

Criptografía y Blockchain

Módulo 1 - Laboratorio

Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.
- Descargar los elementos necesarios.



Ejercicio: Criptoanálisis

Se ha interceptado el siguiente mensaje cifrado:

Gdnkrauvhkdcrdxpxgsxpdkkvggvsxzqnvqwzquv
sxuxnqrndpfzxaxklruxqdguxkdktlvsrnrndklxqpd
wxpvdknmrevpnvqxgviwxurevsxfzxqvazxsdqpx
kgxrsvpavkuvsvpdfzxggvpzpzdkrvpfzxqvxpxq
dzuvkrydsvpdmdnxkgv

Sabiendo que se ha aplicado la transformación
afín, criptoanalizar y extraer el mensaje oculto.



Existen muchas **herramientas para criptoanálisis**, tanto *online* como *offline*, pero todas se basan en la ejecución de algún *script* o programa. De los diversos lenguajes de programación existentes, el más adecuado es Python.

Vamos a usar un pequeño script en Python para hacer un ataque de fuerza bruta. ¿Qué es esto? Muy simple: se trata de probar todas las combinaciones posibles, para dar con la solución correcta. No necesitas saber nada de programación, solo seguir los pasos que se detallan a continuación:

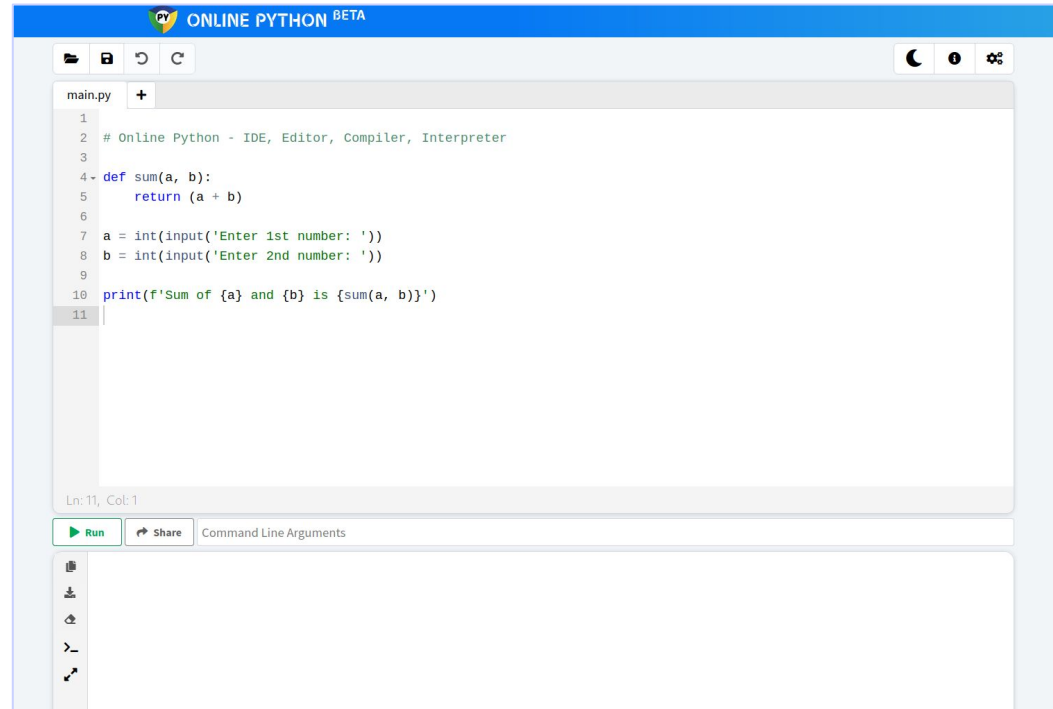
1. Descargar el archivo ***afin.py***, disponible en las descargas de Alumni.
2. Deberás abrir un intérprete online de Python. Existen muchos, los más destacados son:

- [Online-python.com](https://online-python.com)
- [Programiz.com](https://programiz.com)
- [Onlinegdb.com](https://onlinegdb.com)

Para este laboratorio usaremos el primero.

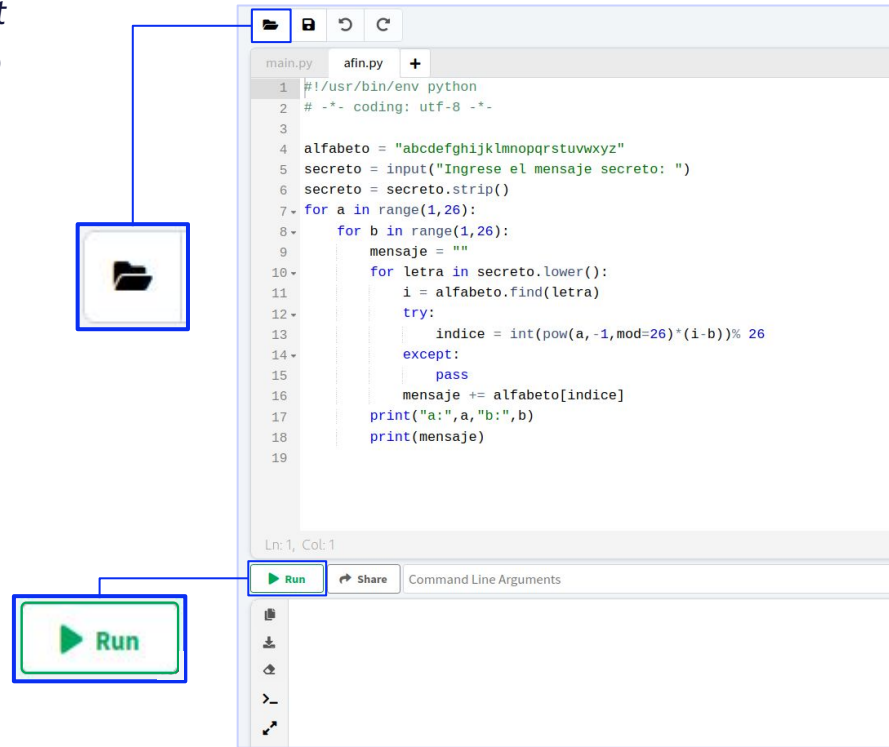
Es requisito para esta tarea utilizar un navegador web.

3. Al abrir **Online Python**, nos encontraremos con una pantalla similar a la siguiente:

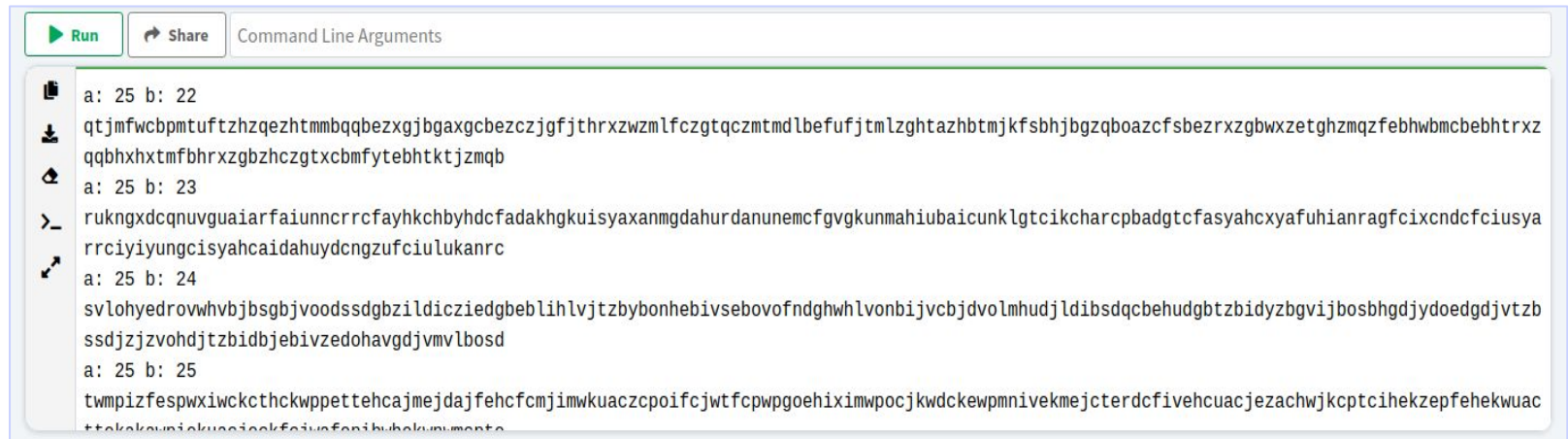


4. En la parte superior, podemos cargar el *script* **afin.py** haciendo clic en el botón. El resultado es el siguiente:

5. Ejecutamos el *script* haciendo clic sobre el botón **Run**.



6. Aparece la leyenda “*Ingrese el mensaje secreto:*”. Ahí copiamos y pegamos el criptograma y presionamos **Enter**. La salida se verá algo así:



```

a: 25 b: 22
qtjmfwbcpmtuftzhzqezhtmmqqbezxgjbaxgcbezcjgfgjthrxzwmfzczgtqcztmdlbfufjtmzgtazhbtmjksbhjbgzqboazcfsbezrxzgbwxzetghzmqzfebhwbmcbebhtrxz
qqbhxxtmfbbhrxzgbzhczgtxcbmfytebhtktjzmqb
a: 25 b: 23
rukngxdcqnuvguaiarfaiunnrrcfayhkchbyhdcfadakhgkuisyaxanmgdahurdanunemcsvgkunmahiuabaicunklgtcikcharcpbadgtcfasyahcxyafuhianragfcixcndcfciusya
rrciyiyungcisyahcaidahuydcngzufciulukanrc
a: 25 b: 24
svlohyedrovwhvbjsbgbjvoodssdgbzildicziedgbeblhlvtzbybonhebvsebovofndghwhlvonbijvcbjdvolmhudjldibsdqcbbehudgbtzbidyzbvgvijbosbhgdjydoedgdjvtzb
ssdjzjzvohdjtzbidbjebivzedohavgdjvmvlbosd
a: 25 b: 25
twmpizfespxiwcckthckwppettehcajmejdajfehcfcmjimwkuaczpciofcjwtfcpwpgoeihximwocjkwdckewpmnivekmejterdcfivehuacjezachwjkptcihekzepfehekhuac
ttakekuniakuaaiaakfaiaafoaibuhakunento

```

7. Encuentra el texto claro.

**¡Sigamos
trabajando!**