Enigma

Inventée par Scherbius au début du XXe siècle, la machine Enigma est une machine électromécanique portative servant au chiffrement et au déchiffrement de l'information. Elle fut utilisée principalement par l'Allemagne nazi lors de la Seconde Guerre mondiale.
Dans sa forme élémentaire, elle consiste en 3 éléments reliés par des câbles : un clavier pour entrer chaque lettre du texte clair, un brouilleur (appelé rotor) qui crypte chaque lettre du texte en clair en une lettre chiffrée, et un tableau lumineux fait d'un certain nombre de lampes pour afficher la lettre du texte crypté. Un exemple est donné dans la figure 1a, sur une version simplifiée de la machine Enigma avec un alphabet réduit à 6 lettres. Lorsqu'on tape "b" sur le clavier, le courant est envoyé dans le rotor où il suit le dessin de son câblage interne et ressort de façon à allumer la lampe "A". Donc "b" est crypté en "A".
Dans ce montage basique, la machine correspond simplement à un chiffre de substitution monoalphabétique. L'idée suivante de Scherbius a été de faire pivoter le rotor automatiquement à chaque fois qu'une lettre est cryptée. Dans l'exemple de la figure 1, la rotation est d'1/6^{e} de tour, mais elle serait d'1/26^{e} de tour dans le cas de l'alphabet complet. Donc si on reprend l'exemple de la figure 1, taper "b" sur le clavier fait éclairer la lettre "A" (figure 1a). Le brouilleur effectue une rotation d'1/6^{e} de tour, ce qui fait que si on retape "b" sur le clavier, la lettre "C" va s'éclairer (figure 1b). Le brouilleur effectue de nouveau une rotation d'1/6^{e} de tour (figure 1c). Avec ce rotor sont définis 6 alphabets chiffrés et la machine peut être utilisée pour appliquer un chiffre de substitution polyalphabétique.
Afin de brouiller encore plus lors du chiffrement, plusieurs rotors peuvent être ajoutés. L'exemple de la figure 2 montre une telle machine avec 2 rotors. A chaque fois qu'une lettre est cryptée, le premier rotor tourne d'un cran (rotor de droite sur la figure 2) pendant que le deuxième rotor reste immobile. Une fois que le premier rotor a fait un tour complet, le deuxième rotor tourne d'un cran. C'est le même mécanisme que les montres avec les aiguilles des minutes et des heures. Sur la figure 2a, le premier rotor est sur le point de déclencher le mouvement du deuxième. Taper "b" sur le clavier fait allumer la lettre "D" (figure 2a). Le premier rotor pivote. Taper "b" de nouveau sur le clavier fait allumer la lettre "B" (figure 2b). Le premier rotor pivote, et comme il a fini sa rotation, le deuxième rotor pivote également. Taper "b" de nouveau sur le clavier fait allumer la lettre "B" (figure 2c).
La machine Enigma était composée de 3 rotors afin d'augmenter la complexité, mais elle avait également un réflecteur. Le réflecteur est fait un peu comme un brouilleur (câblage interne), sauf qu'il ne tourne pas. Lorsque l'on tape sur une touche, le signal électrique passe à travers les 3 rotors, le réflecteur reçoit le signal entrant et le renvoie à travers les 3 mêmes rotors mais suivant un autre circuit. Dans l'exemple de la figure 3, taper "b" au clavier fait allumer la lettre "D". En plus d'augmenter la complexité de chiffrement, le réflecteur permet également de chiffrer et déchiffrer en utilisant la même machine.

En utilisant la machine Enigma comme représenté dans la figure 3, et en supposant que les 3 rotors sont à leur position initiale (celui le plus à droite doit faire une révolution complète avant que celui du milieu ne tourne, idem pour celui du milieu par rapport à celui de gauche, et la rotation se fait par le bas), chiffrez le message "abacdfea".

Codez votre propre machine Enigma sur 26 lettres.

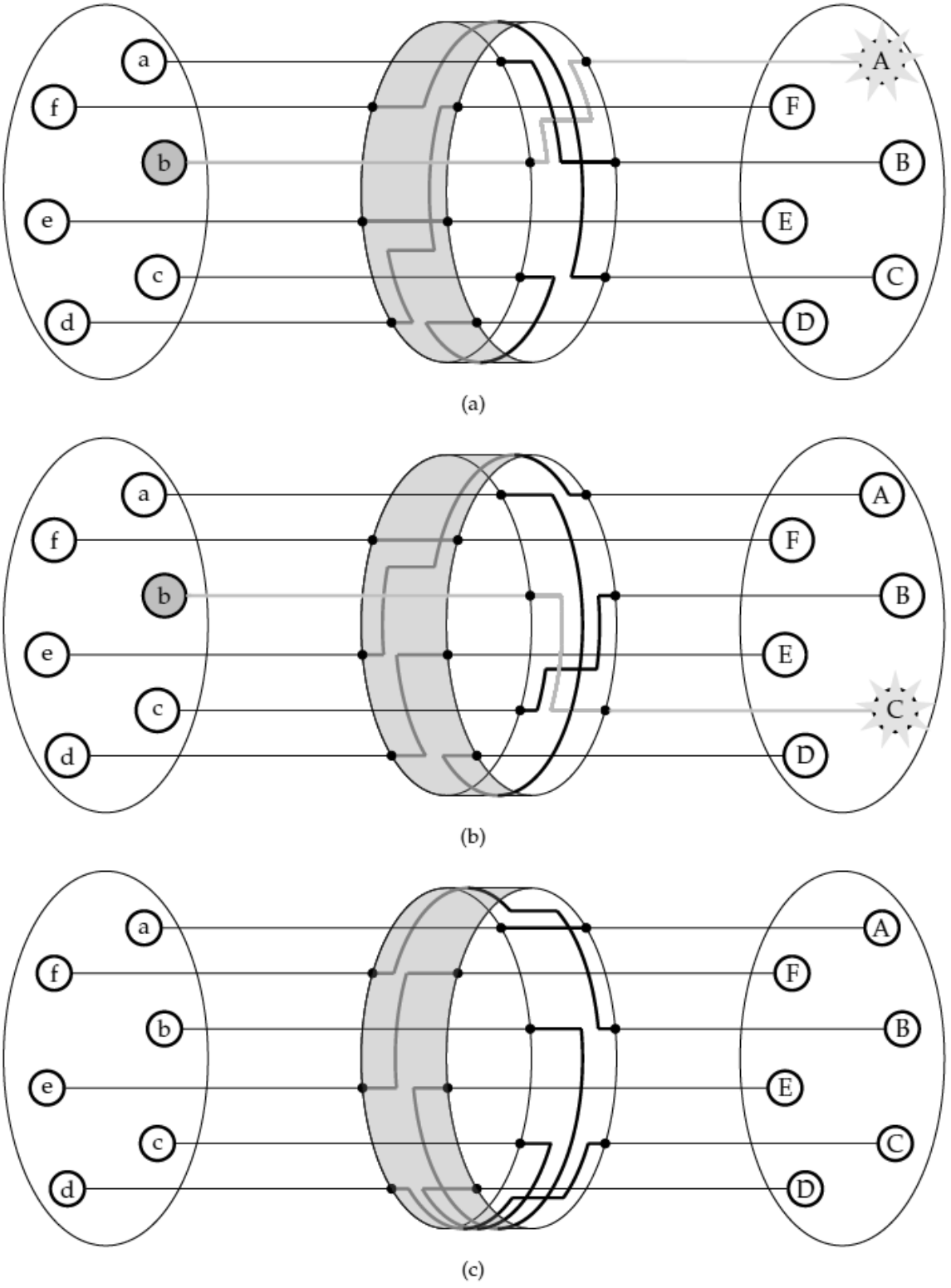

Figure 1 : Fonctionnement d'un rotor.

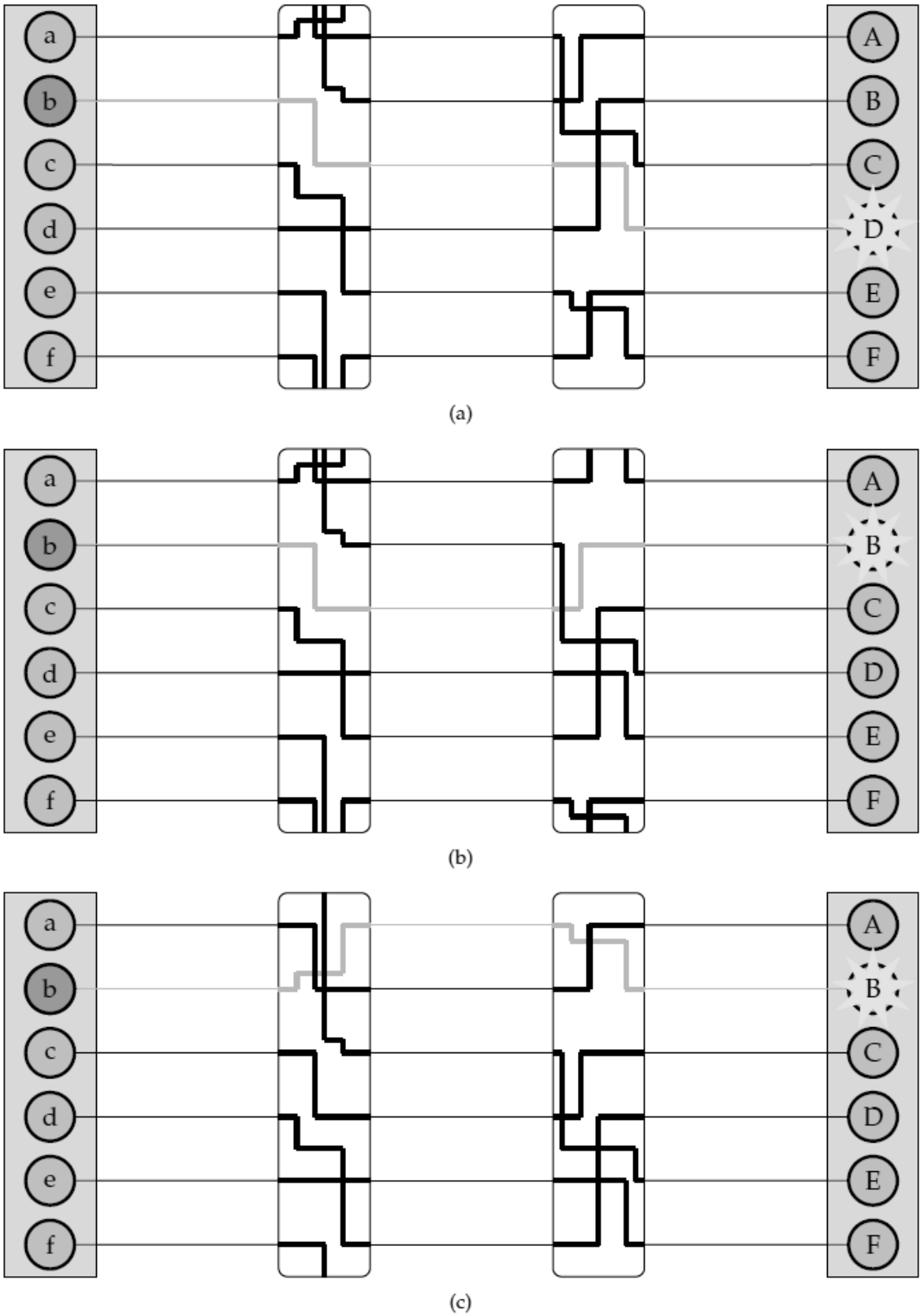

Figure 2 : Mécanisme à deux rotors.

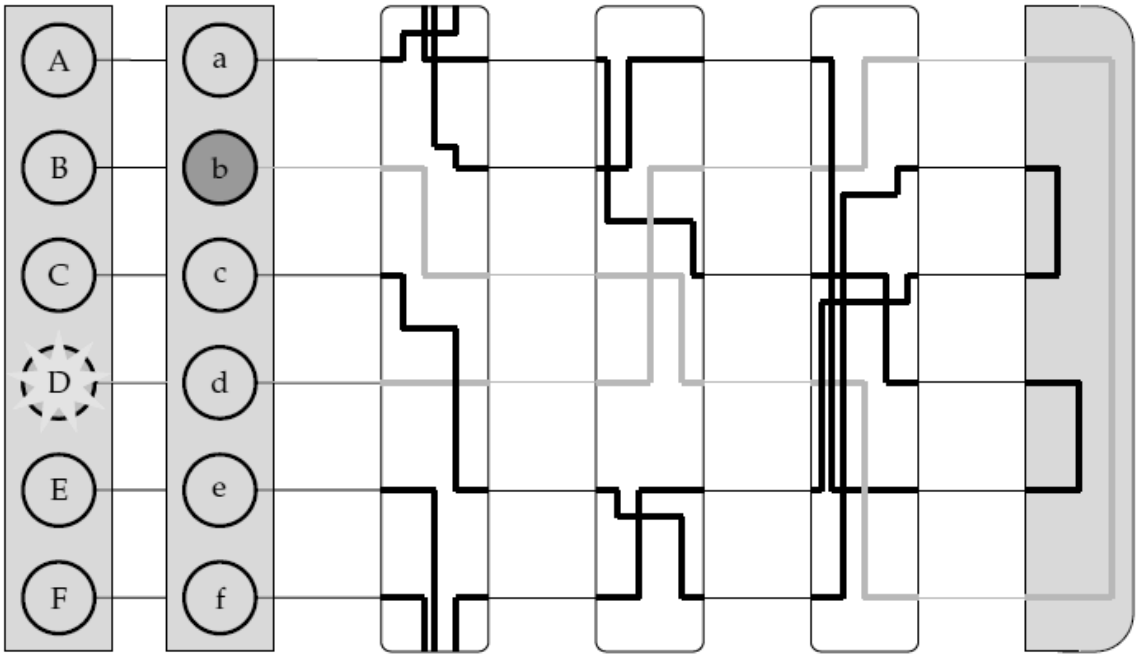

Figure 3 : Machine Enigma