Enunciado

- 1. Pretende-se um protótipo protocolo $\binom{N}{N-1}$ -OT, usando a abordagem LPN "Learning Parity with Noise" +Capítulo 6d: Oblivious Linear Evaluation para mensagens de n bytes (i.e. $8 \times n$ bits) que possa ser convertido para mensagens $m \in \mathbb{F}_p^n$ (vetores de n componentes no corpo finito \mathbb{F}_p). Para isso
 - A. Implemente um protótipo do protocolo LPN $\binom{N}{N-1}$ -OT para mensagens de n bytes (i.e. $8 \times n$ bits). Ver +Capítulo 6d: Oblivious Linear Evaluation
 - B. Codificando os elementos de um corpo primo F_p em "arrays" de "bytes", converta a solução anterior num protocolo $\binom{N}{N-1}$ -OT em que as mensagens são vetores F_p^{ℓ} .

PARTE A

Definição de variáveis

In [1]:

```
p = 2
F = GF(p)
n = 8
V = VectorSpace(F, n) # Espaço vetorial F_p^n
lambda_security = 128
V
```

Out[1]:

Vector space of dimension 8 over Finite Field of size 2

Gerador de Bernoulli

O problema LPN (Learning Parity with Noise) baseia-se na dificuldade computacional de resolver sistemas lineares corrompidos por um erro. Especificamente, em LPN, temos um conjunto de equações da forma:

$$y = Ax + e$$

onde:

- A é uma matriz binária $m \times n$ (geralmente aleatória).
- x é um vetor secreto de n bits.
- e é um vetor de erro, onde cada entrada é 1 com uma pequena probabilidade ε (geralmente pequena, como 0.10.1 ou 0.20.2).
- y é o vetor de observações.

O vetor de erro ee segue uma distribuição Bernoulli com parâmetro $\epsilon \epsilon$, ou seja:

$$e_i \sim Bernoulli(\epsilon)$$

Isso significa que cada bit e_i tem probabilidade ϵ de ser 1 (ruído) e 1 – ϵ de ser 0 (sem ruído).

A forma mais direta de implementar um gerador de Bernoulli $\mathcal{B}(\epsilon)$ com a precisão de n bits, é o algoritmo.

$$\mathcal{B}(\epsilon) \equiv \vartheta \, w \leftarrow \{0,1\}^n \cdot \text{ if } \sum_{i=1}^n w_i 2^{-i} \le \epsilon \text{ then } 1 \text{ else } 0$$

Aqui $\hat{w} \equiv \sum_{i=1}^{n} 2^{-i} w_i$ é o designado racional de Lebesgue determinado pela string de bits w. Em muitos CPU's , \hat{w} pode ser calculado em tempo constante ; por isso, este é um processo usual para gerar uniformemente racionais no intervalo [0, 1].

```
In [2]:
```

```
import random

def bernoulli(epsilon, n=53):
    """

    Gera uma amostra de Bernoulli B(epsilon) usando a construção de Lebesgue.
    - epsilon: parâmetro da distribuição de Bernoulli (0 < epsilon < 1)
    - n: número de bits para a precisão (default: 53, precisão de um double)
    """

# Gera a string de bits aleatórios {0,1}^n
    w = [random.randint(0, 1) for _ in range(1, n+1)]

# Calcula o racional de Lebesgue
    w_hat = sum(w[i-1] * 2^(-i) for i in range(1,n+1))

    return 1 if w_hat <= epsilon else 0

def bernoulli_lambda(epsilon, n=53, lambda_ = lambda_security):
    return [bernoulli(epsilon,n) for _ in range(lambda_)]

# Teste com epsilon = 0.1
epsilon = 0.1
print(bernoulli_lambda(epsilon))</pre>
```

0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0]

Learning Party with Noise

O gerador LPN_{λ e}(s), para um segredo s $\leftarrow \mathcal{B}^{\lambda}$, usa parâmetros λ e ϵ definindo-se do seguinte modo

$$\mathsf{LPN}_{\lambda,\varepsilon}(\mathsf{s}) \equiv \vartheta a \leftarrow \mathcal{B}^{\lambda} \cdot e \leftarrow \mathcal{B}(\varepsilon) \cdot \vartheta t \leftarrow \mathsf{s} \cdot a + e \cdot \langle a, t \rangle$$

Aqui $\mathbf{s} \cdot a \equiv \sum_i \mathbf{s}_i \times a_i$ denota o produto interno dos dois vetores.

In [3]:

```
def LPN_generator(lambda_, epsilon,s):
    """Gera um par (a, t) segundo o protocolo LPN."""
    # Vetor gerado a partir do gerador de Bernouli
    a = bernoulli_lambda(epsilon)
    # Erro e seguindo uma distribuição de Bernoulli B(epsilon)
   e = bernoulli(epsilon)
    # Computa t = s \cdot a + e onde s.a = sum i(s i \times a i)
    for i in range(0,lambda security):
        t += s[i] * a[i]
    t = t % 2
    return a, t
# Exemplo de uso com lambda = 10 e epsilon = 0.1
epsilon = 0.1
# Segredo s gerado a partir do gerador de Bernouli
secret = bernoulli_lambda(epsilon)
a, t = LPN generator(lambda security, epsilon, secret)
print("Vetor a:", a)
print("Valor t:", t)
```

Operação Choose(b)

Definindo primeiramente funções auxiliares:

In [4]:

```
import hashlib
def xof(seed: bytes, nbytes: int):
    shake = hashlib.shake_128()
    shake.update(seed)
    return shake.digest(nbytes) # retorna nbytes de saída
def xof_bits(seed: bytes, nbits: int):
    nbytes = (nbits + 7) // 8
    output = xof(seed, nbytes)
    bits = []
    for byte in output:
        for i in range(8):
             bits.append((byte \gg (7 - i)) & 1)
             if len(bits) == nbits:
                 return bits
def bytes_to_bits(byte_string):
    bits = []
    for byte in byte string:
        for i in range(8):
            bits.append((byte >> i) & 1)
    return bits
def bits_to_bytes(bits):
    byte array = bytearray()
    for \bar{i} in range(0, len(bits), 8):
        byte = 0
        for j in range(8):
             if i + j < len(bits):</pre>
                 byte |= bits[i + j] << j</pre>
        byte_array.append(byte)
    return bytes(byte_array)
```

E definindo as classes Sender e Receiver:

Classe Sender

```
In [5]:
```

```
class Sender:
        __init__(self, alpha, l, xof_name="shake128"):
   def
        self.alpha = alpha
       self.l = l
        self.xof_name = xof_name
       self.seed = f"{alpha}:{l}".encode() # usa <math>\alpha e \ell como seed
        self.criterion = None
       self.pks = []
        self.N = 100
       self.mensagens = self.gerar_mensagens()
        self.r = []
       self.criptogramas = []
        self.t = self.N
   def gerar mensagens(self):
       n bvtes = 6
        return [f"msg{i:03d}".encode().ljust(n_bytes, b'\x00')[:n_bytes] for i in range(self.N)]
   def get_vector_ai_ui(self, i, lambda_):
         ""Retorna (a_i, u_i) & F_2^lambda × F_2, para índice i"""
        # gera (\lambda + 1) bits para cada i
       seed i = self.seed + f":{i}".encode()
       bits = xof_bits(seed_i, lambda_ + 1)
       a i = bits[:lambda_]
       u_i = bits[lambda_] # bit extra
        return a_i, u_i
   def get criterion sequence(self, lambda ):
        self.criterion = [self.get vector ai ui(i, lambda ) for i in range(1, self.l + 1)]
   def receive_and_verifypks(self, pks):
        self.pks = pks
        for i in range(self.l):
            soma = sum(pks[i][k] for k in range(self.N)) % 2
              u_i = self.criterion[i] # a_i não é necessário aqui
            if soma != u_i:
                print(f"FALHA na linha i={i}: soma={soma}, u_i={u_i}")
                return False
       print("Verificação OK: todas as somas coincidem com u_i")
        return True
   def gerar r(self, delta, p=0.1):
       while True:
            r = [bernoulli(p) for _ in range(self.l)]
            if sum(r) <= delta:</pre>
                self.r = r
                return
   def calcular_criptogramas(self):
        for _ in range(self.t):
            self.gerar_r(128)
            a = [0] * lambda_security
            for i in range(self.l):
                if self.r[i] == 1:
                    аi,
                          = self.criterion[i]
                    a = [(a[j] + a i[j]) % 2 for j in range(lambda security)]
            criptogramas k = []
            for k in range(self.N):
                msg_bits = bytes_to_bits(self.mensagens[k]) # Lista de bits da mensagem
                c k = []
                for bit in msg_bits:
                    soma = sum(self.r[i] * self.pks[i][k] for i in range(self.l)) % 2
                    c_k.append((bit + soma) % 2)
                criptogramas_k.append(c k)
            self.criptogramas.append((a, criptogramas_k))
   def print_info(self):
       print("self.alpha: ",self.alpha)
       print("self.l: ",self.l)
       print("self.xof name: ",self.xof name)
       print("self.seed: ",self.seed)
       print("self.criterion: ",self.criterion)
```

Classe Receiver

In [6]:

```
class Receiver:
   def init (self, eps, lambda =128):
```

```
self.alpha = None
    self.l = None
    self.eps = eps
    self.secrets = []
    self.criterion = None
    self.N = 100
    self.t = None
    self.b = 10 # Não quero a décima mensagem do Sender
def receive alpha l(self, alpha, l):
    self.alpha = alpha
    self.l = l
    self.seed = f"{alpha}:{l}".encode()
    self.criterion = self.get criterion sequence(lambda security)
def get_vector_ai_ui(self, i, lambda_):
    seed_i = self.seed + f":{i}".encode()
    bits = xof_bits(seed_i, lambda_ + 1)
    a_i = bits[:lambda_]
    u i = bits[lambda ]
    return a_i, u_i
def get_criterion_sequence(self, lambda_):
    return [self.get_vector_ai_ui(i, lambda_) for i in range(1, self.l + 1)]
def generate N secrets(self):
    self.secrets = []
    for k in range(self.N):
        if k == self.b:
            self.secrets.append(None) # s b = \bot
        else:
            s k = bernoulli lambda(self.eps, lambda security)
            print(f"s_{k} = \{s_{k}\}")
            self.secrets.append(s_k)
def generate_pks(self):
    # Inicializar t[i][k]
    self.t = [[0 for _ in range(self.N)] for _ in range(self.l)]
    for i in range(se\overline{l}f.l):
        a i, u i = self.criterion[i]
        soma = 0
        for k in range(self.N):
            if k != self.b:
                s_k = self.secrets[k]
                dot = sum([a_i[j] * s_k[j] for j in range(lambda_security)]) % 2
                e = bernoulli(self.eps)
                t_i = (dot + e) % 2
                self.t[i][k] = t_ik
                soma = (soma + t_ik) % 2
            else:
                self.t[i][k] = None
        # Calcula t_{i,b} como complemento para somar a u_i
        self.t[i][self.b] = (u_i - soma) % 2
def recuperar_mensagens(self, a, c):
    mensagens recuperadas = []
    for k in range(self.N):
        if k == self.b:
           mensagens recuperadas.append(None)
            s k = self.secrets[k]
            a_dot_s = sum(a[j] * s_k[j] for j in range(lambda_security))
            bits_recuperados = [(c[k][i] + a_dot_s) % 2 for i in range(len(c[k]))]
            msg bytes = bits to bytes(bits recuperados)
            mensagens_recuperadas.append(msg_bytes)
    return mensagens recuperadas
def recuperar mensagens maioritarias(self, lista criptogramas):
    t = len(lista criptogramas)
    resultados_por_k = [[] for _ in range(self.N)]
    for i in range(t):
        a, c = lista_criptogramas[i]
        mks = self.recuperar mensagens(a, c)
        for k in range(self.\overline{N}):
            resultados_por_k[k].append(mks[k])
    mensagens finais = []
    for k in range(self.N):
        if k == self.b:
            mensagens_finais.append(None)
        else:
```

```
# Encontra a mensagem mais frequente (votação majoritária)
             contagem = \{\}
             for msg in resultados por k[k]:
                 contagem[msg] = contagem.get(msg, 0) + 1
             mensagem_mais_votada = max(contagem.items(), key=lambda x: x[1])[0]
             mensagens finais.append(mensagem mais votada)
    return mensagens_finais
def print info(self):
    print("self.alpha: ",self.alpha)
    print("self.l: ",self.l)
    print("self.lambda: ",lambda security)
    print("self.eps: ",self.eps)
    print("self.secrets: ",self.secrets)
print("self.criterion: ",self.criterion)
def print_secrets(self):
    print("[")
    for k in range(N):
        if k == self.b:
            print("None")
             print(self.secrets[k])
    print("]")
```

Nota: As classes já possuem todas as operações que são precisas neste ponto mas será explicado devidamente o processo a partir deste ponto.

Por passos iremos definir o Choose(b):

"O sender escolhe o par (a, ℓ) e a função XOF e envia essa informação para o sender; esta informação determina completamente a sequência $\{(a_i, u_i)\}_{i=1}^{\ell}$ que passa a formar o "oblivious criterion" ; ambos os agentes podem construir estes elementos."

In [7]:

```
# Setup
sender = Sender(alpha="alpha123", l=10)
sender.get_criterion_sequence(lambda_security)
#sender.print_info()
receiver = Receiver(eps=0.1)
receiver.receive_alpha_l("alpha123", 10)
#receiver.print_info()

# Verificação: os critérios devem bater
if sender.criterion == receiver.criterion:
    print("Critérios coincidem")
else:
    print("Critérios não coincidem")
```

Critérios coincidem

o receiver gera N segredos $s_k \leftarrow \mathcal{B}^{\lambda}$, se $k \neq b$, e $s_k \leftarrow \bot$

In [8]:

```
receiver.generate_N_secrets()
#print("Segredos do receiver:")
#receiver.print_secrets()
```

```
0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0,
0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0]
0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,
0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0]
, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0]
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
0, 0,
s 20 = [0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0
0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

```
, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0
0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0,
0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0
0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,
s 37 = [0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0]
s 40 = [0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0
0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0,
```

```
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]
s 48 = [0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
 0, 0,
0, 0, 0, 0,
  1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0]
0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0
0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0
0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1,
s 62 = [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0,
0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0]
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0]
```

```
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0
1, 0, 0, 0,
0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0
, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1,
```

0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0 $0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0$ 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0 $0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0$, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, s 98 = [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, , 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, $0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0]$

Para todo $k \in [N]$ e todo $i \in [\ell]$, calcula $t_{k,i}$ da seguinte forma

$$t_{i,k} \leftarrow \begin{cases} \vartheta \, e_{i,k} \leftarrow \mathcal{B}(\epsilon) \, \cdot \, a_i \cdot \mathbf{s}_k + e_{i,k} & \text{se} \quad k \neq b \\ u_i - \sum_{j \neq b} t_{i,j} & \text{se} \quad k = b \end{cases}$$

Regista esta informação na sua memória. Construímos, para cada $i \in [\ell]$, um vetor em \mathcal{B}^N

$$\mathsf{t}_i \equiv \{t_{i,k} \mid k \in [N]\}$$

e envia-os para o sender como chaves públicas.

In [9]:

receiver.generate pks()

c . o sender recolhe todas os vetores de chaves públicas ti e verifca as igualdades

$$\sum_{k \in [N]} \mathsf{t}_{i,k} = u_i$$

Se, para algum $i \in [\ell]$ a igualdade não se verifica então termina em falha. Se se verificar a igualdade então regista todos os t_i na sua memória para transferência futura.

In [10]:

```
sender.receive and verifypks(receiver.t)
```

Verificação OK: todas as somas coincidem com u i

Out[10]:

True

Operação Transfer $(m_0, m_1, \dots, m_{N-1})$

Por passos:

1. O **sender** conhece as mensagens $m_k \in \mathbb{F}_2$, $k \in [N]$ e, para cada $i \in [\ell]$ as chaves públicas t_i Para as cifrar gera aleatoriamente uma sequências de bits $\{r_i \leftarrow \mathcal{B}\}_{i=0}^{\ell}$ com um peso de Hamming (número de bits 1) limitado a um parâmetro δ , e calcula

$$a \leftarrow \sum_{i} r_{i} \cdot e_{i,k}$$
 , $c_{k} \leftarrow m_{k} + \sum_{i} r_{i} \cdot t_{i,k}$

para todos os $k \in [N]$ O criptograma é o tuplo $\langle a, c_o, \dots, c_{N-1} \rangle$ que é enviado para o **receiver**.

In [11]:

```
#Gerar aletoriamenete a sequência de bits ri
sender.calcular_criptogramas()
print(len(sender.criptogramas))
```

100

1. O receiver conhece os segredos \mathbf{s}_k para todo $k \in [N]$. Sabe que $\mathbf{s}_b = \bot$ e que para todo $k \neq b$ pode calcular $a \cdot \mathbf{s}_k$. Sabe também que se verifica, para todo $k \neq b$, a relação

$$\mbox{sm_k };=\ \mbox{c_k + (a\cdot\mathsf{s}_k) + \mbox{error}_k$$}$$

sendo error $_k = \sum_i r_i \cdot e_{i,k}$ um valor desconhecido (porque o receiver não conhece os r_i) mas com elevada probabilidade de ser nulo.

Procedendo como no protocolo $\binom{2}{1}$ -OT , pode-se reforçar esta probabilidade, iterando ambas as operações t vezes; para isso cifra-se usando vetores $r_i \in \mathcal{B}^t$. As iterações são independentes e podem ser executadas em paralelo. A sender produz t criptogramas distintos, um por iteração. O receiver toma este conjunto de criptogramas e calcula, para cada um, um resultado

$$m_k \leftarrow c_k + (a \cdot s_k)$$

para todo $k \neq b$ Toma-se como resultado final de m_{κ} , para cada $k \neq b$, o valor em maioria nas diferentes iterações; assim obtém-se, com elevada probabilidade, o valor da mensagem inicial.

Finalmente para mensagens $\{m_k\}_{k\in[N]}$ de comprimento arbitrário, tal como no caso, $\binom{2}{1}$ OT, usa-se o protocolo de mensagens binárias para cada posição nas mensagens.

In [12]:

```
mensagens_recuperadas = receiver.recuperar_mensagens_maioritarias(sender.criptogramas)
```

Verificação se conseguiu decifrar corretamente as mensagens assim como não cifrar corretamente a mensagem de índice b

```
In [13]:
for i in range(0,len(sender.mensagens)):
    if receiver.b != i:
        if sender.mensagens[i] == mensagens recuperadas[i]:
            print(f"Mensagem de índice {i} bem decifrada")
            print(f"Mensagem de índice {i} mal decifrada")
    else:
        if sender.mensagens[i] != mensagens_recuperadas[i]:
             print(f"A mensagem de índice {i} foi corretamente omitida")
Mensagem de índice 0 bem decifrada
Mensagem de índice 1 bem decifrada
Mensagem de índice 2 bem decifrada
Mensagem de índice 3 bem decifrada
Mensagem de índice 4 bem decifrada
Mensagem de índice 5 bem decifrada
Mensagem de índice 6 bem decifrada
Mensagem de índice 7 bem decifrada
Mensagem de índice 8 bem decifrada
Mensagem de índice 9 bem decifrada
A mensagem de índice 10 foi corretamente omitida
Mensagem de índice 11 bem decifrada
Mensagem de índice 12 bem decifrada
Mensagem de índice 13 bem decifrada
Mensagem de índice 14 bem decifrada
Mensagem de índice 15 bem decifrada
Mensagem de índice 16 bem decifrada
Mensagem de índice 17 bem decifrada
Mensagem de índice 18 bem decifrada
Mensagem de índice 19 bem decifrada
Mensagem de índice 20 bem decifrada
Mensagem de índice 21 bem decifrada
Mensagem de índice 22 bem decifrada
Mensagem de índice 23 bem decifrada
Mensagem de índice 24 bem decifrada
Mensagem de índice 25 bem decifrada
Mensagem de índice 26 bem decifrada
Mensagem de índice 27 bem decifrada
Mensagem de índice 28 bem decifrada
Mensagem de índice 29 bem decifrada
Mensagem de índice 30 bem decifrada
Mensagem de índice 31 bem decifrada
Mensagem de índice 32 bem decifrada
Mensagem de índice 33 bem decifrada
Mensagem de índice 34 bem decifrada
Mensagem de índice 35 bem decifrada
Mensagem de índice 36 bem decifrada
Mensagem de índice 37 bem decifrada
Mensagem de índice 38 bem decifrada
Mensagem de índice 39 bem decifrada
Mensagem de índice 40 bem decifrada
Mensagem de índice 41 bem decifrada
Mensagem de índice 42 bem decifrada
Mensagem de índice 43 bem decifrada
Mensagem de índice 44 bem decifrada
Mensagem de índice 45 bem decifrada
Mensagem de índice 46 bem decifrada
Mensagem de índice 47 bem decifrada
Mensagem de índice 48 bem decifrada
Mensagem de índice 49 bem decifrada
Mensagem de índice 50 bem decifrada
Mensagem de índice 51 bem decifrada
Mensagem de índice 52 bem decifrada
Mensagem de índice 53 bem decifrada
Mensagem de índice 54 bem decifrada
Mensagem de índice 55 bem decifrada
Mensagem de índice 56 bem decifrada
```

Mensagem de índice 57 bem decifrada Mensagem de índice 58 bem decifrada Mensagem de índice 59 bem decifrada Mensagem de índice 60 bem decifrada Mensagem de índice 61 bem decifrada Mensagem de índice 62 bem decifrada Mensagem de índice 63 bem decifrada Mensagem de índice 64 bem decifrada Mensagem de índice 65 bem decifrada Mensagem de índice 66 bem decifrada Mensagem de índice 67 bem decifrada Mensagem de índice 68 bem decifrada Mensagem de índice 68 bem decifrada Mensagem de índice 69 bem decifrada Mensagem de índice 69 bem decifrada Mensagem de índice 70 bem decifrada

```
Mensagem de índice 71 bem decifrada
Mensagem de índice 72 bem decifrada
Mensagem de índice 73 bem decifrada
Mensagem de índice 74 bem decifrada
Mensagem de índice 75 bem decifrada
Mensagem de índice 76 bem decifrada
Mensagem de índice 77 bem decifrada
Mensagem de índice 78 bem decifrada
Mensagem de índice 79 bem decifrada
Mensagem de índice 80 bem decifrada
Mensagem de índice 81 bem decifrada
Mensagem de índice 82 bem decifrada
Mensagem de índice 83 bem decifrada
Mensagem de índice 84 bem decifrada
Mensagem de índice 85 bem decifrada
Mensagem de índice 86 bem decifrada
Mensagem de índice 87 bem decifrada
Mensagem de índice 88 bem decifrada
Mensagem de índice 89 bem decifrada
Mensagem de índice 90 bem decifrada
Mensagem de índice 91 bem decifrada
Mensagem de índice 92 bem decifrada
Mensagem de índice 93 bem decifrada
Mensagem de índice 94 bem decifrada
Mensagem de índice 95 bem decifrada
Mensagem de índice 96 bem decifrada
Mensagem de índice 97 bem decifrada
Mensagem de índice 98 bem decifrada
Mensagem de índice 99 bem decifrada
```

Parte B

b. Codificando os elementos de um corpo primo F_p em "arrays" de "bytes", converta a solução anterior num protocolo $\binom{N}{N-1}$ -OT em que as mensagens são vetores F_p^ℓ .

```
In [14]:
```

```
p = 257  # Exemplo: primo de 8 bits
l = 10  # Tamanho do vetor F_p^{\ell}
lambda_security = 128
F = GF(p)
```

Definimos as funções auxiliares:

```
In [15]:
```

```
def vector_to_bytes(vector, p):
    """Converte um vetor F_p^ℓ em bytes."""
    byte_array = bytearray()
    for elemento in vector:
        # Assume que elemento está em {0, ..., p-1}
        byte_array.append(elemento % 256) # 1 byte por elemento (se p ≤ 256)
    return bytes(byte_array)

def bytes_to_vector(byte_string, p, l):
    """Converte bytes de volta para F_p^ℓ."""
    vector = []
    for byte in byte_string[:l]:
        vector.append(byte % p)
    return vector
```

E as novas classes que irão suportar arrays de bytes:

In [16]:

```
class Sender:
         __init__(self, alpha, l, xof_name="shake128",n_mensagens=100):
        self.alpha = alpha
        self.l = l
         self.xof_name = xof_name
        self.seed = f"{alpha}:{l}".encode() # usa <math>\alpha e \ell como seed
        self.criterion = None
        self.pks = []
        self.N = n mensagens
        self.mensagens = self.gerar mensagens()
        self.r = []
        self.criptogramas = []
        self.p = 257
        self.t = 50 #Número de criptogramas a serem feitos para enviar ao Receiver
    def gerar_mensagens(self):
         \textbf{return} \ [\textbf{b''.join}(((\textbf{i} + \textbf{j}) \% \textbf{p}).\textbf{to\_bytes}(2, \textbf{byteorder='little'}) \ \textbf{for} \ \textbf{j} \ \textbf{in} \ \texttt{range}(\textbf{l})) \textbf{for} \ \textbf{i} \ \textbf{in} \ \texttt{range}(\textbf{self.N})]
    def get_vector_ai_ui(self, i, lambda_):
          ""Retorna (a_i, u_i) \in F_2^\lambda \times F_2, para índice i"""
        # gera (\lambda + 1) bits para cada i
        seed i = self.seed + f":{i}".encode()
        bits = xof_bits(seed_i, lambda_ + 1)
        a i = bits[:lambda_]
        u i = bits[lambda ] # bit extra
        return a_i, u_i
    def get criterion sequence(self, lambda ):
          ""Gera todos os pares (a i, u i) com base na XOF"""
        self.criterion = [self.get_vector_ai_ui(i, lambda_) for i in range(1, self.l + 1)]
    def receive_and_verifypks(self, pks):
         self.pks = pks
        for i in range(self.l):
             soma = sum(pks[i][k] for k in range(self.N)) % 2
               u i = self.criterion[i] # a i não é necessário aqui
             if soma != u_i:
                 print(f"FALHA na linha i={i}: soma={soma}, u i={u i}")
                 return False
        print("Verificação OK: todas as somas coincidem com u_i")
        return True
    def gerar_r(self, delta, p=0.1):
        while True:
             r = [bernoulli(p) for _ in range(self.l)]
             if sum(r) <= delta:</pre>
                 self.r = r
                 return
    def calcular_criptogramas(self):
        for _ in range(self.t):
             self.gerar_r(128)
             a = [0] * lambda_security # Agora em F_p
             for i in range(self.l):
                 if self.r[i] == 1:
                            = self.criterion[i]
                      аi,
                      a = [(a[j] + a i[j]) % self.p for j in range(lambda security)]
             criptogramas k = []
             for k in range(self.N):
                 msg\_vector = self.mensagens[k] # msg\_vector \'e um vetor em F\_p^{\ell}
                 c k = []
                 for elemento in msg_vector:
                      soma = sum(self.r[i] * self.pks[i][k] for i in range(self.l)) % self.p
                      c k.append((elemento + soma) % self.p)
                 criptogramas k.append(c k)
             self.criptogramas.append((a, criptogramas_k))
    def print info(self):
        print("self.alpha: ",self.alpha)
        print("self.l: ",self.l)
print("self.xof_name: ",self.xof_name)
        print("self.seed: ",self.seed)
        print("self.criterion: ",self.criterion)
```

In [17]:

```
class Receiver:
    def __init__(self, eps, lambda_=128,n_mensagens=100):
        self.alpha = None
        self.l = None
```

```
selt.eps = eps
        self.secrets = []
        self.criterion = None
        self.N = n mensagens
        self.t = None
        self.b = 9 # Não quero a décima mensagem do Sender
        self.p = 257
   def receive_alpha_l(self, alpha, l):
        self.alpha = alpha
        self.l = l
        self.seed = f"{alpha}:{l}".encode()
        self.criterion = self.get criterion sequence(lambda security)
   def get_vector_ai_ui(self, i, lambda_):
    seed_i = self.seed + f":{i}".encode()
        bits = xof_bits(seed_i, lambda_ + 1)
        a i = bits[:lambda ]
        u_i = bits[lambda_]
        return a i, u i
   def get criterion sequence(self, lambda ):
        return [self.get_vector_ai_ui(i, lambda_) for i in range(1, self.l + 1)]
   def generate_N_secrets(self):
        self.secrets = []
        for k in range(self.N):
            if k == self.b:
                self.secrets.append(None) # s b = 1
                s_k = bernoulli_lambda(self.eps, lambda security)
                print(f"s {k} = {s k}"
                self.secrets.append(s k)
   def generate_pks(self):
        # Inicializar t[i][k]
        self.t = [[0 for _ in range(self.N)] for _ in range(self.l)]
        for i in range(self.l):
            a_i, u_i = self.criterion[i]
            soma = 0
            for k in range(self.N):
                if k != self.b:
                    s k = self.secrets[k] # vetor em F_2^{\lambda}
                    dot = sum([a_i[j] * s_k[j] for j in range(lambda_security)]) % 2 # produto escalar mod 2
                    e = bernoulli(self.eps) # bit de erro
                    t_i = (dot + e) % 2
                    self.t[i][k] = t_ik
                    soma = (soma + t_ik) % 2
                else:
                    self.t[i][k] = None # inicializa como None por agora
            # Calcula t {i,b} como complemento para somar a u i
            self.t[i][self.b] = (u_i - soma) % 2
   def recuperar_mensagens(self, a, c):
        mensagens recuperadas = []
        for k in range(self.N):
            if k == self.b:
                mensagens recuperadas.append(None)
                s k = self.secrets[k] # s k é um vetor em F p^{\lambda}
                a_dot_s = sum(a[j] * s_k[j] for j in range(lambda_security)) % self.p
                msg_recuperada = [(c[k][i] + a_dot_s) % self.p for i in range(len(c[k]))]
                mensagens_recuperadas.append(msg_recuperada)
        return mensagens_recuperadas
   def recuperar_mensagens_maioritarias(self, lista criptogramas):
        t = len(lista_criptogramas)
        resultados_por_k = [[] for _ in range(self.N)]
        for i in range(t):
            a, c = lista criptogramas[i]
            mks = self.recuperar mensagens(a, c)
            for k in range(self.N):
                resultados por k[k].append(tuple(mks[k]) if mks[k] is not None else None) # Convertemos para tup
1a
        mensagens_finais = []
        for k in range(self.N):
            if k == self.b:
                mensagens finais.append(None)
            else:
                contagem = {}
```

```
for msg in resultados_por_k[k]:
                        if msg is not None:
                            # Usamos tupla como chave (hashable)
                            msq key = msq
                            contagem[msg_key] = contagem.get(msg_key, 0) + 1
                   # Obtém a mensagem mais frequente
                   \texttt{mensagem\_mais\_votada} = \texttt{max}(\texttt{contagem.items()}, \texttt{ key=lambda} \ x: \ x[1])[\theta] \ \textbf{if} \ \texttt{contagem} \ \textbf{else} \ \textbf{None}
                   mensagens finais.append(bytes(mensagem mais votada) if mensagem mais votada else None) # Converte
mos de vikta para bytes
         return mensagens finais
    def print info(self):
         print("self.alpha: ",self.alpha)
         print("self.l: ",self.l)
         print("self.lambda: ",lambda security)
         print("self.eps: ",self.eps)
         print("self.secrets: ",self.secrets)
print("self.criterion: ",self.criterion)
    def print_secrets(self):
         print("[")
         for k in range(N):
              if k == self.b:
                  print("None")
              else:
                   print(self.secrets[k])
         print("]")
```

In [18]:

```
sender = Sender(alpha="alpha123", l=10)
sender.get_criterion_sequence(lambda_security)
receiver = Receiver(eps=0.1)
receiver.receive_alpha_l("alpha123", 10)
```

In [19]:

```
receiver.generate_N_secrets()
receiver.generate_pks()
sender.receive_and_verifypks(receiver.t)
sender.calcular_criptogramas()
mensagens_decodificadas = receiver.recuperar_mensagens_maioritarias(sender.criptogramas)
```

 0^- , 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0 , 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, , 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, $s_4 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0]$ 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 00, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0] 0^- , 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]

```
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0,
, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0]
, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0
0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0]
0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

```
0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0]
0^-, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0
0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1
0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
s 45 = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0,
1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1]
0^-, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1]
0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0
0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0
```

```
0, 0, 0, 0, 0, 0, 0, 0,
         , 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,
1, 1, 0, 0, 0, 0, 0, 0,
         1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0,
s 61 = [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0]
0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0,
0, 1,
  0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0]
1, 0, 0, 0,
0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0]
0, 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1
0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0]
s_72 = [1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1,
```

```
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
0, 0,
0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0]
1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0]
\overline{\phantom{a}}, 0, 1, \overline{\phantom{a}}, \overline{\phantom
0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0]
0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0
 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0]
0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0,
s 88 = [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0
0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0]
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0
```

0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0 $0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1$ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, Verificação OK: todas as somas coincidem com u i

In [20]:

```
for i in range(0,len(sender.mensagens)):
    print(f"{sender.mensagens[i]} // {mensagens_recuperadas[i]}")
```

```
b'\x00\x00\x01\x00\x02\x00\x03\x00\x04\x00\x05\x00\x06\x00\x07\x00\x08\x00\t\x00' // b'msq000'
b'\x01\x00\x02\x00\x03\x00\x04\x00\x05\x00\x06\x00\x07\x00\x08\x00\t\x00\n\x00' // b'msg001'
b'\x02\x00\x03\x00\x04\x00\x05\x00\x06\x00\x07\x00\x08\x00\t\x00\n\x00\x0b\x00' // b'msq002'
b'\x03\x00\x04\x00\x05\x00\x06\x00\x07\x00\x08\x00\t\x00\n\x00\x0b\x00\x0c\x00' // b'msg003'
b'\x04\x00\x05\x00\x06\x00\x06\x00\x08\x00\t\x00\n\x00\x06\x00\x06\x00\r\x00' // b'msg004' b'\x05\x00\x06\x00\x08\x00\t\x00\n\x00\x06\x00\x06\x00' // b'msg005' b'\x06\x00\x07\x00\x08\x00\t\x00\n\x00\x06\x00\x06\x00\x06\x00' // b'msg006'
b'\x07\x00\x08\x00\t\x00\n\x00\x0b\x00\x0c\x00\r\x00\x0e\x00\x0f\x00\x10\x00' // b'msg007'
b'\n\x00\x0b\x00\x0c\x00\r\x00\x0e\x00\x0f\x00\x11\x00\x12\x00\x13\x00' // None
b'\x0b\x00\x0c\x00\r\x00\x0e\x00\x0f\x00\x11\x00\x12\x00\x13\x00\x14\x00' // b'msg011'
b'\x0c\x00\r\x00\x0e\x00\x0f\x00\x10\x00\x11\x00\x12\x00\x13\x00\x14\x00\x15\x00' // b'msg012'b'\r\x00\x0e\x00\x0f\x00\x11\x00\x12\x00\x13\x00\x15\x00' // b'msg013'
b'\x0e\x00\x10\x00\x11\x00\x12\x00\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00' // b'msq014'
b' \times 0f \times 00 \times 10 \times 00 \times 11 \times 00 \times 12 \times 00 \times 13 \times 00 \times 14 \times 00 \times 15 \times 00 \times 17 \times 00 \times 18 \times 00' \text{ } f \text{ } b' \text{ } msg015' \text{ } b' \text{ } msg015' \text{ } b' \text{ } msg015' \text{ } f \text{ } b' \text{ } msg015' \text{ } b' \text{ } msg015' \text{ } b' \text{ } msg015' \text{ } f \text{ } msg015'' \text{ } msg015''
b'\x10\x00\x11\x00\x12\x00\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00\x18\x00\x19\x00' // b'msg016' b'\x11\x00\x12\x00\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00\x18\x00\x19\x00' // b'msg017' b'\x12\x00\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00\x18\x00\x19\x00\x1a\x00' // b'msg018'
b'\x13\x00\x14\x00\x15\x00\x16\x00\x17\x00\x18\x00\x19\x00\x1a\x00\x1b\x00\x1c\x00' // b'msq019'
 b' \times 14 \times 00 \times 15 \times 00 \times 16 \times 00 \times 17 \times 00 \times 18 \times 00 \times 19 \times 00 \times 1a \times 00 \times 1b \times 00 \times 1c \times 00 \times 1d \times 00' \ // \ b' \times 15 \times 00 \times 16 \times 00 \times 17 \times 00 \times 18 \times 00 \times 1a \times 00 \times 1b \times 00 \times 1c \times 00 \times 1d \times 00' \ // \ b' \ msg 021' \
b'\x19\x00\x1a\x00\x1b\x00\x1c\x00\x1d\x00\x1e\x00\x1f\x00\x00!\x00"\x00' // b'msg025
b'\x1b\x00\x1c\x00\x1d\x00\x1e\x00\x1f\x00\x00!\x00"\x00\#\x00$\x00' // b'\msg027
b'\x1c\x00\x1d\x00\x1e\x00\x1f\x00\x00!\x00"\x00#\x00$\x00$\x00' // b'msq028
b'\x1d\x00\x1e\x00\x1f\x00 \x00!\x00"\x00#\x00$\x00$\x00$\x00' // b'msg029
b'\x1e\x00\x1f\x00 \x00!\x00!\x00#\x00$\x00$\x00&\x00\'\x00' // b'msq030'
b'\x1f\x00 \x00!\x00"\x00#\x00$\x00%\x00&\x00\'\x00(\x00' // b'msg031
b'\x00!\x00"\x00#\x00$\x00%\x00&\x00\'\x00(\x00)\x00' // b'msg032'b'!\x00"\x00#\x00$\x00%\x00\'\x00(\x00)\x00*\x00' // b'msg033'
b'"\x00#\x00$\x00$\x00&\x00\'\x00(\x00)\x00*\x00+\x00' // b'msg034'
b"#\x00$\x00%\x00\x00'\x00(\x00)\x00*\x00+\x00,\x00" // b'msg035'
 b"$\times 00\%\times 006\times 00'\times 00(\times 00)\times 00*\times 00+\times 00, \times 00-\times 00" // b"msg036' b"\%\times 006\times 00'\times 00(\times 00)\times 00*\times 00, \times 00-\times 00. \times 00'' // b'msg037' 
b"&\x00'\x00(\x00)\x00*\x00+\x00,\x00-\x00.\x00/\x00" // b'msg038'
b"'\x00(\x00)\x00*\x00+\x00,\x00.\x00\x000\x00" // b'msg039' b'(\x00)\x00*\x00+\x00,\x00-\x00.\x00/\x000\x00' // b'msg040' b')\x00*\x00+\x00,\x00-\x00/\x000\x001\x00' // b'msg041'
b'*\x00+\x00,\x00-\x00.\x00/\x000\x001\x002\x003\x00' // b'msg042'
b'+\x00,\x00-\x00\x000\x001\x002\x003\x004\x00' // b'msg043'
b',\x00-\x00.\x00/\x000\x001\x002\x003\x004\x005\x00' // b'msg044'
b'-\x00.\x00/\x000\x001\x002\x003\x004\x005\x00' // b'msg045'
b'.\x00/\x000\x001\x002\x003\x004\x005\x006\x007\x00' // b'msg046'
b'/\x000\x001\x002\x003\x004\x005\x006\x007\x008\x00' // b'msg047'b'0\x001\x002\x003\x004\x005\x006\x007\x008\x009\x00' // b'msg048'
b'1\x002\x003\x004\x005\x006\x007\x008\x009\x00:\x00' // b'msq049'
```

```
b'4\x005\x006\x007\x008\x009\x00:\x00;\x00<\x00=\x00' // b'msg052'
b'5\x006\x007\x008\x009\x00:\x00;\x00<\x00=\x00' // b'msg053'
b'6\x007\x008\x009\x00:\x00;\x00<\x00=\x00?\x00?\x00' // b'msq054'
b'7\x008\x009\x00:\x00;\x00<\x00=\x00?\x00@\x00' // b'msg055'
b'8\x009\x00:\x00;\x00<\x00=\x00>\x00?\x00@\x00A\x00' // b'msg056'
b'9\x00:\x00;\x00<\x00=\x00>\x00?\x00@\x00A\x00B\x00' // b'msg057'
b':\x00;\x00<\x00=\x00>\x00?\x00@\x00A\x00B\x00C\x00' // b'msg058'
b';\x00<\x00=\x00>\x00?\x00@\x00A\x00B\x00C\x00D\x00' // b'msg059'
b'<\x00=\x00>\x00@\x00@\x00A\x00B\x00C\x00D\x00E\x00' // b'msg060'
b'=\x00>\x00@\x00@\x00A\x00B\x00C\x00D\x00F\x00' // b'msg061'
b'>\x00?\x00@\x00A\x00B\x00C\x00D\x00E\x00F\x00G\x00' // b'msq062'
b'?\x00@\x00A\x00B\x00C\x00D\x00E\x00F\x00G\x00H\x00' // b'msg063'
b'@\x00A\x00B\x00C\x00D\x00E\x00F\x00G\x00H\x00I\x00' // b'msg064'
b'A\x00B\x00C\x00D\x00E\x00F\x00G\x00H\x00I\x00J\x00' // b'msg065'
b'B\x00C\x00D\x00E\x00F\x00G\x00H\x00I\x00J\x00K\x00' // b'msq066'
b'C\x00D\x00E\x00F\x00G\x00H\x00I\x00J\x00K\x00L\x00' // b'msg067'
b'D\x00E\x00F\x00G\x00H\x00I\x00J\x00K\x00L\x00M\x00' // b'msg068'
b'E\x00F\x00G\x00H\x00I\x00J\x00K\x00H\x00N\x00' // b'msg069'
b'F\x00G\x00H\x00I\x00J\x00K\x00L\x00M\x00N\x000\x00' // b'msg070'
b'G\x00H\x00I\x00J\x00K\x00L\x00M\x00N\x00O\x00P\x00' // b'msg071'
b'H\x00I\x00J\x00K\x00L\x00M\x00N\x00O\x00P\x00' // b'msg072'
b'I\x00J\x00K\x00L\x00M\x00N\x00O\x00P\x00Q\x00' // b'msg073'
b'J\x00K\x00L\x00M\x00N\x000\x00P\x00Q\x00R\x00S\x00' // b'msg074'
b'K\x00L\x00M\x00N\x000\x00P\x00Q\x00R\x00S\x00T\x00' // b'msg075' b'L\x00M\x00N\x000\x00P\x00Q\x00R\x00S\x00T\x00U\x00' // b'msg076'
b'M\x00N\x000\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00' // b'msg077'
b'N\x000\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00' // b'msg078'
b'0\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00X\x00' // b'msg079' b'P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00Y\x00' // b'msg080' b'Q\x00R\x00S\x00T\x00U\x00W\x00X\x00Y\x00Z\x00' // b'msg081'
b'R\x00S\x00T\x00U\x00V\x00W\x00X\x00Y\x00Z\x00[\x00' // b'msg082'
b'S\x00T\x00U\x00V\x00W\x00X\x00Y\x00Z\x00[\x00\\\x00' // b'msg083'
b'T\x00U\x00V\x00W\x00X\x00Y\x00Z\x00[\x00\\\x00]\x00'
                                                                  // b'msg084'
b'U\x00V\x00W\x00X\x00Y\x00Z\x00[\x00\\\x00]\x00^\x00' // b'msg085
b'V\x00W\x00X\x00Y\x00Z\x00[\x00\\\x00]\x00^\x00 \x00' // b'msg086'
b'W\x00X\x00Y\x00Z\x00[\x00\\x00]\x00^\x00_\x00`\x00' // b'msg087
b'X\x00Y\x00Z\x00[\x00\\\x00]\x00^\x00_\x00\\x00a\x00' // b'msg088'
b'Y\x00Z\x00[\x00\\x00]\x00^\x00`\x00a\x00b\x00' // b'msg089'
b'Z\x00[\x00\\\x00]\x00^\x00_\x00\\x00b\x00c\x00' // b'msg090'
 b'[\x00\\x00^\x00^\x00a\x00b\x00c\x00d\x00' // b'msg091'b'\\x00]\x00^\x00a\x00b\x00c\x00d\x00e\x00' // b'msg092' 
b']\x00^\x00\x00\\x00a\x00b\x00c\x00d\x00e\x00f\x00' // b'msq093'
b'^\x00 \x00\\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00' // b'msg094'
  _\x00`\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00h\x00' // b'msg095'
`\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00h\x00i\x00' // b'msg096'
b'a\x00b\x00c\x00d\x00e\x00f\x00q\x00h\x00i\x00j\x00' // b'msq097'
b'b\x00c\x00d\x00e\x00f\x00g\x00h\x00i\x00j\x00k\x00' // b'msg098'
b'c\x00d\x00e\x00f\x00g\x00h\x00i\x00j\x00k\x00l\x00' // b'msg099'
In [21]:
for i in range(0,len(sender.mensagens)):
     if receiver.b != i:
          if sender.mensagens[i] == mensagens decodificadas[i]:
              print(f"Mensagem de índice {i} bem decifrada")
              print(f"Mensagem de índice {i} mal decifrada")
     else:
          if sender.mensagens[i] != mensagens decodificadas[i]:
              print(f"A mensagem de índice {i} foi corretamente omitida")
Mensagem de índice 0 bem decifrada
Mensagem de índice 1 bem decifrada
Mensagem de índice 2 bem decifrada
Mensagem de índice 3 bem decifrada
Mensagem de índice 4 bem decifrada
Mensagem de índice 5 bem decifrada
Mensagem de índice 6 bem decifrada
Mensagem de índice 7 bem decifrada
Mensagem de índice 8 bem decifrada
A mensagem de índice 9 foi corretamente omitida
Mensagem de índice 10 bem decifrada
Mensagem de índice 11 bem decifrada
Mensagem de índice 12 bem decifrada
Mensagem de índice 13 bem decifrada
Mensagem de índice 14 bem decifrada
```

b'2\x003\x004\x005\x006\x007\x008\x009\x00:\x00;\x00' // b'msg050' b'3\x004\x005\x006\x007\x008\x009\x00:\x00;\x00' // b'msg051'

Mensagem de índice 15 bem decifrada Mensagem de índice 16 bem decifrada Mensagem de índice 17 bem decifrada Mensagem de índice 18 bem decifrada Mensagem de índice 19 bem decifrada

```
Mensagem de índice 20 bem decifrada
Mensagem de índice 21 bem decifrada
Mensagem de índice 22 bem decifrada
Mensagem de índice 23 bem decifrada
Mensagem de índice 24 bem decifrada
Mensagem de índice 25 bem decifrada
Mensagem de índice 26 bem decifrada
Mensagem de índice 27 bem decifrada
Mensagem de índice 28 bem decifrada
Mensagem de índice 29 bem decifrada
Mensagem de índice 30 bem decifrada
Mensagem de índice 31 bem decifrada
Mensagem de índice 32 bem decifrada
Mensagem de índice 33 bem decifrada
Mensagem de índice 34 bem decifrada
Mensagem de índice 35 bem decifrada
Mensagem de índice 36 bem decifrada
Mensagem de índice 37 bem decifrada
Mensagem de índice 38 bem decifrada
Mensagem de índice 39 bem decifrada
Mensagem de índice 40 bem decifrada
Mensagem de índice 41 bem decifrada
Mensagem de índice 42 bem decifrada
Mensagem de índice 43 bem decifrada
Mensagem de índice 44 bem decifrada
Mensagem de índice 45 bem decifrada
Mensagem de índice 46 bem decifrada
Mensagem de índice 47 bem decifrada
Mensagem de índice 48 bem decifrada
Mensagem de índice 49 bem decifrada
Mensagem de índice 50 bem decifrada
Mensagem de índice 51 bem decifrada
Mensagem de índice 52 bem decifrada
Mensagem de índice 53 bem decifrada
Mensagem de índice 54 bem decifrada
Mensagem de índice 55 bem decifrada
Mensagem de índice 56 bem decifrada
Mensagem de índice 57 bem decifrada
Mensagem de índice 58 bem decifrada
Mensagem de índice 59 bem decifrada
Mensagem de índice 60 bem decifrada
Mensagem de índice 61 bem decifrada
Mensagem de índice 62 bem decifrada
Mensagem de índice 63 bem decifrada
Mensagem de índice 64 bem decifrada
Mensagem de índice 65 bem decifrada
Mensagem de índice 66 bem decifrada
Mensagem de índice 67 bem decifrada
Mensagem de índice 68 bem decifrada
Mensagem de índice 69 bem decifrada
Mensagem de índice 70 bem decifrada
Mensagem de índice 71 bem decifrada
Mensagem de índice 72 bem decifrada
Mensagem de índice 73 bem decifrada
Mensagem de índice 74 bem decifrada
Mensagem de índice 75 bem decifrada
Mensagem de índice 76 bem decifrada
Mensagem de índice 77 bem decifrada
Mensagem de índice 78 bem decifrada
Mensagem de índice 79 bem decifrada
Mensagem de índice 80 bem decifrada
Mensagem de índice 81 bem decifrada
Mensagem de índice 82 bem decifrada
Mensagem de índice 83 bem decifrada
Mensagem de índice 84 bem decifrada
Mensagem de índice 85 bem decifrada
Mensagem de índice 86 bem decifrada
Mensagem de índice 87 bem decifrada
Mensagem de índice 88 bem decifrada
Mensagem de índice 89 bem decifrada
Mensagem de índice 90 bem decifrada
Mensagem de índice 91 bem decifrada
Mensagem de índice 92 bem decifrada
Mensagem de índice 93 bem decifrada
Mensagem de índice 94 bem decifrada
Mensagem de índice 95 bem decifrada
Mensagem de índice 96 bem decifrada
Mensagem de índice 97 bem decifrada
Mensagem de índice 98 bem decifrada
Mensagem de índice 99 bem decifrada
```