Zadanie 1

Dane jest funkcja f:

```
import hashlib

SIZE = ... # w zależności od wariantu zadania

def f(x):
    # x[:SIZE] zwraca SIZE pierwszych znaków x
    return hashlib.sha256("WarsztatyWWW" + x).hexdigest()[:SIZE]
```

Znajdź kolizje funkcji `f` tzn. takie różne dwie wartości x, y takie, że $f(x) = f(y)$, dla:

- `SIZE=4` (łatwe)
- `SIZE=10` (średnie)
- `SIZE=18` (trudniejsze)

W rozwiązaniu opisz sposób pozyskania wyniku (prześlij kody programów itp).

Wskazówka: nie analizuj funkcji SHA-256, potraktuj ją jako *czarną skrzynkę*.

Zadanie 2

Niech X, Y będą niezależnymi zmiennymi losowymi na zbiorze $0, 1, ..., N-1$. Dodatkowo X ma rozkład jednostany. Pokaż, że $(X + Y) \mod N$ jest zmienną o rozkładzie jednostajnym.

Pomyśl, co to oznacza dla bezpieczeństwa szyfrów jednorazowych (one-time pad).

Zadanie 3

Przechwyciłeś wiadomość zaszyfrowaną następującym programem (napisanym w Pythonie 2):

```
import binascii

key = '.....' # tutaj jest tajny klucz, tobie nieznany
data = 'YYYYYY' # tutaj jest wiadomość do zaszyfrowania
ret = ''
for i in range(len(data)):
    ret += chr(ord(key[i]) ^ ord(data[i]))
print(binascii.hexlify(ret).encode())
```

Odszyfruj:

```
4e68f8385e6cde624b68a501e0e64eb77fbe89e92db95a282ff62a4415f8a8a6838f750a4e68a246
d829ad5b22eb0a29c7d2390fda2a5011771c6d3cad22b3d60477759a1ead5137c8cde82d493c9208
eb3ea02133438508
```

Udało ci się także pozyskać zarówno zaszyfrowany jak i niezaszyfrowany tekst innej wiadomości. Wiesz, że następująca wiadomość (*nie ma w niej znaków podziału linii*)

```
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud
exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
```

szyfruje się do:

```
4c46de08610997735679e86fe5fd57aa68b989a015f84c366aee671d56ffafb1c6856f4f7474b70e
cd77ce6c24fc4933c8dc7d4696616858234f463dfa32b398417c65c851e25479d888e4314a6ec500
f67da52c3d4f8448ef183ff6587a2d1b7d053de83bc92cd73712de075e3c0b94a6bbf442550db80a
775dcaba910cdb8bd20e6296b7cf1c087426491ee266a7b7ae61bcb8771c1a315f4160b66642bdde
edb528677baf6763b8b82d4bf6aa6c2d012c737c7842802f4437f18c2c8600e16618a0a1a5b83513
84edc392067d3d30ab7b0851406ca61e46a7e23bd72b81bf87c0694a9c2298736c
```

Informacje

Nie musisz robić wszystkich zadań. Rozwiązania prześlij na adres michal+www12@zielinscy.org.pl.