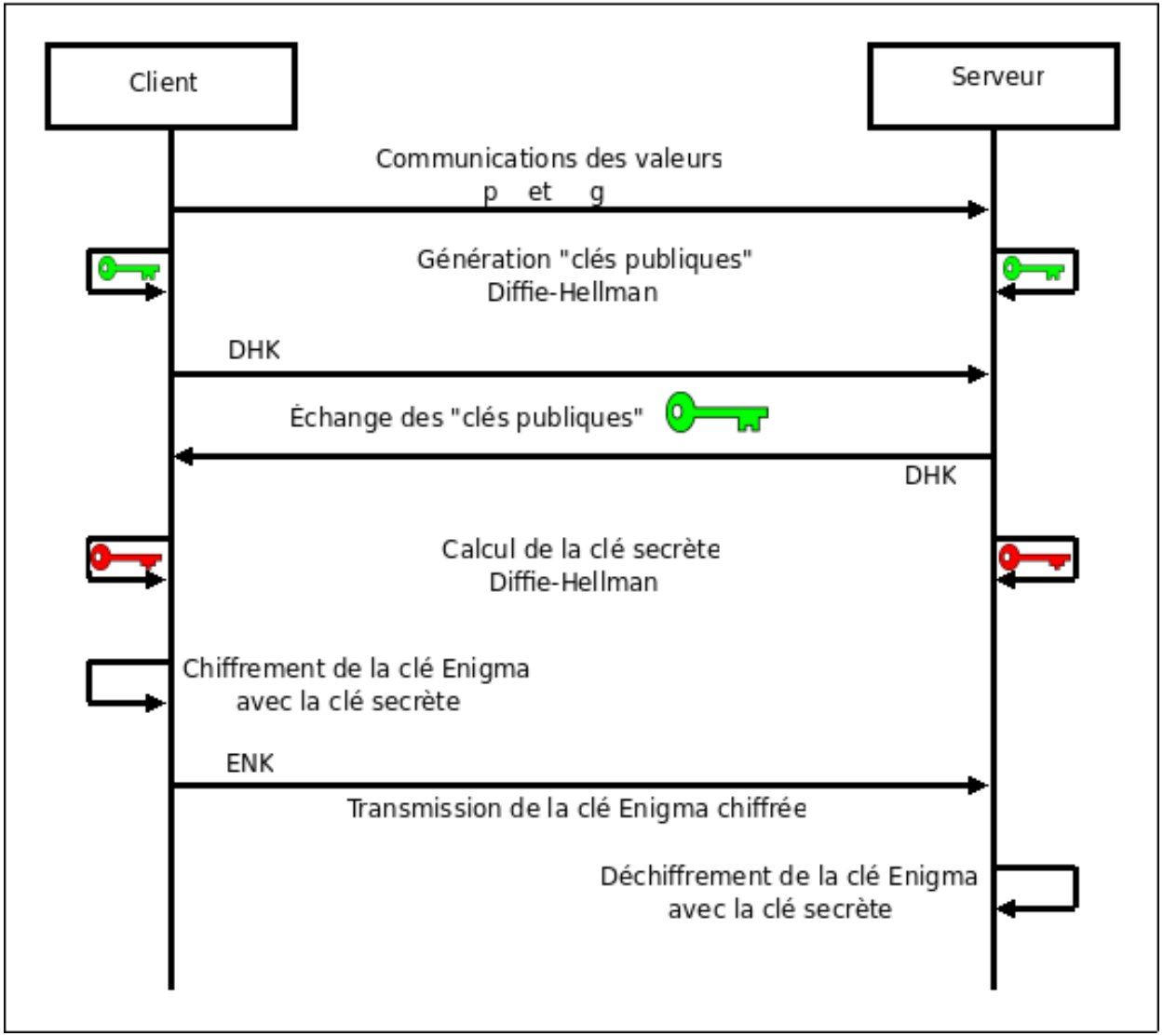
Exemple

- Message : HELLO — Clé : XMCKL

```
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) masque
= 30      16       13      21      25     masque + message
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) masque + message  modulo 26
```

- Message chiffré : EQNVZ

Procédure d'échange



Exemple de message

Message en clair

```
0000  00 e0 18 2a 3b 48 00 1b  fc 75 5f e3 08 00 45 00   ...*;H.. .u_...E.
0010  00 74 13 04 40 00 40 06  a4 26 c0 a8 01 03 c0 a8   .t..@.@. .&......
0020  01 06 8c ef 1a 0a e5 7f  0c 7b 6d 5d d4 05 80 18   ........ .{m]....
0030  00 5c dd cf 00 00 01 01  08 0a 00 79 67 e9 00 05   .\...... ...yg...
0040  23 49 4e 65 71 75 65 20  70 6f 72 72 6f 20 71 75   #INeque  porro qu
0050  69 73 71 75 61 6d 20 65  73 74 20 71 75 69 20 64   isquam e st qui d
0060  6f 6c 6f 72 65 6d 20 69  70 73 75 6d 20 71 75 69   olorem i psum qui
0070  61 20 64 6f 6c 6f 72 20  73 69 74 20 61 6d 65 74   a dolor  sit amet
0080  0d 0a                                             ..
```

Message chiffré

```
0000  00 e0 18 2a 3b 48 00 1b  fc 75 5f e3 08 00 45 00   ...*;H.. .u_...E.
0010  00 80 8e e6 40 00 40 06  28 38 c0 a8 01 03 c0 a8   ....@.@. (8......
0020  01 06 d9 17 1a 0a 97 7b  57 cf 1f 11 52 01 80 18   .......{ W...R...
0030  00 5c de fe 00 00 01 01  08 0a 00 79 e0 09 00 05   .\...... ...y....
0040  dd 45 3f 2c 21 78 2e 20  38 4b 49 7d 6f 20 30 33   .E?,!x.  8KI}o 03
0050  71 61 26 20 5f 63 28 6f  6c 20 6d 70 43 50 7a 20   qa& _c(o l mpCPz
0060  3d 47 52 58 45 20 52 67  5a 4a 5a 20 59 40 30 70   =GRXE Rg ZJZ Y@0p
0070  61 20 5d 6d 52 52 44 20  69 33 26 74 28 20 43 43   a ]mRRD  i3&t( CC
0080  72 6f 75 20 22 5f 23 5f  76 20 36 6b 0d 0a         rou "_#_ v 6k..
```

Quelques Liens

- http://www.ellsbury.com/enigmabombe.htm
- http://en.wikipedia.org/wiki/Enigma_machine
- http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
- http://www.ietf.org/rfc/rfc2631.txt
- http://primes.utm.edu/