Enigma M3 Crack (Version 1.0)

EnigmaM3Crack is a free program destined to decipher messages coded by the legendary Enigma machine used by the German armies during World War II.

The ciphering was based on a twin system:

- Three mobile rotors chosen among a game of five available rotors
- A board of connections (Stecker) capable to permute up to ten couples of letters

Every rotor had the 26 letters of the alphabet, the game of three rotors permitted therefore 26x26x26 = 17576 different combinations.
As these three rotors were chosen within a group of five, there were 60 possible different choices (Number of arrangements of 3 among 5).
The Stecker is the device that offered, from afar, the largest number of scrambling possibilities: In the case where one used the ten provided cables, the calculation shows that the number of possible combinations is 1,5 x ten to the power of 14.
In counterpart, this Stecker only provides a ciphering by mono-substitution alphabet, vulnerable to attacks by analysis of frequencies.
The power of ciphering of Enigma comes therefore mainly from the poly-alphabetic substitution provided by the three rotors with automatic advance, the Stecker being there to considerably increase the number of possible keys, what makes impossible the unciphering by brute-force (successive test of all possible keys)
The total number of possible keys for the machine Enigma M3 is 17576 x 60 x of 1,5 x ten to the power of 14 = 1,5 x ten to the power of 20: Even with modern powerful computers, many millions of years would be needed to try each of these possible keys one after the other.

EnigmaM3Crack proposes a functional tool aiming to considerably reduce this time of unciphering.
For that, it uses the concept of **Index of Coincidence** (IOC),which was invented in 1920 by William Friedman: On a very long text, the IOC'S are as follow: Random text (for example a ciphered text) = 0,0385, text in French = 0,0778, text in German = 0,0762, text in English = 0,0667

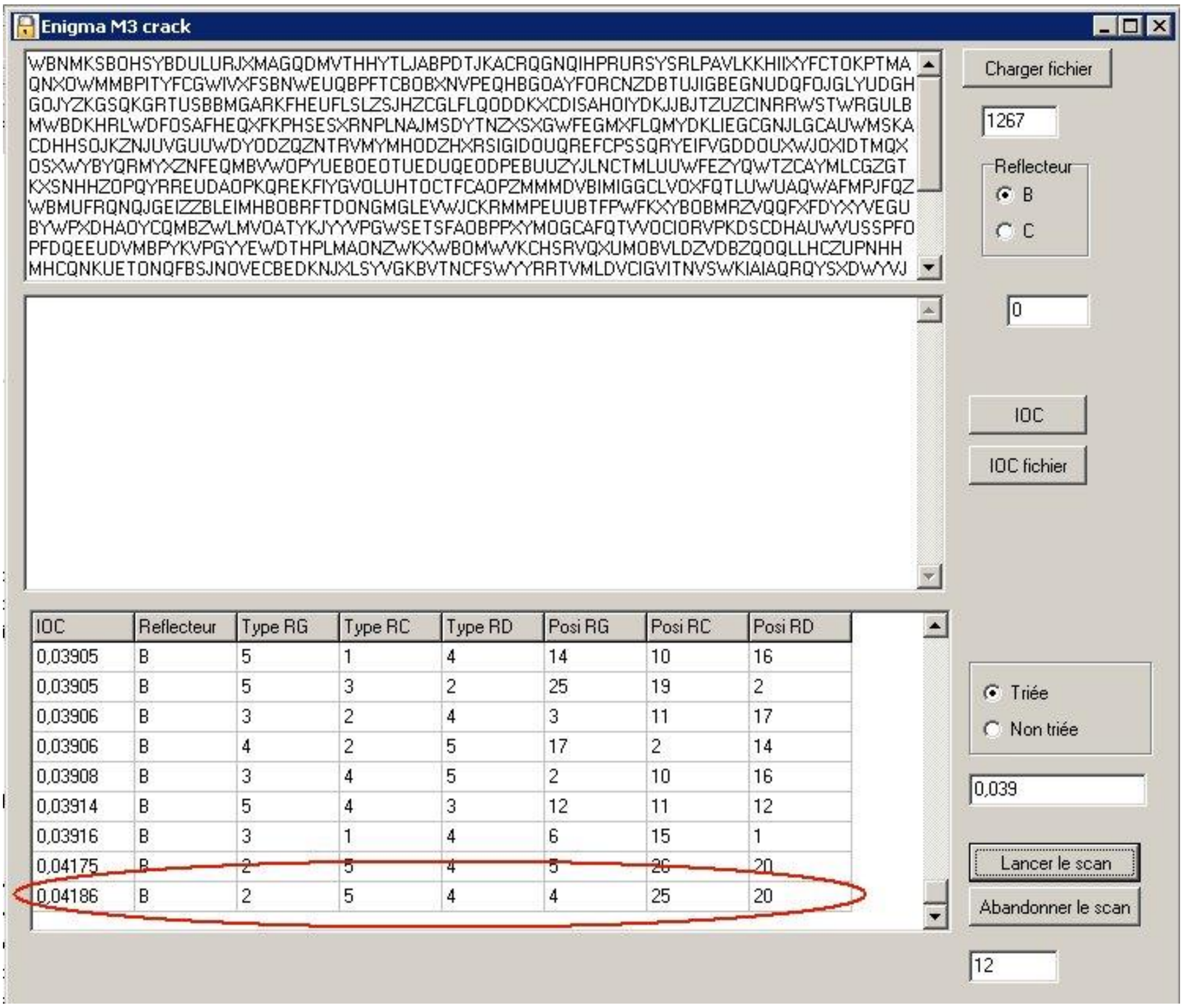
The operation will occur in two steps:

- Research of the rotors (types and initial positions) used during the ciphering
- Research of the cables (number and positions) used for the board of connections (Stecker)

The first research uses the **EnigmaM3Crack.exe** program, the second research uses the **Enigma_M3_sim.exe** program
The text below indicates step-by-step how one must proceed to decipher the provided message-example.

Research of the rotors

Run **EnigmaM3Crack.exe** and load the **Message-exemple.txt** file (*Button 'Charger fichier*').
With reflector B selected (default choice), push on the button ' *Lancer le scan*' (bottom right)
The scan is going to decode the text provided with each of the 17576 x 60 possible rotor configurations, and will calculate the IOC on the such gotten text.
When the scan is finished, you get a list of IOC'S, classified by increasing order, with indication of the corresponding configuration of rotors .
You can have the number of retained lines modified by changing the minimum threshold for the IOC: In the example, only the IOC'S of at least 0,03900 are kept.
The configuration used for the ciphering is either the last one of the list, or one of the lasts, at least when you deal with a relatively long ciphered text (1267 characters in the provided example)



```
WBNMKSBOHSYBDULURJXMAGQDMVTHHYTLJABPDTJKACRQGNQIHPRURSYSRLPAVLKKHIIXYFCTOKPTMA
QNXOWMMBPITYFCGWIVXFSBNWEUQBPFTCBOBXNVPEQHBGOAYFORCNZDBTUJIGBEGNUDQFOJGLYUDGH
GOJYZKGSQKGRTUSBBMGARKFHEUFLSLZSJHZCGLFLQODDKXCDISAHOIYDKJJBJTZUZCINRRWSTWRGULB
MWBDKHRLWDFOSAFHEQXFKPHSESXRNPLNAJMSDYTNZXSXGWFEGMXFLQMYDKLIEGCGNJLGCAUWMSKA
CDHHSOJKZNJUVGUUWDYODZQZNTRVMYMHODZHXRSIGIDOUQREFCPSSQRYEIFVGDDOUXWJOXIDTMQX
OSXWYBYQRMYXZNFEQMBVWOPYUEBOEOTUEDUQEODPEBUUZYJLNCTMLUUWFEZYQWTZCAYMLCGZGT
KXSNHHZOPQYRREUDAOPKQREKFIYGVOLUHTOCTFCAOPZMMMDVBIMIGGCLVOXFQTLUWUAQWAFMPJFQZ
WBMUFRQNQJGEIZZBLEIMHBOBRFTDONGMGLEVWJCKRMMPEUUBTFPWFKXYBOBMRZVQQFXFDYXYVEGU
BYWPXDHAOYCQMBZWLMVOATYKJYYVPGWSETSFAOBPPXYMOGCAFQTVVOCIORVPKDSCDHAUWVUSSPFO
PFDQEEUDVMBPYKVPGYYEWDTHPLMAONZWKXWBOMWVKCHSRVQXUMOBVLDZVDBZQOQLLHCZUPNHH
MHCQNKUETONQFBSJNOVECBEDKNJXLSYVGKBVTNCFSWYYRRTVMLDVCIGVITNVSWKIAIAQRQYSXDWYVJ
```

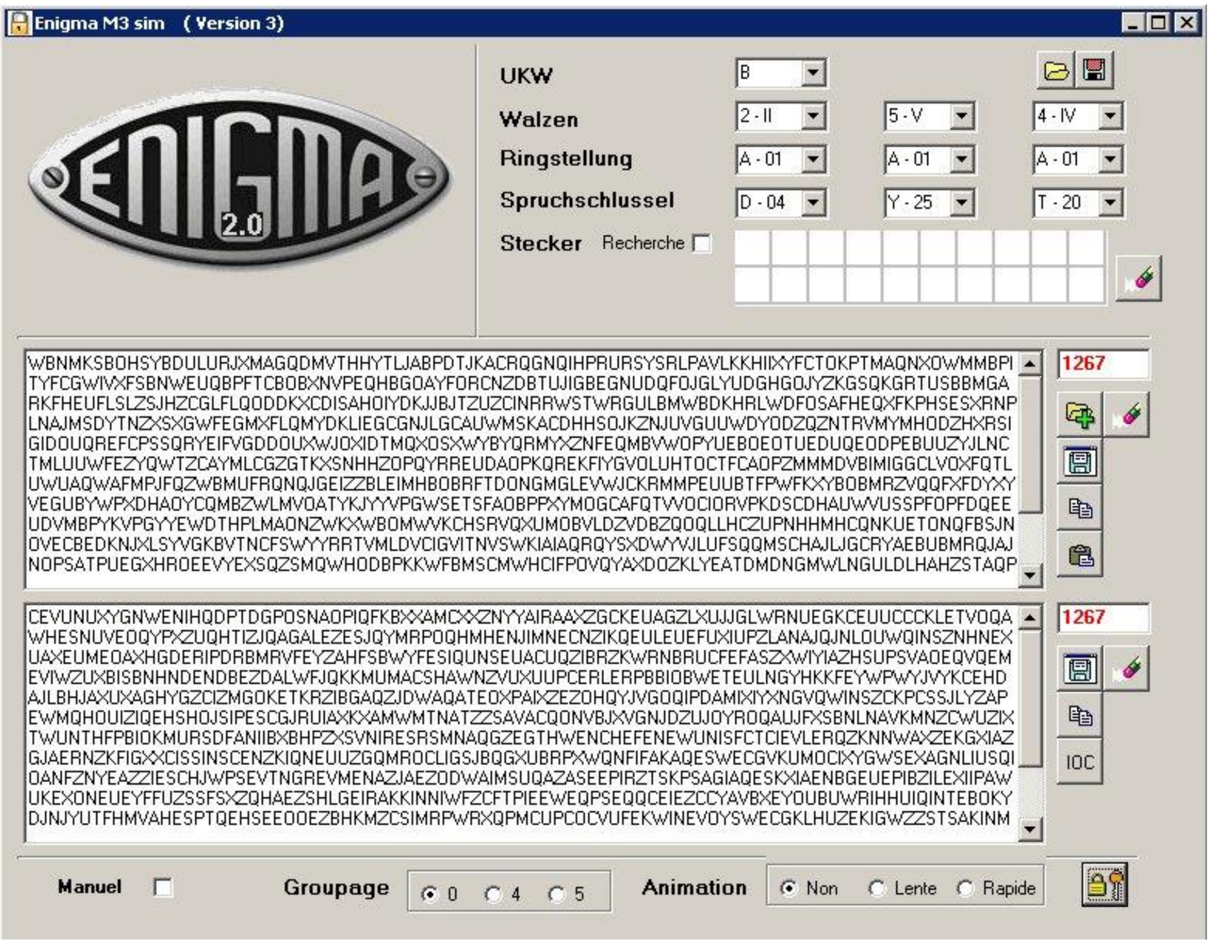
IOC	Reflecteur	Type RG	Type RC	Type RD	Posi RG	Posi RC	Posi RD
0,03905	B	5	1	4	14	10	16
0,03905	B	5	3	2	25	19	2
0,03906	B	3	2	4	3	11	17
0,03906	B	4	2	5	17	2	14
0,03908	B	3	4	5	2	10	16
0,03914	B	5	4	3	12	11	12
0,03916	B	3	1	4	6	15	1
0,04175	B	2	5	4	5	26	20
0,04186	B	2	5	4	4	25	20

If you renew the operation using the C reflector instead of the B reflector, you will note that the IOC'S are 0.03933 or less, instead of 0,04186: It is therefore likely that the reflector used for the ciphering was the B reflector.

Now, knowing the probable configuration of the rotors, you can start your attack to find what was the connections used for the Stecker.

Research of the cables for the Stecker

Run **Enigma_M3_sim.exe** (version 3 or more recent), select the configuration of rotors found above, and load the **Message-exemple.txt** file.
Push the uncipher button, bottom right: You can see, in the lower box, that the deciphered text is incomprehensible, which means that one or several cables have been used for the Stecker, at ciphering time.



UKW B

Walzen 2 - II | 5 - V | 4 - IV

Ringstellung A - 01 | A - 01 | A - 01

Spruchschlussel D - 04 | Y - 25 | T - 20

Stecker Recherche □

```
WBNMKSBOHSYBDULURJXMAGQDMVTHHYTLJABPDTJKACRQGNQIHPRURSYSRLPAVLKKHIIXYFCTOKPTMAQNXOWMMBPI
TYFCGWIVXFSBNWEUQBPFTCBOBXNVPEQHBGOAYFORCNZDBTUJIGBEGNUDQFOJGLYUDGHGOJYZKGSQKGRTUSBBMGA
RKFHEUFLSLZSJHZCGLFLQODDKXCDISAHOIYDKJJBJTZUZCINRRWSTWRGULBMWBDKHRLWDFOSAFHEQXFKPHSESXRNP
LNAJMSDYTNZXSXGWFEGMXFLQMYDKLIEGCGNJLGCAUWMSKACDHHSOJKZNJUVGUUWDYODZQZNTRVMYMHODZHXRSI
GIDOUQREFCPSSQRYEIFVGDDOUXWJOXIDTMQXOSXWYBYQRMYXZNFEQMBVWOPYUEBOEOTUEDUQEODPEBUUZYJLNC
TMLUUWFEZYQWTZCAYMLCGZGTKXSNHHZOPQYRREUDAOPKQREKFIYGVOLUHTOCTFCAOPZMMMDVBIMIGGCLVOXFQTL
UWUAQWAFMPJFQZWBMUFRQNQJGEIZZBLEIMHBOBRFTDONGMGLEVWJCKRMMPEUUBTFPWFKXYBOBMRZVQQFXFDYXY
VEGUBYWPXDHAOYCQMBZWLMVOATYKJYYVPGWSETSFAOBPPXYMOGCAFQTVVOCIORVPKDSCDHAUWVUSSPFOPFDQEE
UDVMBPYKVPGYYEWDTHPLMAONZWKXWBOMWVKCHSRVQXUMOBVLDZVDBZQOQLLHCZUPNHHMHCQNKUETONQFBSJN
OVECBEDKNJXLSYVGKBVTNCFSWYYRRTVMLDVCIGVITNVSWKIAIAQRQYSXDWYVJLUFSQQMSCHAJLJGCRYAEBUBMRQJAJ
NOPSATPUEGXHROEEVYEXSQZSMQWHODBPKKWFBMSCMWHCIFPOVQYAXDOZKLYEATDMDNGMWLNGULDLHAHZSTAQP
```

1267

```
CEVUNUXYGNWENIHQDPTDGPOSNAOPIQFKBXXAMCXXZNYYAIRAAXZGCKEUAGZLXUJJGLWRNUEGKCEUUCCCKLETVOQA
WHESNUVEOQYPXZUQHTIZJQAGALEZESJQYMRPOQHMHENJIMNECNZIKQEULEUEFUXIUPZLANAJQJNLOUWQINSZNHNEX
UAXEUMEOAXHGDERIPDRBMRVFEYZAHFSBWYFESIQUNSEUACUQZIBRZKWRNBRUCFEFASZXWIYIAZHSUPSVAOEQVQEM
EVIWZUXBISBNHNDENDBEZDALWFJQKKMUMACSHAWNZVUXUUPCERLERPBBIOBWETEULNGYHKKFEYWPWYJVYKCEHD
AJLBHJAXUXAGHYGZCIZMGOKETKRZIBGAQZJDWAQATEOXPAIXZEZOHQYJVGOQIPDAMIXIYXNGVQWINSZCKPCSSJLYZAP
EWMQHOUIZIQEHSHOJSIPESCGJRUIAXKXAMWMTNATZZSAVACQONVBJXVGNJDZUJOYROQAUJFXSBNLNAVKMNZCWUZIX
TWUNTHFPBIOKMURSDFANIIBXBHPZXSVNIRESRSMNAQGZEGTHWENCHEFENEWUNISFCTCIEVLERQZKNNWAXZEKGXIAZ
GJAERNZKFIGXXCISSINSCENZKIQNEUUZGQMROCLIGSJBQGXUBRPXWQNFIFAKAQESWECGVKUMOCIXYGWSEXAGNLIUSQI
OANFZNYEAZZIESCHJWPSEVTNGREVMENAZJAEZODWAIMSUQAZASEEPIRZTSKPSAGIAQESKXIAENBGEUEPIBZILEXIIPAW
UKEXONEUEYFFUZSSFSXZQHAEZSHLGEIRAKKINNIWFZCFTPIEEWEQPSEQQCEIEZCCYAVBXEYOUBUWRIHHUIQINTEBOKY
DJNJYUTFHMVAHESPTQEHSEEOOEZBHKMZCSIMRPWRXQPMCUPCOCVUFEKWINEVOYSWECGKLHUZEKIGWZZSTSAKINM
```

1267

Manuel □ Groupage ● 0 ○ 4 ○ 5 Animation ● Non ○ Lente ○ Rapide

Check the box *'Stecker, recherche'* and depress the uncipher button, bottom right: For each of the possible couples of letters (AB, AC,....., XZ, YZ), the program will calculate the IOC of the unciphered text, and show the result in a worksheet 25 x 25 in size.

In order to make the provided results more clear, the shown numbers are the IOC multiplied by 100,000

Besides, you can filter the results by masking all numbers lower than a fixed threshold (4300 in the example below, that is to say an IOC = 0,04300)

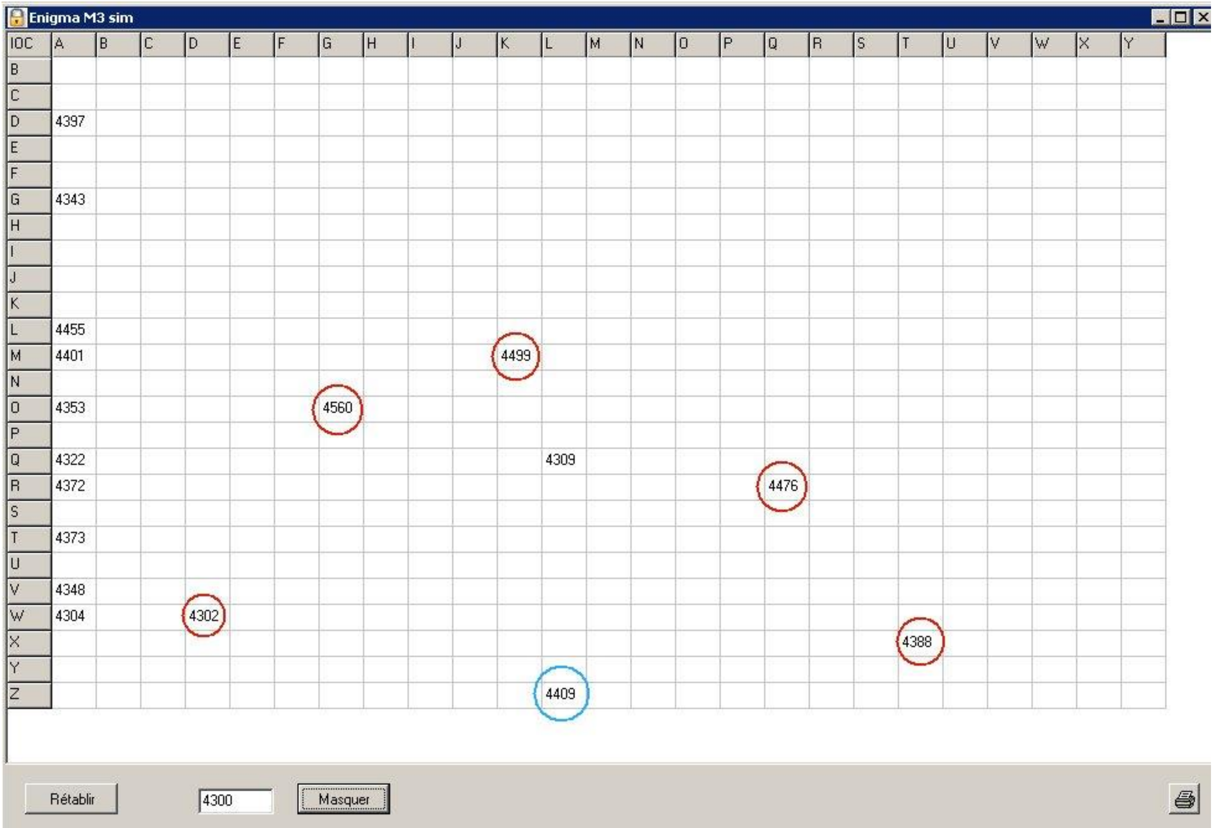
You can also mark some cells in red color by a right click on the grid, or erase those red marks with a left click.

In the picture you can note the likely associations for the following letters:

- D with W
- G with O
- K with M
- Q with R
- T with X

Concerning the letter **L**, two associations provide a rather high IOC: Z and Q, the letter **Z** seeming the likeliest.

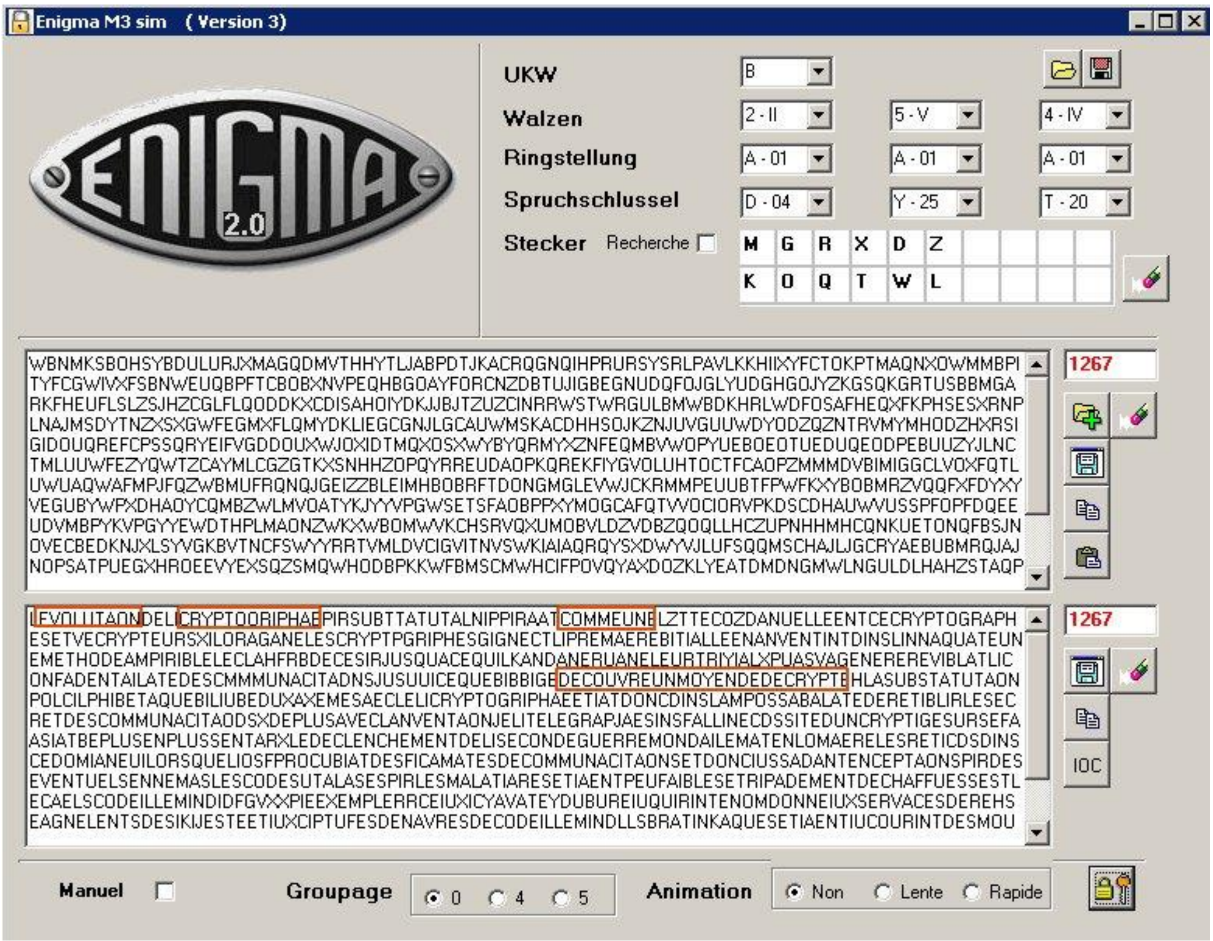
Concerning the letter **A**, no conclusion is possible, because all IOC'S found have near values.
We therefore have to try to decipher with the associations DW, GO, KM, QR, TX and LZ, and tempt to find the right associated letter for A, knowing that the possible binomials are only the remaining letters: B, C, E, F, H, I, J, N, P, S, U, V and Y.



Enigma M3 sim

IOC	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
B																									
C																									
D	4397																								
E																									
F																									
G	4343																								
H																									
I																									
J																									
K																									
L	4455																								
M	4401										4499														
N																									
O	4353						4560																		
P																									
Q	4322											4309													
R	4372																4476								
S																									
T	4373																								
U																									
V	4348																								
W	4304			4302																					
X																				4388					
Y																									
Z												4409													

Uncheck the box *'Stecker*, *recherche'*, type-in the letters of the Stecker supposed good (DW, GO, KM, QR, TX and LZ) and push again on the uncipher button, bottom right:



Enigma M3 sim (Version 3)

UKW: B

Walzen: 2 - II | 5 - V | 4 - IV

Ringstellung: A - 01 | A - 01 | A - 01

Spruchschlussel: D - 04 | Y - 25 | T - 20

Stecker Recherche □

M	G	R	X	D	Z
K	O	Q	T	W	L

```
WBNMKSBOHSYBDULURJXMAGQDMVTHHYTLJABPDTJKACRQGNQIHPRURSYSRLPAVLKKHIIXYFCTOKPTMAQNXOWMMBPI
TYFCGWIVXFSBNWEUQBPFTCBOBXNVPEQHBGOAYFORCNZDBTUJIGBEGNUDQFOJGLYUDGHGOJYZKGSQKGRTUSBBMGA
RKFHEUFLSLZSJHZCGLFLQODDKXCDISAHOIYDKJJBJTZUZCINRRWSTWRGULBMWBDKHRLWDFOSAFHEQXFKPHSESXRNP
LNAJMSDYTNZXSXGWFEGMXFLQMYDKLIEGCGNJLGCAUWMSKACDHHSOJKZNJUVGUUWDYODZQZNTRVMYMHODZHXRSI
GIDOUQREFCPSSQRYEIFVGDDOUXWJOXIDTMQXOSXWYBYQRMYXZNFEQMBVWOPYUEBOEOTUEDUQEODPEBUUZYJLNC
TMLUUWFEZYQWTZCAYMLCGZGTKXSNHHZOPQYRREUDAOPKQREKFIYGVOLUHTOCTFCAOPZMMMDVBIMIGGCLVOXFQTL
UWUAQWAFMPJFQZWBMUFRQNQJGEIZZBLEIMHBOBRFTDONGMGLEVWJCKRMMPEUUBTFPWFKXYBOBMRZVQQFXFDYXY
VEGUBYWPXDHAOYCQMBZWLMVOATYKJYYVPGWSETSFAOBPPXYMOGCAFQTVVOCIORVPKDSCDHAUWVUSSPFOPFDQEE
UDVMBPYKVPGYYEWDTHPLMAONZWKXWBOMWVKCHSRVQXUMOBVLDZVDBZQOQLLHCZUPNHHMHCQNKUETONQFBSJN
OVECBEDKNJXLSYVGKBVTNCFSWYYRRTVMLDVCIGVITNVSWKIAIAQRQYSXDWYVJLUFSQQMSCHAJLJGCRYAEBUBMRQJAJ
NOPSATPUEGXHROEEVYEXSQZSMQWHODBPKKWFBMSCMWHCIFPOVQYAXDOZKLYEATDMDNGMWLNGULDLHAHZSTAQP
```

1267

```
LEVOLUTAONDELICRYPTOORIPHAEPIRSUBTTATUTALNIPPIRAATCOMMEUNELZTTECOZDANUELLEENTCECRYPTOGRAPH
ESETVECRYPTEURSXILORAGANELESCRYPTPGRIPHESGIGNECTLIPREMAEREBITIALLEENANVENTINTDINSLINNAQUATEUN
EMETHODEAMPIRIBLELECLAHFRBDECESIRJUSQUACEQUILKANDANERUANELEURTRIYIALXPUASVAGENEREREVIBLATLIC
ONFADENTAILATEDESCMMMUNACITADNSJUSUUICEQUEBIBBIGEDECOUVREUNMOYENDEDECRYPTEHLASUBSTATUTAON
POLCILPHIBETAQUEBILIUBEDUXAXEMESAECLELICRYPTOGRIPHAEETIATDONCDINSLAMPOSSABALATEDERETIBLIRLESEC
RETDESCOMMUNACITAODSXDEPLUSAVECLANVENTAONJELITELEGRAPJAESINSFALLINECDSSITEDUNCRYPTIGESURSEFA
ASIATBEPLUSENPLUSSENTARXLEDECLENCHEMENTDELISECONDEGUERREMONDAILEMATENLOMAERELESRETICDSDINS
CEDOMIANEUILORSQUELIOSFPROCUBIATDESFICAMATESDECOMMUNACITAONSETDONCIUSSADANTENCEPTAONSPIRDES
EVENTUELSENNEMASLESCODESUTALASESPIRLESMALATIARESETIAENTPEUFAIBLESETRIPADEMENTDECHAFFUESSESTL
ECAELSCODEILLEMINDIDFGVXXPIEEXEMPLERRCEIUXICYAVATEYDUBUREIUQUIRINTENOMDONNEIUXSERVACESDEREHS
EAGNELENTSDESIKIJESTEETIUXCIPTUFESDENAVRESDECODEILLEMINDLLSBRATINKAQUESETIAENTIUCOURINTDESMOU
```

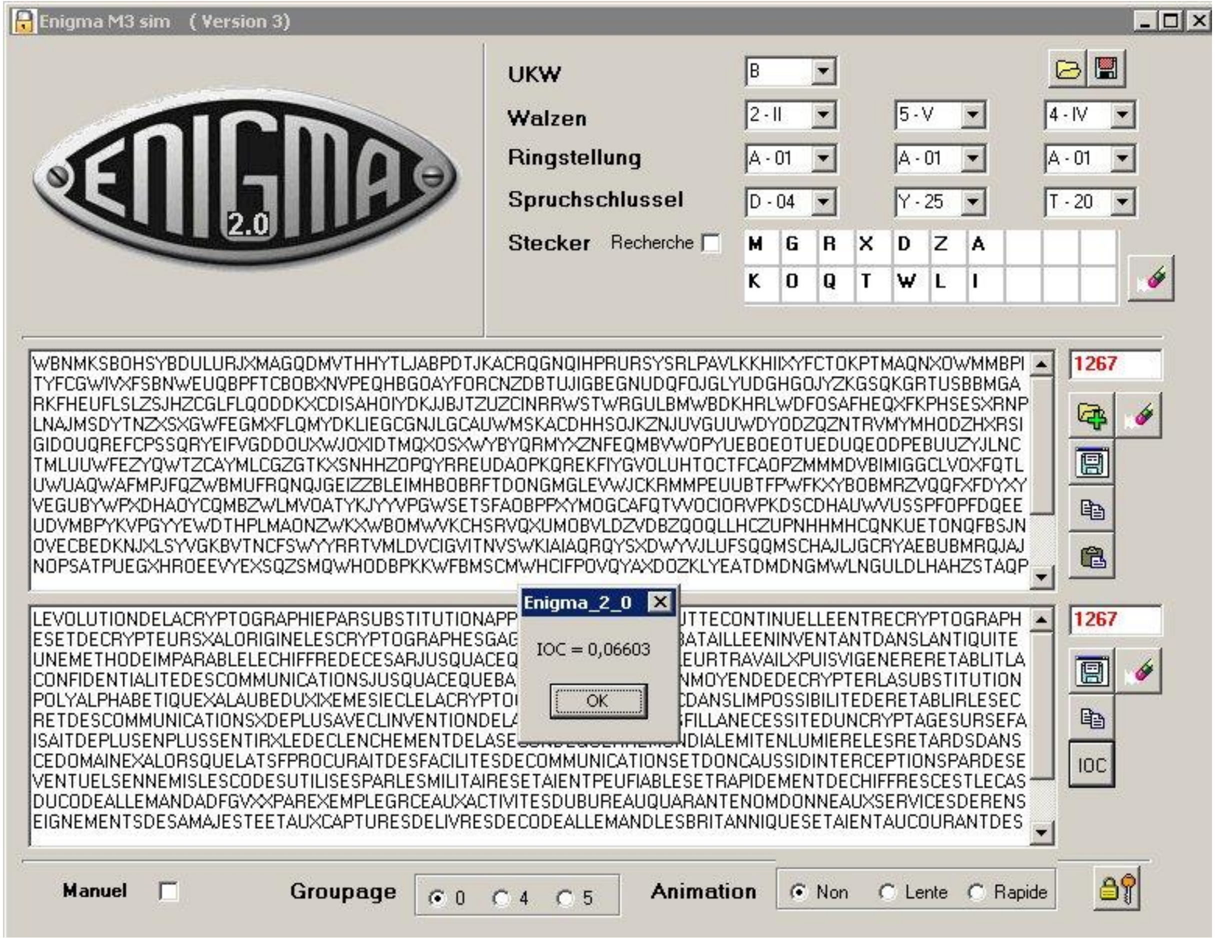
1267

Manuel □

Groupage ● 0 ○ 4 ○ 5

Animation ● Non ○ Lente ○ Rapide

You can see that the deciphered text became a lot less hermetic: Whole pieces of sentences are now legible.
It is necessary to determine now what is the good letter to associate to A, among the thirteen possible letters (B, C, E, F, H, I, J, N, P, S, U, V and Y)
The simplest is to try these 13 possible binomials successively, and you will quickly discover that the only couple giving a completely legible text is **AI**.
It must be noticed that for this final operation, the legible text is not necessarily the one giving the most elevated IOC, because the text is not long enough: 'AI' gives an IOC = 0,06603, whereas with ' AV' one gets an IOC = 0,06812 (Recall: The IOC on a very long text in French language is 0.0778)



UKW B
Walzen 2 - II 5 - V 4 - IV
Ringstellung A - 01 A - 01 A - 01
Spruchschlussel D - 04 Y - 25 T - 20
Stecker Recherche □

M	G	R	X	D	Z	A
K	O	Q	T	W	L	I

```
WBNMKSBOHSYBDULURJXMAGQDMVTHHYTLJABPDTJKACRQGNQIHPRURSYSRLPAVLKKHIIXYFCTOKPTMAQNXOWMMBPI
TYFCGWIVXFSBNWEUQBPFTCBOBXNVPEQHBGOAYFORCNZDBTUJIGBEGNUDQFOJGLYUDGHGOJYZKGSQKGRTUSBBMGA
RKFHEUFLSLZSJHZCGLFLQODDKXCDISAHOIYDKJJBJTZUZCINRRWSTWRGULBMWBDKHRLWDFOSAFHEQXFKPHSESXRNP
LNAJMSDYTNZXSXGWFEGMXFLQMYDKLIEGCGNJLGCAUWMSKACDHHSOJKZNJUVGUUWDYODZQZNTRVMYMHODZHXRSI
GIDOUQREFCPSSQRYEIFVGDDOUXWJOXIDTMQXOSXWYBYQRMYXZNFEQMBVWOPYUEBOEOTUEDUQEODPEBUUZYJLNC
TMLUUWFEZYQWTZCAYMLCGZGTKXSNHHZOPQYRREUDAOPKQREKFIYGVOLUHTOCTFCAOPZMMMDVBIMIGGCLVOXFQTL
UWUAQWAFMPJFQZWBMUFRQNQJGEIZZBLEIMHBOBRFTDONGMGLEVWJCKRMMPEUUBTFPWFKXYBOBMRZVQQFXFDYXY
VEGUBYWPXDHAOYCQMBZWLMVOATYKJYYVPGWSETSFAOBPPXYMOGCAFQTVVOCIORVPKDSCDHAUWVUSSPFOPFDQEE
UDVMBPYKVPGYYEWDTHPLMAONZWKXWBOMWVKCHSRVQXUMOBVLDZVDBZQOQLLHCZUPNHHMHCQNKUETONQFBSJN
OVECBEDKNJXLSYVGKBVTNCFSWYYRRTVMLDVCIGVITNVSWKIAIAQRQYSXDWYVJLUFSQQMSCHAJLJGCRYAEBUBMRQJAJ
NOPSATPUEGXHROEEVYEXSQZSMQWHODBPKKWFBMSCMWHCIFPOVQYAXDOZKLYEATDMDNGMWLNGULDLHAHZSTAQP
```

1267

```
LEVOLUTIONDELACRYPTOGRAPHIEPARSUBSTITUTIONAPP              UTTECONTINUELLEENTRECRYPTOGRAPH
ESETDECRYPTEURSXALORIGINELESCRYPTOGRAPHESGAG              BATAILLEENINVENTANTDANSLANTIQUITE
UNEMETHODEIMPARABLELECHIFFREDECESARJUSQUACEQ              LEURTRAVAILXPUISVIGENERERETABLITLA
CONFIDENTIALITEDESCOMMUNICATIONSJUSQUACEQUEBA              NMOYENDEDECRYPTERLASUBSTITUTION
POLYALPHABETIQUEXALAUBEDUXIXEMESIECLELACRYPTO             CDANSLIMPOSSIBILITEDERETABLIRLESEC
RETDESCOMMUNICATIONSXDEPLUSAVECLINVENTIONDELA              FILLANECESSITEDUNCRYPTAGESURSEFA
ISAITDEPLUSENPLUSSENTIRXLEDECLENCHEMENTDELASE             NDIALEMITENLUMIERELESRETARDSDANS
CEDOMAINEXALORSQUELATSFPROCURAITDESFACILITESDECOMMUNICATIONSETDONCAUSSIDINTERCEPTIONSPARDESE
VENTUELSENNEMISLESCODESUTILISESPARLESMILITAIRESETAIENTPEUFIABLESETRAPIDEMENTDECHIFFRESCESTLECAS
DUCODEALLEMANDADFGVXXPAREXEMPLEGRCEAUXACTIVITESDUBUREAUQUARANTENOMDONNEAUXSERVICESDERENS
EIGNEMENTSDESAMAJESTEETAUXCAPTURESDELIVRESDECODEALLEMANDLESBRITANNIQUESETAIENTAUCOURANTDES
```

Enigma_2_0

IOC = 0,06603

1267

Manuel □ Groupage ● 0 ○ 4 ○ 5 Animation ● Non ○ Lente ○ Rapide

Remark

The twin programs proposed here won't, most of the time, give you, a turnkey solution, especially if the coded text is short and if numerous substitutions of letters have been operated at Stecker level.
It is mainly a tool making possible, with a little time and savvy, an uncipher that would not have been possible using the usual ways (brute-force, frequency of apparition of the letters, etc.)

Condition of use

This programs is provided free and *'as is'*, without no explicit or implicit guarantee. Its use is only at the user's risk when he chose to use it. Under no circonstances will the author be held responsible of any possible dammage occuring by this use.

The most recent version can be downloaded here: http://www.allec.fr/Download.htm

Help can be found on this forum of discussion: http://alainlecomte.free.fr/phpBB2/index.php