Κρυπτογραφία

Εργασία εξαμήνου (2)

Εκπονήθηκε από τις:

Όλγα Βασιλείου, 01691

Χριστίνα Παναγιώτα Κομμάτα, 01637

Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική

2021-2022

Project 2 – The notepad

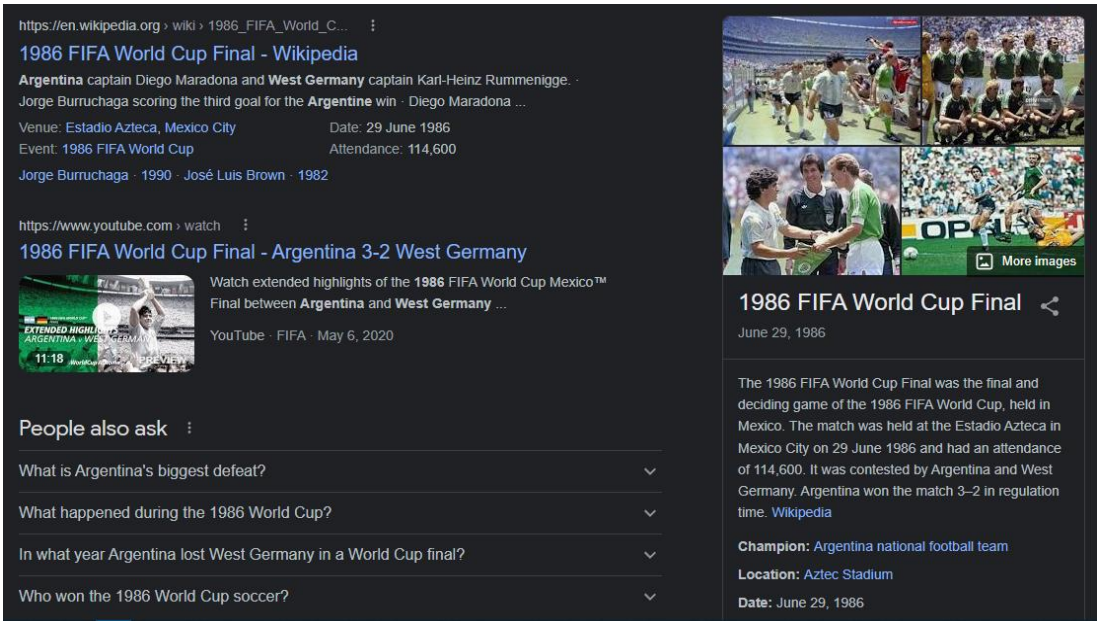
Στην παρούσα εργασία αποκρυπτογραφούμε τα δύο κρυπτογραφημένα μηνύματα ώστε να συλλέξουμε πληροφορίες για κάποιο ζητούμενο. Το κάθε μήνυμα περιέχει πληροφορία που είναι απαραίτητη για τα επόμενα.

Κείμενο 1 (text.pdf):

Διαβάζοντας το παρακάτω κείμενο, συλλέγουμε πληροφορίες για τον τρόπο κρυπτογράφησης του πρώτου κρυπτοκειμένου (screen.pdf):

« I have just returned from the concert. It was a fantastic end to a very bad day. Everybody was talking about the final and how we have lost the World Cup a few hours ago[1]. To be honest I believe that he is a great footballer, maybe the best of his generation, so let him take the World Cup to the capital of Campania[2]. The band in the concert was great[3]. I can't stop singing their last song. Maybe I will use the title of the last song, as the key to encrypt (DES) my next electronic message to you. From the title of the song, I will use only the consonants[4]. »

1) Η συναυλία πραγματοποιήθηκε στη χώρα που έχασε το World Cup.
2) Ο καλύτερος ποδοσφαιριστής της γενιάς του, ο οποίος ήταν παίκτης της Νάπολης (πρωτεύουσα της Καμπανίας) είναι ο *Diego Maradona*. Επομένως, συμπεραίνουμε ότι πρόκειται για τον αγώνα *1986 FIFA World Cup Final* μεταξύ Αργεντινής και Δυτικής Γερμανίας (https://en.wikipedia.org/wiki/1986_FIFA_World_Cup_Final).

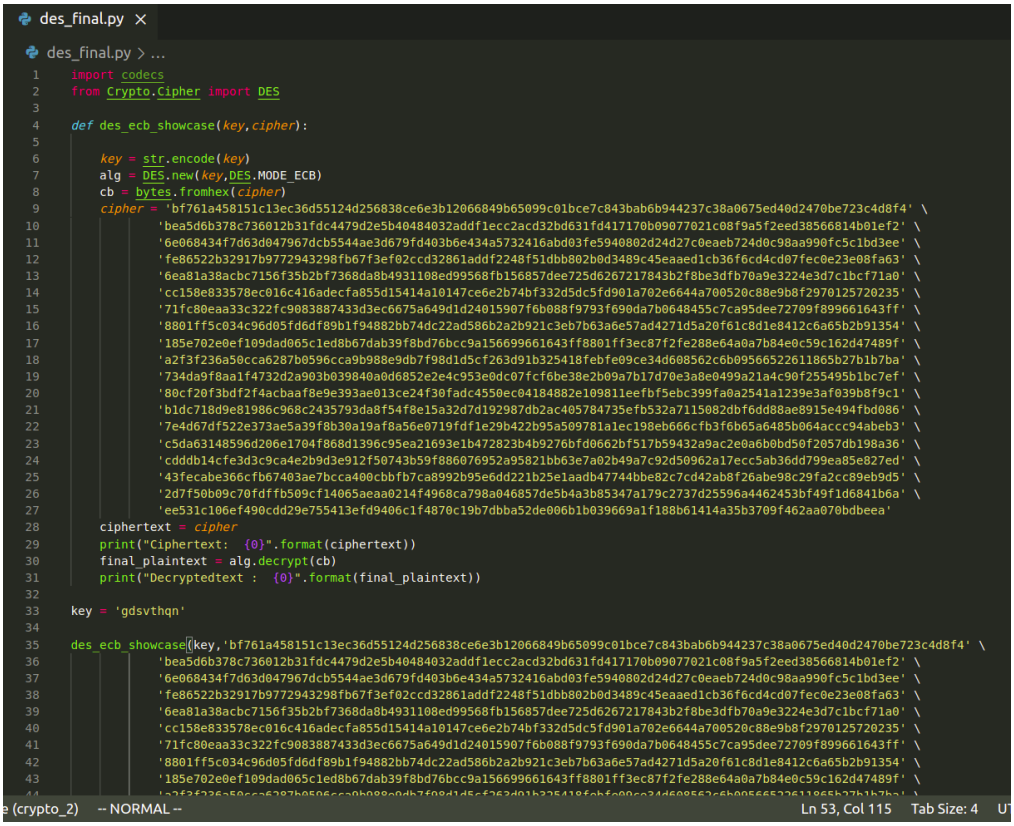


Εικόνα 1. Αποτελέσματα αναζήτησης του αγώνα

3) Η συναυλία που πραγματοποιήθηκε εκείνη την ημέρα (29 Ιουνίου 1986) στη Γερμανία από συγκρότημα είναι αυτή των *Queen*.
4) Το τελευταίο τραγούδι της συναυλίας τους ήταν το *God save the Queen* (https://www.setlist.fm/setlist/queen/1986/olympiahalle-munich-germany-13d45539.html), άρα το κλειδί της κρυπτογράφησης DES είναι *gdsvthqn*.

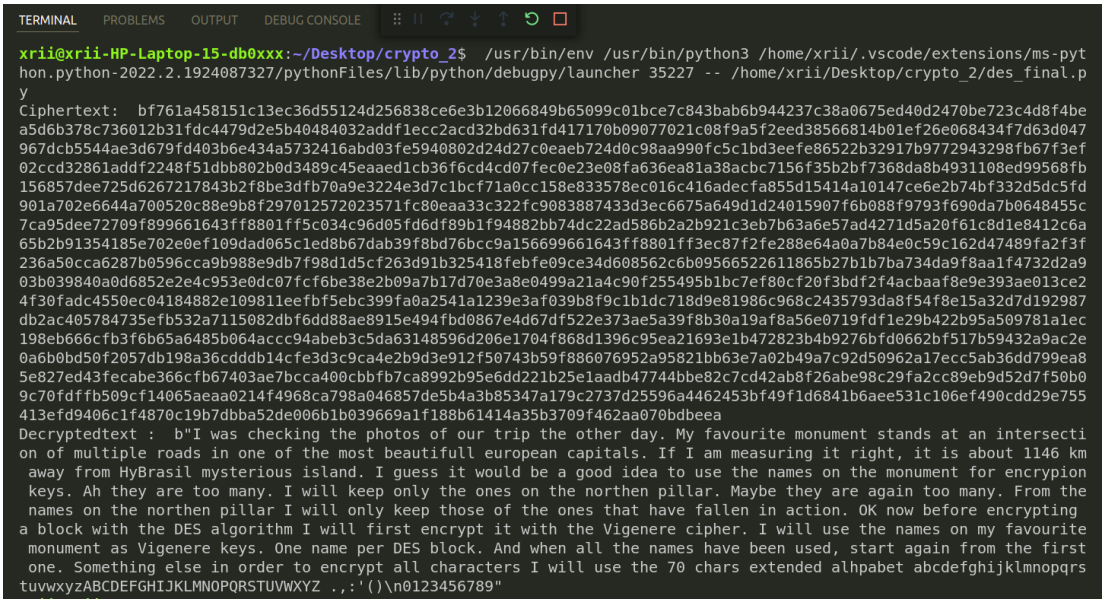
Κρυπτοκείμενο 1 (screen.pdf):

Το δεύτερο μήνυμα είναι κρυπτογραφημένο με τον αλγόριθμο μπλοκ *DES ECB* και κλειδί *gdsvthqn*. Χρησιμοποιώντας τον παρακάτω κώδικα σε python, φανερώνεται το αποκρυπτογραφημένο κείμενο.



```python
import codecs
from Crypto.Cipher import DES

def des_ecb_showcase(key,cipher):

    key = str.encode(key)
    alg = DES.new(key,DES.MODE_ECB)
    cb = bytes.fromhex(cipher)
    cipher = 'bf761a458151c13ec36d55124d256838ce6e3b12066849b65099c01bce7c843bab6b944237c38a0675ed40d2470be723c4d8f4' \
             'bea5d6b378c736012b31fdc4479d2e5b40484032addf1ecc2acd32bd631fd417170b09077021c08f9a5f2eed38566814b01ef2' \
             '6e068434f7d63d047967dcb5544ae3d679fd403b6e434a5732416abd03fe5940802d24d27c0eaeb724d0c98aa990fc5c1bd3ee' \
             'fe86522b32917b9772943298fb67f3ef02ccd32861addf2248f51dbb802b0d3489c45eaaed1cb36f6cd4cd07fec0e23e08fa63' \
             '6ea81a38acbc7156f35b2bf7368da8b4931108ed99568fb156857dee725d6267217843b2f8be3dfb70a9e3224e3d7c1bcf71a0' \
             'cc158e833578ec016c416adecfa855d15414a10147ce6e2b74bf332d5dc5fd901a702e6644a700520c88e9b8f297012572023571' \
             '71fc80eaa33c322fc9083887433d3ec6675a649d1d24015907f6b088f9793f690da7b0648455c7ca95dee72709f899661643ff' \
             '8801ff5c034c96d05fd6df89b1f94882bb74dc22ad586b2a2b921c3eb7b63a6e57ad4271d5a20f61c8d1e8412c6a65b2b91354' \
             '185e702e0ef109dad065c1ed8b67dab39f8bd76bcc9a156699661643ff8801ff3ec87f2fe288e64a0a7b84e0c59c162d47489f' \
             'a2f3f236a50cca6287b0596cca9b988e9db7f98d1d5cf263d91b325418febfe09ce34d608562c6b095665226118 65b27b1b7ba' \
             '734da9f8aa1f4732d2a903b039840a0d6852e2e4c953e0dc07fcf6be38e2b09a7b17d70e3a8e0499a21a4c90f255495b1bc7ef' \
             '80cf20f3bdf2f4acbaaf8e9e393ae013ce24f30fadc4550ec04184882e109811eefbf5ebc399fa0a2541a1239e3af039b8f9c1' \
             'b1dc718d9e81986c968c2435793da8f54f8e15a32d7d192987db2ac405784735efb532a7115082dbf6dd88ae8915e494fbd086' \
             '7e4d67df522e373ae5a39f8b30a19af8a56e0719fdf1e29b422b95a509781a1ec198eb666cfb3f6b65a6485b064accc94abeb3' \
             'c5da63148596d206e1704f868d1396c95ea21693e1b472823b4b9276bfd0662bf517b59432a9ac2e0a6b0bd50f2057db198a36' \
             'cdddb14cfe3d3c9ca4e2b9d3e912f50743b59f886076952a95821bb63e7a02b49a7c92d50962a17ecc5ab36dd799ea85e827ed' \
             '43fecabe366cfb67403ae7bcca400cbbfb7ca8992b95e6dd221b25e1aadb47744bbe82c7cd42ab8f26abe98c29fa2cc89eb9d5' \
             '2d7f50b09c70fdffb509cf14065aeaa0214f4968ca798a046857de5b4a3b85347a179c2737d25596a4462453bf49f1d6841b6a' \
             'ee531c106ef490cdd29e755413efd9406c1f4870c19b7dbba52de006b1b039669a1f188b61414a35b3709f462aa070bdbeea'
    ciphertext = cipher
    print("Ciphertext:  {0}".format(ciphertext))
    final_plaintext = alg.decrypt(cb)
    print("Decryptedtext :  {0}".format(final_plaintext))

key = 'gdsvthqn'

des_ecb_showcase(key,'bf761a458151c13ec36d55124d256838ce6e3b12066849b65099c01bce7c843bab6b944237c38a0675ed40d2470be723c4d8f4' \
             'bea5d6b378c736012b31fdc4479d2e5b40484032addf1ecc2acd32bd631fd417170b09077021c08f9a5f2eed38566814b01ef2' \
             '6e068434f7d63d047967dcb5544ae3d679fd403b6e434a5732416abd03fe5940802d24d27c0eaeb724d0c98aa990fc5c1bd3ee' \
             'fe86522b32917b9772943298fb67f3ef02ccd32861addf2248f51dbb802b0d3489c45eaaed1cb36f6cd4cd07fec0e23e08fa63' \
             '6ea81a38acbc7156f35b2bf7368da8b4931108ed99568fb156857dee725d6267217843b2f8be3dfb70a9e3224e3d7c1bcf71a0' \
             'cc158e833578ec016c416adecfa855d15414a10147ce6e2b74bf332d5dc5fd901a702e6644a700520c88e9b8f297012572023571' \
             '71fc80eaa33c322fc9083887433d3ec6675a649d1d24015907f6b088f9793f690da7b0648455c7ca95dee72709f899661643ff' \
             '8801ff5c034c96d05fd6df89b1f94882bb74dc22ad586b2a2b921c3eb7b63a6e57ad4271d5a20f61c8d1e8412c6a65b2b91354' \
             '185e702e0ef109dad065c1ed8b67dab39f8bd76bcc9a156699661643ff8801ff3ec87f2fe288e64a0a7b84e0c59c162d47489f' \
             'a2f3f236a50cca6287b0596cca9b988e9db7f98d1d5cf263d91b325418febfe09ce34d608562c6b095665226118 65b27b1b7ba' \
             '734da9f8aa1f4732d2a903b039840a0d6852e2e4c953e0dc07fcf6be38e2b09a7b17d70e3a8e0499a21a4c90f255495b1bc7ef' \
             '80cf20f3bdf2f4acbaaf8e9e393ae013ce24f30fadc4550ec04184882e109811eefbf5ebc399fa0a2541a1239e3af039b8f9c1' \
             'b1dc718d9e81986c968c2435793da8f54f8e15a32d7d192987db2ac405784735efb532a7115082dbf6dd88ae8915e494fbd086' \
             '7e4d67df522e373ae5a39f8b30a19af8a56e0719fdf1e29b422b95a509781a1ec198eb666cfb3f6b65a6485b064accc94abeb3' \
             'c5da63148596d206e1704f868d1396c95ea21693e1b472823b4b9276bfd0662bf517b59432a9ac2e0a6b0bd50f2057db198a36' \
             'cdddb14cfe3d3c9ca4e2b9d3e912f50743b59f886076952a95821bb63e7a02b49a7c92d50962a17ecc5ab36dd799ea85e827ed' \
             '43fecabe366cfb67403ae7bcca400cbbfb7ca8992b95e6dd221b25e1aadb47744bbe82c7cd42ab8f26abe98c29fa2cc89eb9d5' \
             '2d7f50b09c70fdffb509cf14065aeaa0214f4968ca798a046857de5b4a3b85347a179c2737d25596a4462453bf49f1d6841b6a' \
             'ee531c106ef490cdd29e755413efd9406c1f4870c19b7dbba52de006b1b039669a1f188b61414a35b3709f462aa070bdbeea')
```

Εικόνα 2. Κώδικας αποκρυπτογράφησης DES ECB



```
TERMINAL  PROBLEMS  OUTPUT  DEBUG CONSOLE

xrii@xrii-HP-Laptop-15-db0xxx:~/Desktop/crypto_2$  /usr/bin/env /usr/bin/python3 /home/xrii/.vscode/extensions/ms-python.python-2022.2.1924087327/pythonFiles/lib/python/debugpy/launcher 35227 -- /home/xrii/Desktop/crypto_2/des_final.py
Ciphertext:  bf761a458151c13ec36d55124d256838ce6e3b12066849b65099c01bce7c843bab6b944237c38a0675ed40d2470be723c4d8f4bea5d6b378c736012b31fdc4479d2e5b40484032addf1ecc2acd32bd631fd417170b09077021c08f9a5f2eed38566814b01ef26e068434f7d63d047967dcb5544ae3d679fd403b6e434a5732416abd03fe5940802d24d27c0eaeb724d0c98aa990fc5c1bd3eefe86522b32917b9772943298fb67f3ef02ccd32861addf2248f51dbb802b0d3489c45eaaed1cb36f6cd4cd07fec0e23e08fa636ea81a38acbc7156f35b2bf7368da8b4931108ed99568fb156857dee725d6267217843b2f8be3dfb70a9e3224e3d7c1bcf71a0cc158e833578ec016c416adecfa855d15414a10147ce6e2b74bf332d5dc5fd901a702e6644a700520c88e9b8f297012572023571fc80eaa33c322fc9083887433d3ec6675a649d1d24015907f6b088f9793f690da7b0648455c7ca95dee72709f899661643ff8801ff5c034c96d05fd6df89b1f94882bb74dc22ad586b2a2b921c3eb7b63a6e57ad4271d5a20f61c8d1e8412c6a65b2b91354185e702e0ef109dad065c1ed8b67dab39f8bd76bcc9a156699661643ff8801ff3ec87f2fe288e64a0a7b84e0c59c162d47489fa2f3f236a50cca6287b0596cca9b988e9db7f98d1d5cf263d91b325418febfe09ce34d608562c6b095665226118 65b27b1b7ba734da9f8aa1f4732d2a903b039840a0d6852e2e4c953e0dc07fcf6be38e2b09a7b17d70e3a8e0499a21a4c90f255495b1bc7ef80cf20f3bdf2f4acbaaf8e9e393ae013ce24f30fadc4550ec04184882e109811eefbf5ebc399fa0a2541a1239e3af039b8f9c1b1dc718d9e81986c968c2435793da8f54f8e15a32d7d192987db2ac405784735efb532a7115082dbf6dd88ae8915e494fbd0867e4d67df522e373ae5a39f8b30a19af8a56e0719fdf1e29b422b95a509781a1ec198eb666cfb3f6b65a6485b064accc94abeb3c5da63148596d206e1704f868d1396c95ea21693e1b472823b4b9276bfd0662bf517b59432a9ac2e0a6b0bd50f2057db198a36cdddb14cfe3d3c9ca4e2b9d3e912f50743b59f886076952a95821bb63e7a02b49a7c92d50962a17ecc5ab36dd799ea85e827ed43fecabe366cfb67403ae7bcca400cbbfb7ca8992b95e6dd221b25e1aadb47744bbe82c7cd42ab8f26abe98c29fa2cc89eb9d52d7f50b09c70fdffb509cf14065aeaa0214f4968ca798a046857de5b4a3b85347a179c2737d25596a4462453bf49f1d6841b6aee531c106ef490cdd29e755413efd9406c1f4870c19b7dbba52de006b1b039669a1f188b61414a35b3709f462aa070bdbeea
Decryptedtext :  b"I was checking the photos of our trip the other day. My favourite monument stands at an intersection of multiple roads in one of the most beautifull european capitals. If I am measuring it right, it is about 1146 km
 away from HyBrasil mysterious island. I guess it would be a good idea to use the names on the monument for encrypion
 keys. Ah they are too many. I will keep only the ones on the northen pillar. Maybe they are again too many. From the
 names on the northen pillar I will only keep those of the ones that have fallen in action. OK now before encrypting
a block with the DES algorithm I will first encrypt it with the Vigenere cipher. I will use the names on my favourite
 monument as Vigenere keys. One name per DES block. And when all the names have been used, start again from the first
 one. Something else in order to encrypt all characters I will use the 70 chars extended alhpabet abcdefghijklmnopqrs
tuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ .,:'()\n0123456789"
```

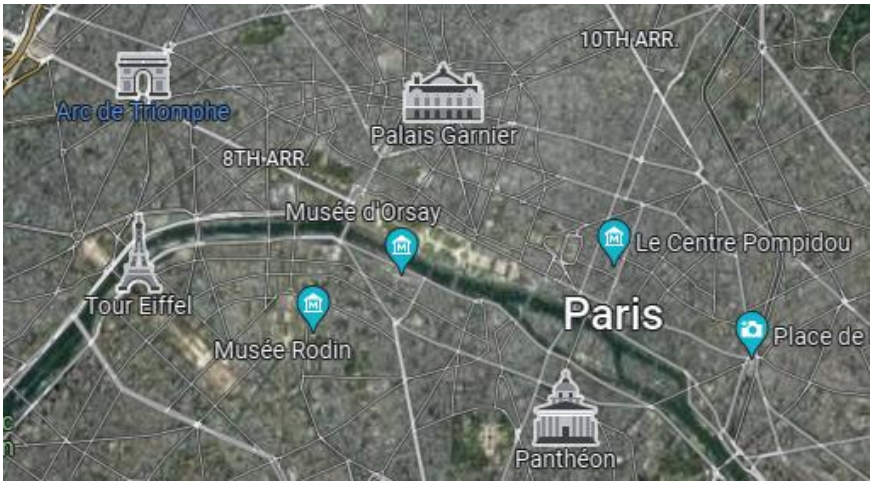
Εικόνα 3. Αποκρυπτογραφημένο μήνυμα

Από το αποκρυπτογραφημένο μήνυμα, συλλέγουμε πληροφορίες για τον τρόπο κρυπτογράφησης του τελευταίου κρυπτοκειμένου (paper2.pdf):

« I was checking the photos of our trip the other day. My favourite monument stands at an intersection of multiple roads in one of the most beautiful European capitals. If I am measuring it right, it is about 1146 km away from HyBrasil mysterious island[1]. I guess it would be a good idea to use the names on the monument for encryption keys. Ah they are too many. I will keep only the ones on the northern pillar. Maybe they are again too many. From the names on the northern pillar I will only keep those of the ones that have fallen in action[2]. OK now before encrypting a block with the DES algorithm I will first encrypt it with the Vigenere cipher[3]. I will use the names on my favourite monument as Vigenere keys[4]. One name per DES block. And when all the names have been used, start again from the first one. Something else in order to encrypt all characters I will use the 70 chars extended alphabet abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ .,:'()\n0123456789 »

1) Τοποθεσία του μυστηριώδους νησιού HyBrasil: https://www.google.com/search?q=hy+brasil+map+distance+from+ireland&newwindow=1&hl=en&sxsrf=APq-WBvcAWRlP4zZ7j_FYwk604b3x37s6w:1646128123372&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjKhrGQ0aT2AhX0SfEDHSuJCnwQ_AUoAXoECAEQAw&biw=1292&bih=609&dpr=1
Μνημείο σε απόσταση 1146 χιλιομέτρων από το νησί, σε "μία από τις ωραιότερες ευρωπαϊκές πρωτεύουσες": *Αψίδα του Θριάμβου, Παρίσι, Γαλλία*

Εικόνα 4. Απόσταση νησιού από ζητούμενη τοποθεσία



Εικόνα 5. Ζητούμενο μνημείο - Arc de Triomphe

2) Ως κλειδιά κρυπτογράφησης Vigenère, χρησιμοποιούνται τα ονόματα όσων σκοτώθηκαν στη μάχη, τα οποία βρίσκονται στον βόρειο πυλώνα του μνημείου (https://en.wikipedia.org/wiki/Names_inscribed_under_the_Arc_de_Triomphe#Northern_pillar). Τα κλειδιά είναι τα εξής: *DAMAS, PENNE, DAMPIERRE, MEUNIER, MARCEAU, DUHESME, GIRARD, LETORT, GOUVION, BASTOUL, BEAUREPAIRE, HUARD, JAMIN A., DESVAUX, BURCY, LOCHET, BINOT, GRILLOT*.
3) Το μήνυμα έχει κρυπτογραφηθεί πρώτα με αλγόριθμο Vigenère και στη συνέχεια με αλγόριθμο μπλοκ DES CBC, άρα αποκρυπτογραφούμε αρχικά το δοθέν κρυπτοκείμενο με τον αλγόριθμο αποκρυπτογράφησης DES.
4) Για την αποκρυπτογράφηση με Vigenère, χρησιμοποιούνται τα κλειδιά – ονόματα για κάθε DES μπλοκ.