Conclusion

Après la guerre, les cryptographes allemands furent interrogés par

des spécialistes de la mission TICOM. Les interrogateurs constatèrent que leurs prisonniers savaient qu'Enigma n'était pas incassable et qu'il était possible de déchiffrer certains messages. Alan Turing, qui aura largement contribué à « casser » Enigma, est aussi considéré comme un des pères de l’ordinateur moderne. Aujourd’hui, la machine Enigma ne résisterait pas à une « attaque » par la « force brute » de nos ordinateurs, c’est-à-dire en essayant toutes les combinaisons possibles. Côté dénombrement, nous allons chercher à estimer le temps qu’il faudrait dans les années 1930 à un ordinateur pour « casser » Enigma par la « force brute », c’est-à-dire en essayant toutes ces combinaisons.