CAHIER DE CHARGE (objectifs et spécifications technique)

L’objectif du projet est de concevoir un programme qui simule la machine Enigma.

Le programme respecte l’API de base en couche.

Le tableau d’inversion de lettre n’est pas codé dans cette version.

La modélisation des rotors est réalisée par des tableaux/listes qui correspondent aux décalages provoqués par les liaisons électriques avec un réglage initial par défaut immuable : par exemple, chaque « a » devient « e », chaque « b » devient « k », chaque « c » devient « m » …

Les rotors sont toujours les mêmes, mais peuvent être placés différemment selon l’initiation. La version des rotors et du réflecteur serons partagés dans un fichier « rotors.init » au format JSON du style suivant :

Graphical user interface

Description automatically generated with low confidence

Le message à coder est lu à partir d’un simple fichier texte. Vous devez formater le message en majuscule, sans espace et sans accent. A chaque lettre, le premier rotor tourne ce qui signifie que deux lettres ne serons jamais codées de la même manière. Dans cette version simplifier, le codage démarre toujours avec les rotors sur leur position initiale.

* Etat de l’art sur la machine Enigma[1]

Enigma est une machine électromécanique portative servant au chiffrement et au déchiffrement de l’information.

* + Schema fonctionnel de la machine Enigma

Diagram

Description automatically generated

* + Mise en Œuvre
    - Préparation de la machine
      1. Ordre des rotors : choix et positionnement des trois rotors prescrits par des instructions (ex I – V – III)
      2. Disposition de la bague des rotors gauche, milieu et droit (ex 06-20-24 affiché FTX) prescrite par les instructions
      3. Permutations des fils du tableau de connexions
      4. Le premier chiffreur dispose les trois rotors sur la position initiale définis par les instructions quotidiennes
      5. Le premier chiffreur choisit au Hazard un réglage initial des rotors et le frappe deux fois, (ex BGZBGZ). C’est la clef brute du message
      6. Le second chiffreur note le résultat affiché par les voyants ; c’est l’indicateur ou clef chiffrée (ex TNUFDQ) ;
      7. Le premier chiffreur dispose ses rotors sur BGZ puis entre au clavier le texte du message en clair, lettre par lettre ; le second chiffreur note les lettres signalées par l’allumage des voyants.
    - Formatage et émission du message
      1. Préambule, en clair, avant le message proprement dit : indicatif radio, groupe date-heure, et nombre de lettre du message, plus le grundstellung(ex : JCM) ;
      2. Groupe de cinq lettres comprenant deux lettre tempons suivies du discriminant, ex : JEU
      3. Les six lettres de l’indicateur ou clef chiffrée(ex TNUFDQ)
      4. Le message chiffré en groupe de 5 lettres. Au maximum, 50 groupes de 5 lettres. Le message plus long sont découpés en plusieurs messages transmis séparément.
    - Réception et déchiffrement du message

A l’autre bout du réseau, le destinataire capte le message au moyen d’un autre poste radio. Le message est noté noir sur blanc. Il est remis à un chiffreur dont la machine Enigma est déjà reglé en fonction des mêmes instructions quotidiennes(1-2-3) que l’autorité éméttrice.le routeur dispose ses rotors sur JCM (4), frappe TNUFDQ(6) et note le résultat, BGZBGZ(5). Ensuite, le chiffreur dispose ses rotors sur BGZ. Le texte est déchiffré lettre par lettre, le second chiffreur note la mesure

NB : Cette procédure ne s'applique qu'à l'Enigma standard de la Heer (armée de terre) et de la Luftwaffe