SYLVARCON
a cybersecurity adventure
2049

Mission Name

The DNA Vaccine

Historical Context

Ethan and Claire uncover a crucial book containing the sequence of the DNA Vaccine they've been searching for during their adventures.

Technical Synopsis

The mission revolves around decrypting or decoding a crypto message hidden within the DNA sequence, essential for advancing their quest.

Mission Brief

In a designated location, an image depicting the DNA vaccine sequence awaits discovery. Can you decipher it and reveal the hidden message?

Detailed Assignment

Tasked with a vital role, Ethan must identify the cross-reference sequence hidden within the DNA and reconstruct it, a step critical for progressing in their journey.

Location

SHANGHAI | BACKSTREET BAR

Tools

- IP

Questions

What is the original key?

- 00111001001110000011001000110011001101110011010100110001001101000011000000110110

How many keys would be possible solution?

- 8!

What kind of chars are each element of the key?

- digits

Hints

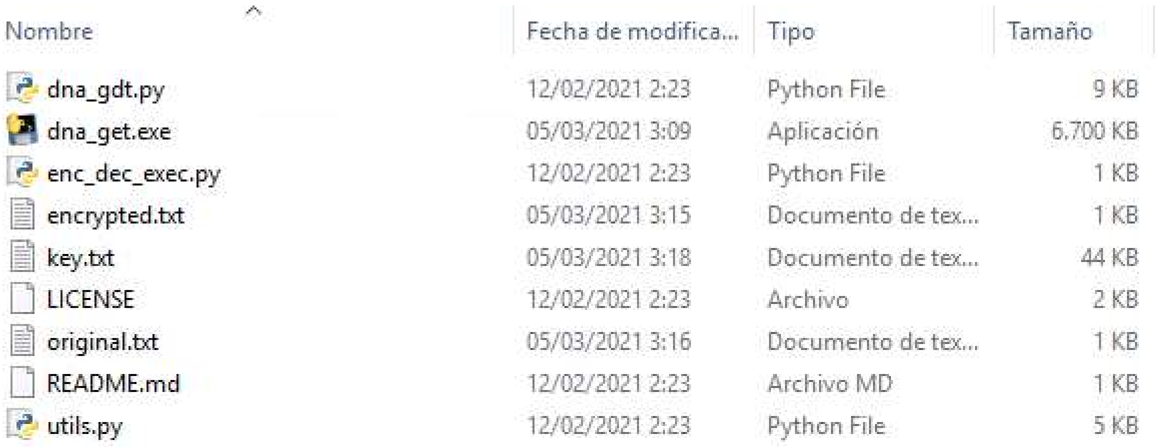
1. Maybe that link helps: https://github.com/JohnBogdan1/DNA-Genetic-Encryption-Technique/
2. The <key> is the key
3. Use the programme to generate lot of keys and find out its weakness or reverse the .exe to extract the key algorithm

Categories

- Encoding
- Steganography
- Cryptography
- Reversing
- Brute force

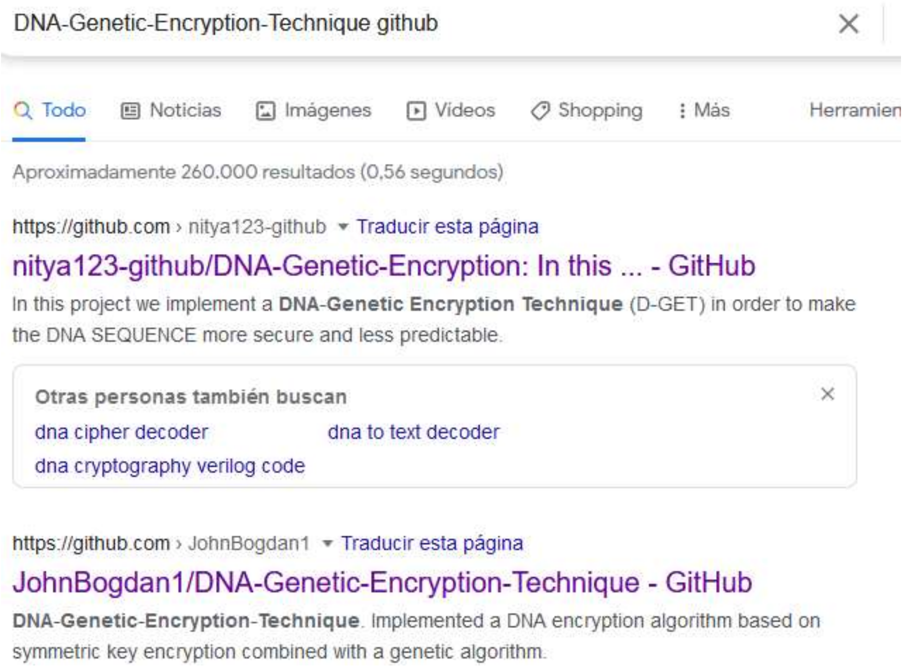
Write Up

To solve the challenge presented, players need to decrypt a message encoded in a DNA sequence using a missing encryption key. The process involves several steps, including locating a GitHub repository for a missing script, understanding the encryption process described in a key file, and ultimately, brute-forcing the encryption key based on provided clues. Here's a breakdown of the steps to solve the challenge



Nombre	Fecha de modifica...	Tipo	Tamaño
dna_gdt.py	12/02/2021 2:23	Python File	9 KB
dna_get.exe	05/03/2021 3:09	Aplicación	6.700 KB
enc_dec_exec.py	12/02/2021 2:23	Python File	1 KB
encrypted.txt	05/03/2021 3:15	Documento de tex...	1 KB
key.txt	05/03/2021 3:18	Documento de tex...	44 KB
LICENSE	12/02/2021 2:23	Archivo	2 KB
original.txt	05/03/2021 3:16	Documento de tex...	1 KB
README.md	12/02/2021 2:23	Archivo MD	1 KB
utils.py	12/02/2021 2:23	Python File	5 KB

Figure 1



DNA-Genetic-Encryption-Technique github

Aproximadamente 260.000 resultados (0,56 segundos)

https://github.com › nitya123-github ▾ Traducir esta página

nitya123-github/DNA-Genetic-Encryption: In this ... - GitHub

In this project we implement a **DNA-Genetic Encryption Technique** (D-GET) in order to make the DNA SEQUENCE more secure and less predictable.

Otras personas también buscan

dna cipher decoder
dna to text decoder
dna cryptography verilog code

https://github.com › JohnBogdan1 ▾ Traducir esta página

JohnBogdan1/DNA-Genetic-Encryption-Technique - GitHub

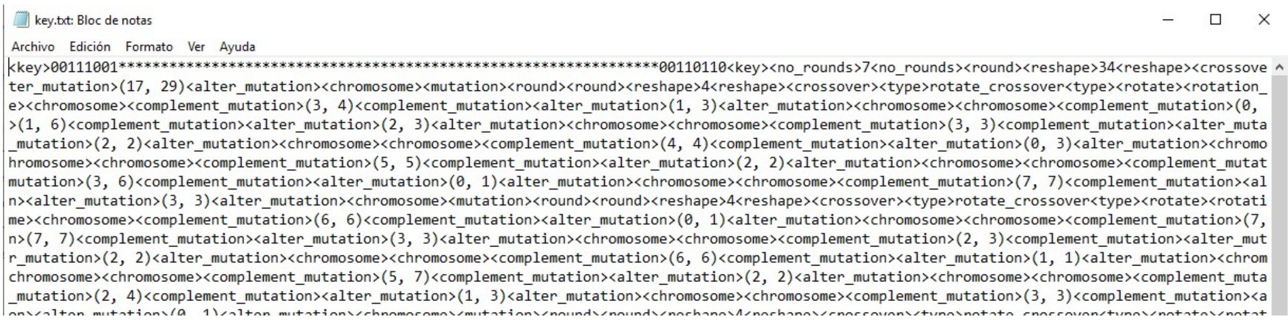
DNA-Genetic-Encryption-Technique. Implemented a DNA encryption algorithm based on symmetric key encryption combined with a genetic algorithm.

Figure 2

Step 1: Locate the GitHub Repository

Players find information in a README file that leads them to a GitHub repository: https://github.com/JohnBogdan1/DNA-Genetic-Encryption-Technique/

The repository contains an encryption technique, but the original script dna_get.py has been replaced with an executable, dna_get.exe.



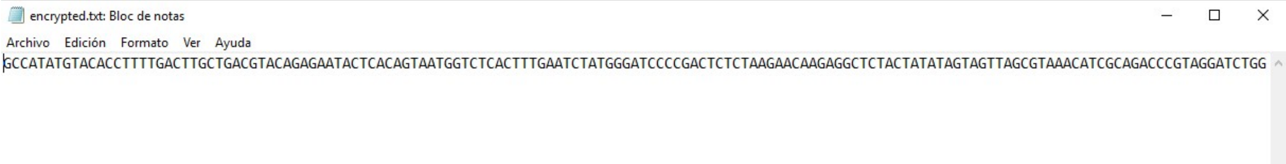
```
<key>00111001****************************************************************00110110<key><no_rounds>7<no_rounds><round><reshape>34<reshape><crossove
ter_mutation>(17, 29)<alter_mutation><chromosome><mutation><round><round><reshape>4<reshape><crossover><type>rotate_crossover<type><rotate><rotation_
e><chromosome><complement_mutation>(3, 4)<complement_mutation><alter_mutation>(1, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(0,
>(1, 6)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_mutation><alter_muta
_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 4)<complement_mutation><alter_mutation>(0, 3)<alter_mutation><chromo
hromosome><chromosome><complement_mutation>(5, 5)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutat
mutation>(3, 6)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(7, 7)<complement_mutation><al
n><alter_mutation>(3, 3)<alter_mutation><chromosome><mutation><round><round><reshape>4<reshape><crossover><type>rotate_crossover<type><rotate><rotati
me><chromosome><complement_mutation>(6, 6)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(7,
n>(7, 7)<complement_mutation><alter_mutation>(3, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mut
r_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(6, 6)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chrom
chromosome><chromosome><complement_mutation>(5, 7)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_muta
_mutation>(2, 4)<complement_mutation><alter_mutation>(1, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_mutation><a
on><alter_mutation>(0, 1)<alter_mutation><chromosome><mutation><round><round><reshape>4<reshape><crossover><type>rotate_crossover<type><rotate><rotat
```

Figure 3

Step 2: Understand the Encryption Process

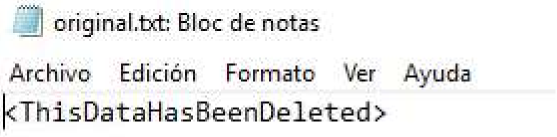
A key.txt file provides details on the encryption process and partially reveals the binary key: 00111001***00110110.

The Encripted.txt file contains the ciphered text as a DNA sequence, while the Original.txt shows that the original message has been removed.


encrypted.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

```
GCCATATGTACACCTTTTGACTTGCTGACGTACAGAGAATACTCACAGTAATGGTCTCACTTTGAATCTATGGGATCCCCGACTCTCTAAGAACAAGAGGCTCTACTATATAGTAGTTAGCGTAAACATCGCAGACCCGTAGGATCTGG
```

Figure 4


original.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

```
<ThisDataHasBeenDeleted>
```

Figure 5

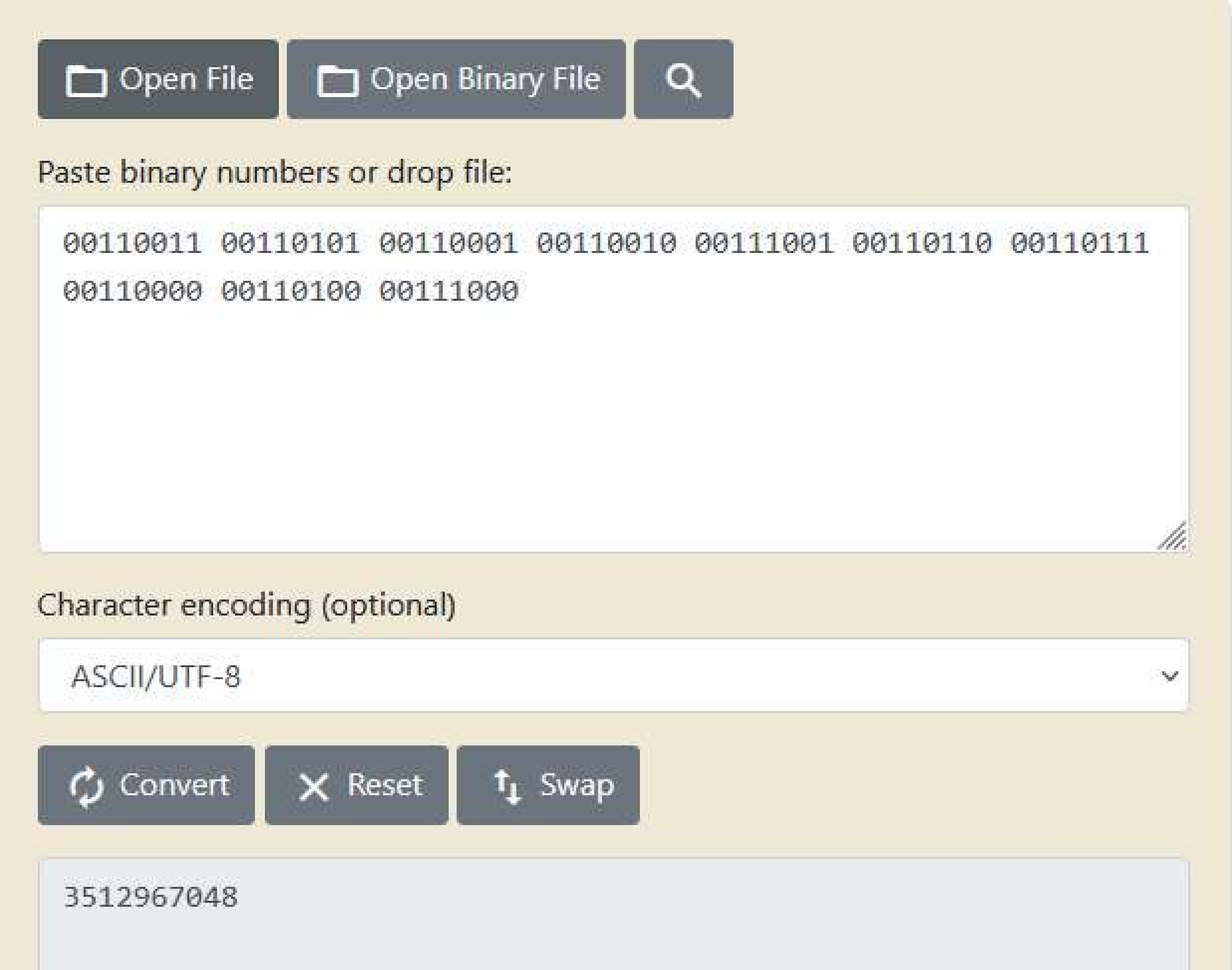
Step 3: Analyze the Encryption Key

Running dna_get.exe generates a new key, suggesting the need to reconstruct the original key for decryption.

The encryption key is predictable, composed of a 10-digit sequence using digits 0-9 in a random order, represented in binary format, with a length of 80 binary bits.

Step 4: Reconstruct the Encryption Key

Observations from generated keys indicate that each 8-bit block represents a different digit in binary, mapping directly to string digits.
The original key's known bits (00111001 and 00110110, translating to '9' and '6') reduce the brute-force scope to 8! (40,320) possibilities, making it feasible to attempt all combinations.



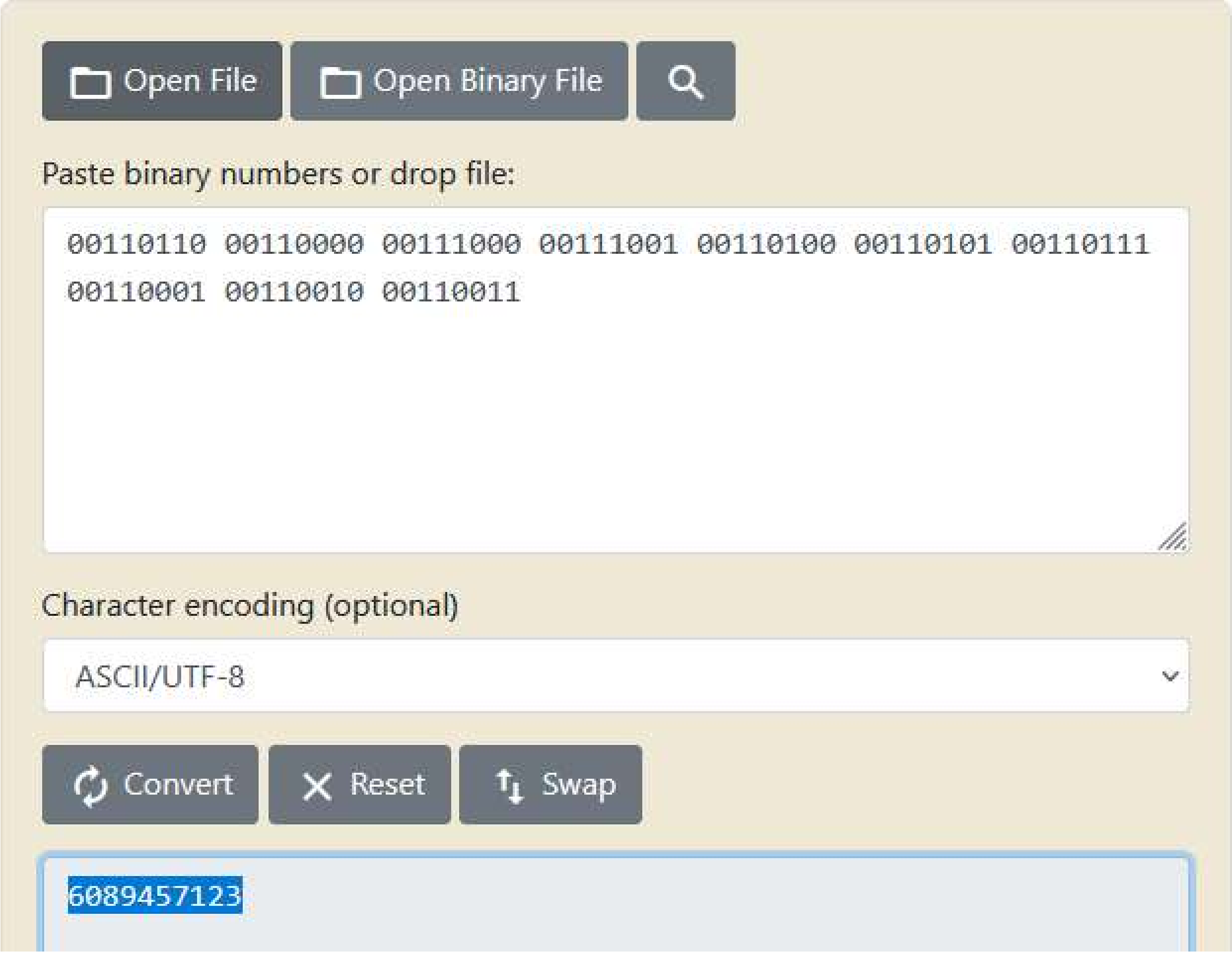
Paste binary numbers or drop file:

```
00110011 00110101 00110001 00110010 00111001 00110110 00110111
00110000 00110100 00111000
```

Character encoding (optional): ASCII/UTF-8

```
3512967048
```

Figure 6


Open File
Open Binary File
Paste binary numbers or drop file:
Character encoding (optional)
ASCII/UTF-8
Convert
Reset
Swap

```
00110110 00110000 00111000 00111001 00110100 00110101 00110111
00110001 00110010 00110011
```

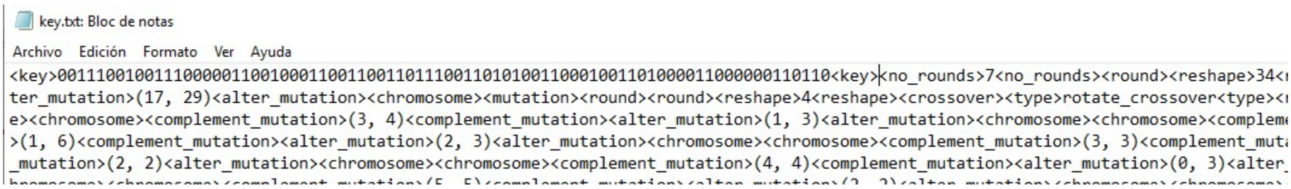
```
6089457123
```

Figure 7

Step 5: Brute-Force the Encryption Key

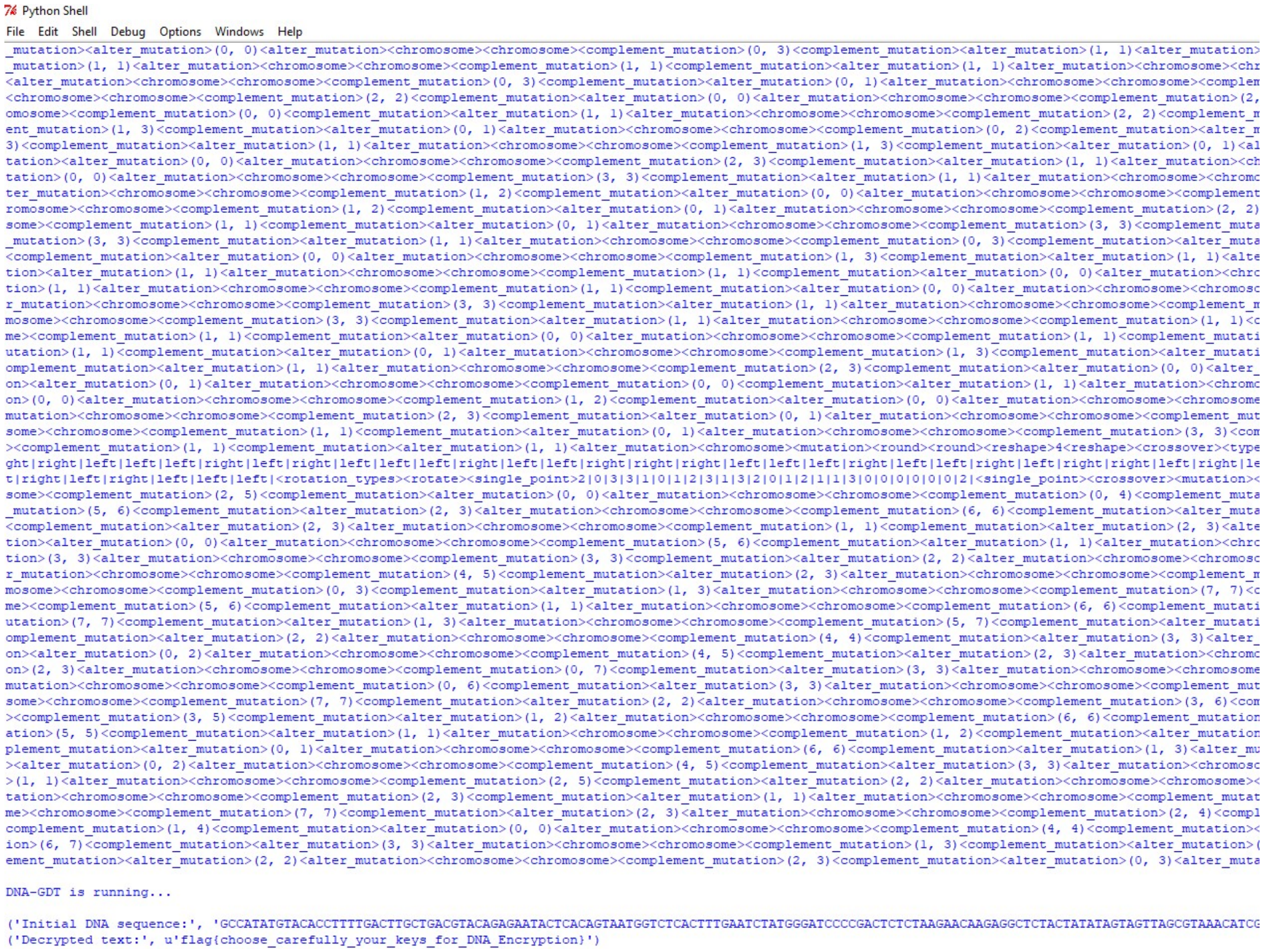
Develop a script to generate all possible keys considering the known parts of the original key and the pattern identified in the generated keys.

The script should use each generated key to attempt decryption using the dna_gdt.py (or corrected script name) against the encrypted DNA sequence.



```
<key>00111001001110000011001000110011001101110011010100110001001101000011000000110110<key><no_rounds>7<no_rounds><round><reshape>34<r
ter_mutation>(17, 29)<alter_mutation><chromosome><mutation><round><round><reshape>4<reshape><crossover><type>rotate_crossover<type><r
e><chromosome><complement_mutation>(3, 4)<complement_mutation><alter_mutation>(1, 3)<alter_mutation><chromosome><chromosome><compleme
>(1, 6)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_muta
_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 4)<complement_mutation><alter_mutation>(0, 3)<alter_
hromosome><chromosome><complement_mutation>(5, 5)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome>
```

Figure 8



```
_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation>
_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chr
<alter_mutation><chromosome><chromosome><complement_mutation>(0, 3)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complem
<chromosome><chromosome><complement_mutation>(2, 2)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(2,
omosome><complement_mutation>(0, 0)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 2)<complement_m
ent_mutation>(1, 3)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 2)<complement_mutation><alter_m
3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 3)<complement_mutation><alter_mutation>(0, 1)<al
tation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><ch
tation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromo
ter_mutation><chromosome><chromosome><complement_mutation>(1, 2)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement
romosome><chromosome><complement_mutation>(1, 2)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 2)
some><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_muta
_mutation>(3, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 3)<complement_mutation><alter_muta
<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 3)<complement_mutation><alter_mutation>(1, 1)<alte
tion><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chro
tion>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromoso
r_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_m
mosome><chromosome><complement_mutation>(3, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<c
me><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<complement_mutati
utation>(1, 1)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 3)<complement_mutation><alter_mutati
omplement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mutation>(0, 0)<alter_
on><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 0)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromo
on>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 2)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome
mutation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mut
some><chromosome><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<com
><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><mutation><round><round><reshape>4<reshape><crossover><type
ght|right|left|left|left|right|left|right|left|left|left|right|left|left|right|right|right|left|left|left|right|left|left|right|left|right|right|left|right|le
t|right|left|right|left|left|left|<rotation_types><rotate><single_point>2|0|3|3|1|0|1|2|3|1|3|2|0|1|2|1|1|3|0|0|0|0|0|0|2|<single_point><crossover><mutation><
some><complement_mutation>(2, 5)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 4)<complement_muta
_mutation>(5, 6)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(6, 6)<complement_mutation><alter_muta
<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 1)<complement_mutation><alter_mutation>(2, 3)<alte
tion><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(5, 6)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chro
tion>(3, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 3)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromoso
r_mutation><chromosome><chromosome><complement_mutation>(4, 5)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_m
mosome><chromosome><complement_mutation>(0, 3)<complement_mutation><alter_mutation>(1, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(7, 7)<c
me><complement_mutation>(5, 6)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(6, 6)<complement_mutati
utation>(7, 7)<complement_mutation><alter_mutation>(1, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(5, 7)<complement_mutation><alter_mutati
omplement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 4)<complement_mutation><alter_mutation>(3, 3)<alter_
on><alter_mutation>(0, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 5)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromo
on>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(0, 7)<complement_mutation><alter_mutation>(3, 3)<alter_mutation><chromosome><chromosome
mutation><chromosome><chromosome><complement_mutation>(0, 6)<complement_mutation><alter_mutation>(3, 3)<alter_mutation><chromosome><chromosome><complement_mut
some><chromosome><complement_mutation>(7, 7)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(3, 6)<com
><complement_mutation>(3, 5)<complement_mutation><alter_mutation>(1, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(6, 6)<complement_mutation
ation>(5, 5)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 2)<complement_mutation><alter_mutation
plement_mutation><alter_mutation>(0, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(6, 6)<complement_mutation><alter_mutation>(1, 3)<alter_mu
><alter_mutation>(0, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 5)<complement_mutation><alter_mutation>(3, 3)<alter_mutation><chromoso
>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 5)<complement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><
tation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mutation>(1, 1)<alter_mutation><chromosome><chromosome><complement_mutat
me><chromosome><complement_mutation>(7, 7)<complement_mutation><alter_mutation>(2, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 4)<compl
complement_mutation>(1, 4)<complement_mutation><alter_mutation>(0, 0)<alter_mutation><chromosome><chromosome><complement_mutation>(4, 4)<complement_mutation><
ion>(6, 7)<complement_mutation><alter_mutation>(3, 3)<alter_mutation><chromosome><chromosome><complement_mutation>(1, 3)<complement_mutation><alter_mutation>(
ement_mutation><alter_mutation>(2, 2)<alter_mutation><chromosome><chromosome><complement_mutation>(2, 3)<complement_mutation><alter_mutation>(0, 3)<alter_muta

DNA-GDT is running...

('Initial DNA sequence:', 'GCCATATGTACACCTTTTGACTTGCTGACGTACAGAGAATACTCACAGTAATGGTCTCACTTTGAATCTATGGGATCCCCGACTCTCTAAGAACAAGAGGCTCTACTATATAGTAGTTAGCGTAAACATCG
('Decrypted text:', u'flag{choose_carefully_your_keys_for_DNA_Encryption}')
```

Figure 9

Step 6: Decrypt the Message

Upon finding the correct key, use the DNA Genetic Encryption Technique to decrypt the Encripted.txt DNA sequence back into the original message.

The successful decryption will reveal the hidden message or flag that players were tasked to find.

Flag Information

flag{choose_carefully_your_keys_for_DNA_Encryption}