Attaque Enigma par indice de coincidence :

Une méthode, adaptée aux moyens modernes, **consiste à essayer toutes les possibilités** et à **calculer l'indice de coïncidence** du texte déchiffré.

Un message proche au contenu aléatoire aura un indice proche de 0.075 pour du français. L'indice varie selon la langue mais il est invariant aux substitutions monoalphabétiques.

Dans le cas d'Enigma, on peut essayer toutes les combinaisons des rotors et regarder l'indice obtenu.

Soit un message intercepté crypté par une Enigma comme celle utilisée par la Wehrmacht (3 rotors) :

RFCNT RAONM CVIJZ CBRWS XOTJG SMOMX DUWFW LBYBK BPOFY AOEQW PHNLJ MXMYM JDVPI TOHOC MUIYW WYQRZ LTBEI HUDJE Y

Maintenant, essayons toutes les configurations des rotors et calculons l'indice de coïncidence après déchiffrement, voici un extrait des résultats :

Rotors	Message	IC
ONS	GKNQC CJIBD GYEFO ZQCBH OWJVU AYYLR IXJTC URIEA LVCLS KIVVR GQFEQ DBTMU GIAAY FXVRH RRBPO TQEFF XNQBV ZFMGZ J	0.03909
ONT	DWRIE GMZSA RQVWC NEGNJ GLFAQ PDANF RAZVG DOKHW NUEPO USNUZ KOXCV VLYPX SHOWP BJYKV QDCLT CVKLO JGEKS EKYPM O	0.03492
ONU	ATTAQ UECES OIRSU RWIKI PEDIA ILFAU TECRI REPLU SDART ICLES ETSUR TOUTT ERMIN ERCET ARTIC LEDEC RYPTA NALYS E	**0.07473**
ONV	CLRHE MPTBX LPUVM FOGOE DBNKW FNNWN PGGPN QHXNE AFYWF LFQHM IPGSU YSXNF MUEMM AKWVL AAYQL ZNVWN NNKHF WGRMY K	0.04591

Au vu des résultats et en présence d'un indice proche de 0.074, on peut en conclure que la configuration " ONU " est probablement la bonne alors que les autres ont un indice largement inférieur et proche d'une distribution uniforme.

Pour plus d'assurance, on pourrait procéder à une analyse de la fréquence des lettres dans le message.

On se rendrait compte que le message " ONU " contient un grand nombre de 'E' et de 'A' et qu'il est probablement en français.

Le message est de ce fait : « ATTAQ UECES OIRSU RWIKI PEDIA ILFAU TECRI REPLU SDART ICLES ETSUR TOUTT ERMIN ERCET ARTIC LEDEC RYPTA NALYS E » que l'on transforme en :

"attaque ce soir sur wikipedia il faut ecrire plus d articles et surtout terminer cet article de cryptanalyse"

https://www.techno-science.net/definition/6149.html