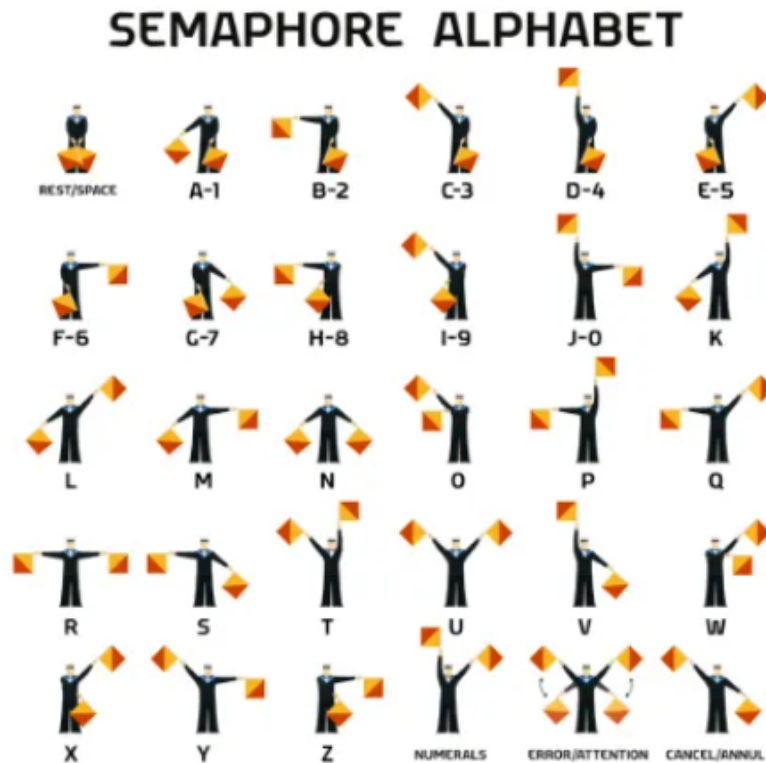


C++ Mettre en pratique

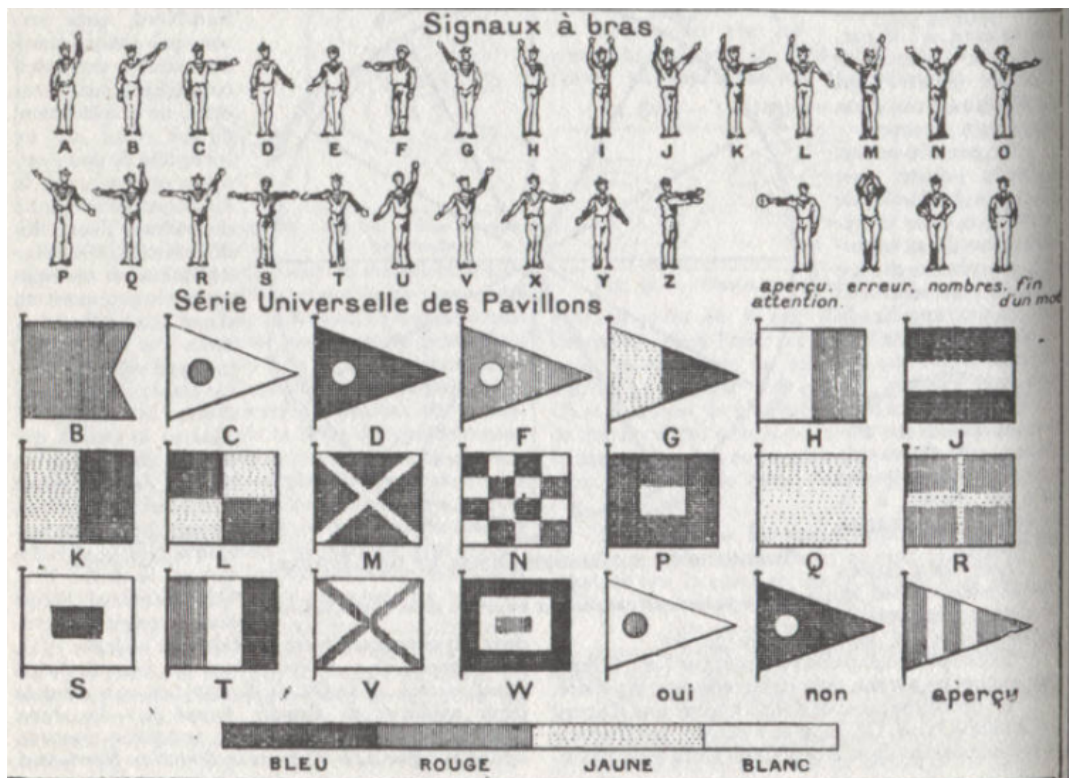
Crypter un livre de code



Un livre de code est un outil utilisé pour crypter des messages en utilisant un système de codage préétabli. Les livres de code sont utilisés depuis des siècles pour protéger les communications sensibles, en particulier dans les domaines militaire et diplomatique.

L'un des premiers exemples de livre de code a été utilisé par les lignes de sémaphores. Les dirigeants de la corporation des Chappe ont utilisé un code secret qui prenait 92 symboles basiques par deux pour former 8 464 mots et expressions codées .

La corporation des Chappe était une organisation créée par les frères Chappe pour développer et exploiter leur invention du télégraphe optique. Ce dernier était un système de communication à distance qui utilisait des signaux visuels pour transmettre des messages sur de longues distances. Les frères Chappe ont mis au point un code qui correspondait à une série de mots, de chiffres ou de phrases, adapté aux dépêches de l'administration. Les dirigeants de la corporation des Chappe ont utilisé un code secret qui prenait 92 symboles basiques par deux pour former 8 464 mots et expressions codés. Ce système a été rapidement adopté par l'administration française et a été utilisé pour transmettre des messages officiels sur de longues distances.



Napoléon Bonaparte a compris l'avantage militaire qui résultait de l'invention des frères Chappe et emportait un sémaphore portable dans ses quartiers généraux. Au fil du temps, les livres de code sont devenus de plus en plus complexes et sophistiqués, avec l'ajout de nouvelles techniques de codage et l'utilisation de technologies avancées pour générer des codes difficiles à casser. Aujourd'hui, les livres de code ne sont plus aussi couramment utilisés qu'auparavant, car les méthodes modernes de cryptographie offrent des moyens plus sûrs et plus efficaces de protéger les communications. Cependant, l'histoire des livres de code reste un sujet fascinant qui témoigne de l'ingéniosité humaine dans la recherche de moyens pour protéger les informations sensibles.

Voici un exemple de code en C++ qui utilise un fichier comme livre de code pour crypter

```
#include <fstream>
#include <iostream>
#include <sstream>
#include <string>
#include <vector>

// Fonction pour lire le livre de code à partir d'un fichier
std::vector<std::string> readCodebook(const std::string &filename) {
    std::vector<std::string> pages;
    std::ifstream file(filename);
    if (!file) {
        std::cerr << "Erreur lors de l'ouverture du fichier" << std::endl;
        return pages;
    }

    std::string line;
    while (std::getline(file, line)) {
        pages.push_back(line);
    }

    file.close();
    return pages;
}

// Fonction pour crypter un texte en utilisant le livre de code
std::string encrypt(const std::string &text, const std::vector<std::string> &codebook) {
    std::ostringstream oss;
    for (char c : text) {
        bool found = false;
        for (size_t i = 0; i < codebook.size(); i++) {
            size_t pos = codebook[i].find(c);
            if (pos != std::string::npos) {
                oss << i << '-' << pos << ' ';
                found = true;
                break;
            }
        }
        if (!found) {
            oss << "?-? ";
        }
    }
    return oss.str();
}
```

```
int main() {
    // Lecture du livre de code à partir d'un fichier
    std::vector<std::string> codebook = readCodebook("codebook.txt");

    // Cryptage d'un texte en utilisant le livre de code
    std::string text = "Hello, World!";
    std::string encrypted_text = encrypt(text, codebook);

    // Affichage du texte crypté
    std::cout << "Texte crypté: " << encrypted_text << std::endl;

    return 0;
}
```

Ce code définit deux fonctions: `readCodebook` pour lire le livre de code à partir d'un fichier et `encrypt` pour crypter un texte en utilisant le livre de code. La fonction `encrypt` parcourt chaque caractère du texte et recherche sa position dans le livre de code. Si le caractère est trouvé, sa page et sa position sont ajoutées au texte crypté sous la forme `page-position`. Si le caractère n'est pas trouvé, `?-?` est ajouté au texte crypté.

Dans l'exemple, le livre de code est lu à partir du fichier `codebook.txt` et utilisé pour crypter le texte "Hello, World!". Le texte crypté est ensuite affiché.