Write-Up: Discreet Psychologist (Crypto)

|  |  |
| --- | --- |
| Ομάδα: | mousiko\_gymsasio\_agriniou\_lt\_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.) |
| Μαθητές/Μαθήτριες | Πέτρος Παπαθανασίου |

# Επισκόπηση Δοκιμασίας

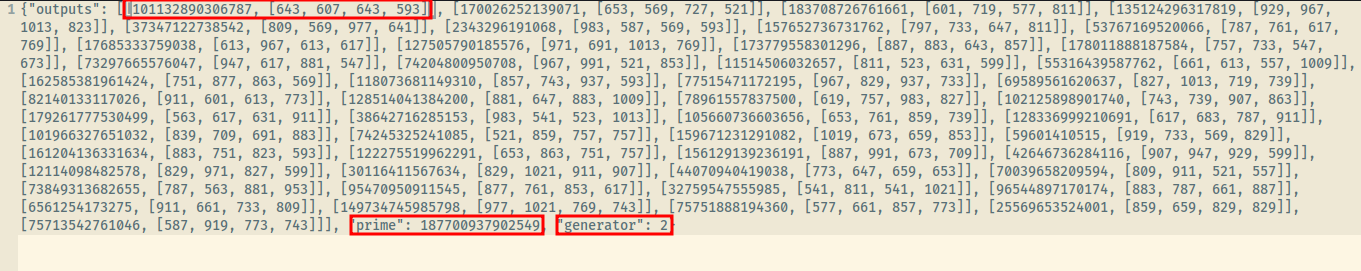
Η δοκιμασία μας δίνει δύο αρχεία, το source.py και το output.txt. Το source.py ασχολείται με την κρυπτογράφηση ενός μηνύματος και το output.txt μας δίνει τις πληροφορίες της κρυπτογράφησης. Σκοπός της δοκιμασίας είναι να προσπαθήσουμε να αντιστρέψουμε την διαδικασία κωδικοποίησης και να ανακτήσουμε το flag

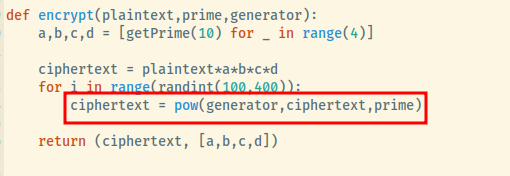
# Επίλυση

## Αρχική ανάλυση

Το αρχείο source.py ασχολείται με κρυπτογράφηση με την συνάρτηση pow(generator,ciphertext,prime). Από το αρχείο output.txt αμέσως παρατηρούμε ότι γνωρίζουμε το prime, τον generator και μια σειρά από αριθμούς της μορφής [101132890306787, [643, 607, 643, 593]]. Ο πρώτος αριθμός (101132890306787) δηλώνει τον κωδικοποιημένο χαρακτήρα του flag ciphertext. Οι επόμενοι τέσσερεις αριθμοί αποτελούν τους παράγοντες που χρησιμοποιούνται για την κωδικοποίηση του plaintext.

Η ευπάθεια είναι το γεγονός ότι γνωρίζουμε όλες τις πληροφορίες που χρησιμοποιήθηκαν στην κωδικοποίηση, δηλαδή τα ciphertext, prime, generator και τους παράγοντες.

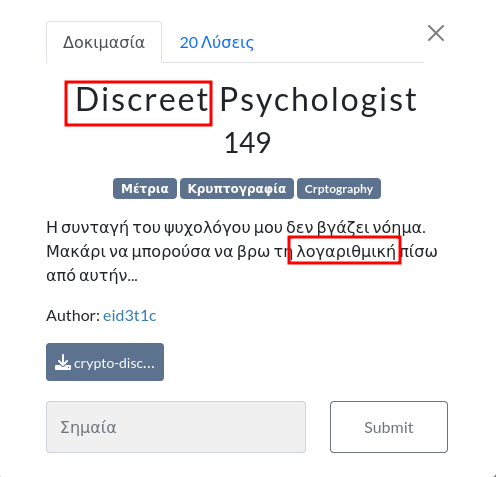




Τέλος, είναι γνωστό ότι η κωδικποίηση επαναλαμβάνεται από 100 έως 400 φορές.

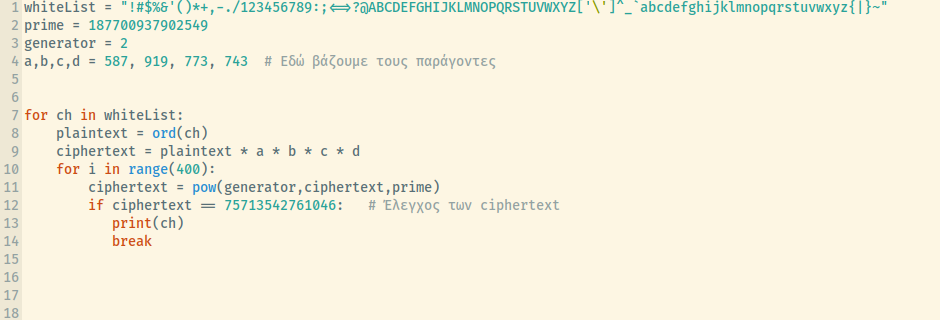
## Εκμετάλλευση ευπάθειας

Το πρώτο πράγμα που έκανα ήταν να ακολουθήσω την εκφώνηση και να χρησιμοποιήσω διακριτούς λογαρίθμους για να αντιστρέψω την λογική της κωδικοποίησης.

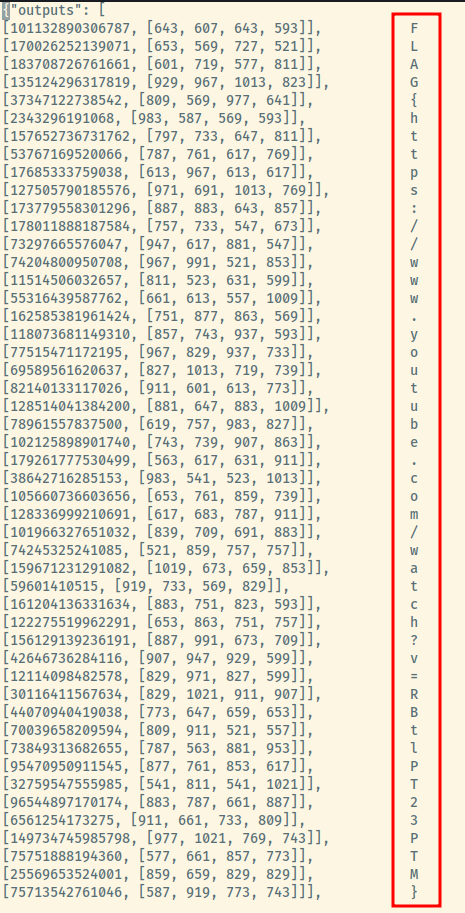


Αυτό δεν έχει αποτέλεσμα, καθώς διαπίστωσα ότι η επανάληψη από 100-400 φορές μου έδινε ως αποτέλεσμα μία ακολουθία χαρακτήρων και δεν ήξερα ποιος είναι ο σωστός.

Οπότε, προσανατολίστηκα στο να κάνω την διαδικασία της κωδικοποίησης και να ελέχγω αν τα αποτέλεσμα ciphertext που μου δίνει κάθε φορά θα ισούται με το ciphertext στο output.txt. Ως text για την κωδικοποίηση έπαιρνα χαρακτήρες από μία λίστα που είχε όλους τους εκτυπούμενους, και πιθανούς για flag, ascii χαρακτήρες. Άρα το πρόγραμμα κάθε φορά που έφτανε στην ισότητα, σταμάταγε και μου έκανε print στην κονσόλα τον χαρακτήρα που βρήκε. Με αυτήν την τεχνική, μπορούσα να τσεκάρω και την εγκυρότητα του προγράμματός μου, αφού γνώριζα ότι οι πρώτοι χαρακτήρες θα ήταν FLAG{. Κάθε φορά που έβρισκα έναν χαρακτήρα τον σημείωνα, ώστε που βρήκα όλο το flag.



Το πρόγραμμα το έτρεξα για όλα τα ciphertext.



# Σημαία

Η σημαία που βρέθηκε:

|  |
| --- |
| FLAG{https://www.youtube.com/watch?v=RBtlPT23PTM} |