

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 \mathbb{F}_p em “arrays” de “bytes”, converta a solução anterior num protocolo $\binom{N}{N-1}$ -OT em que as mensagens são vetores \mathbb{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 e segue uma distribuição Bernoulli com parâmetro ϵ , ou seja:

$$e_i \sim \text{Bernoulli}(\epsilon)$$

Isso significa que cada bit e_i tem probabilidade ϵ de ser 1 (ruído) e $1 - \epsilon$ 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.

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

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 $[0, 1]$.

```
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))
```

Learning Party with Noise

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

```
def LPN_generator(lambda_, epsilon,s):
    """Gera um par (a, t) segundo o protocolo LPN."""

    # Vetor gerado a partir do gerador de Bernoulli
    a = bernoulli_lambda(epsilon)

    # Erro e seguindo uma distribuição de Bernoulli B(epsilon)
    e = bernoulli(epsilon)
    t = 0

    # 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 Bernoulli
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 >> (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 i in range(0, len(bits), 8):
        byte = 0
        for j in range(8):
            if i + j < len(bits):
                byte |= bits[i + j] << j
        byte_array.append(byte)
    return bytes(byte_array)
```

E definindo as classes Sender e Receiver :

Classe Sender

In [5]:

```
class Sender:
    def __init__(self, alpha, l, xof_name="shake128"):
        self.alpha = alpha
        self.l = l
        self.xof_name = xof_name
        self.seed = f"{alpha}:{l}".encode() # usa  $\alpha$  e  $l$  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_bytes = 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  $(a_i, u_i) \in F_2^{\lambda} \times F_2$ , 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_):
        self.criterion = [self.get_vector_ai_ui(i, lambda_) for i in range(1, self.l + 1)]

    def receive_and_verify_pks(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:
                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:
                    a_i, _ = 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 = 1
        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(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]
                dot = sum([a_i[j] * s_k[j] for j in range(lambda_security)]) % 2
                e = bernoulli(self.eps)
                t_ik = (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)
        else:
            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.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:

```

```

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

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)

print_secrets(self):
print("[")
for k in range(N):
    if k == self.b:
        print("None")
    else:
        print(self.secrets[k])
print("]")

```

Por passos iremos definir o Choose(b):

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

In [8]:

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

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
receiver.generate_pks()
```

c . o sender recolhe todas os vetores de chaves públicas t_i e verifica as igualdades

$$\sum_{k \in [N]} t_{i,k} = u_i$$

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

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

$$a \leftarrow \sum_i r_i \cdot e_{i,k} \quad , \quad c_k \leftarrow m_k + \sum_i r_i \cdot t_{i,k}$$

para todos os $k \in [N]$ O criptograma é o tuplo $\langle a, c_0, \dots, c_{N-1} \rangle$ que é enviado para o **receiver**.

In [11]:

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

100

1. O receiver conhece os segredos s_k para todo $k \in [N]$. Sabe que $s_b = \perp$ e que para todo $k \neq b$ pode calcular $a \cdot s_k$. Sabe também que se verifica, para todo $k \neq b$, a relação

$$m_k = c_k + (a \cdot s_k) + \text{error}_k$$

sendo $\text{error}_k = \sum_i r_i \cdot e_{i,k}$ 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_k , 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")
        else:
            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 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^l
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:
    def __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  $\alpha$  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):
        return [b''.join(((i + j) % p).to_bytes(2, byteorder='little') for j in range(l)) for i in range(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 (l + 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_verify_pks(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:
                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:
                    a_i, _ = self.criterion[i]
                    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 é 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
```

```

self.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
        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(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 F2^λ
                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_ik = (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)
        else:
            s_k = self.secrets[k] # s_k é um vetor em F_p^λ
            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

la

mensagens_finais = []
for k in range(self.N):
    if k == self.b:
        mensagens_finais.append(None)
    else:
        contagem = {}

```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

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

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<\x00' // b'msg051'
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>\x00' // b'msg053'
b'6\x007\x008\x009\x00:\x00;\x00<\x00=\x00>\x00?\x00' // b'msg054'
b'7\x008\x009\x00:\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\x00E\x00F\x00' // b'msg061'
b'>\x00?\x00@\x00A\x00B\x00C\x00D\x00E\x00F\x00G\x00' // b'msg062'
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'msg066'
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\x00L\x00M\x00N\x00' // b'msg069'
b'F\x00G\x00H\x00I\x00J\x00K\x00L\x00M\x00N\x00O\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\x00Q\x00' // b'msg072'
b'I\x00J\x00K\x00L\x00M\x00N\x00O\x00P\x00Q\x00R\x00' // b'msg073'
b'J\x00K\x00L\x00M\x00N\x00O\x00P\x00Q\x00R\x00S\x00' // b'msg074'
b'K\x00L\x00M\x00N\x00O\x00P\x00Q\x00R\x00S\x00T\x00' // b'msg075'
b'L\x00M\x00N\x00O\x00P\x00Q\x00R\x00S\x00T\x00U\x00' // b'msg076'
b'M\x00N\x00O\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00' // b'msg077'
b'N\x00O\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00' // b'msg078'
b'O\x00P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00X\x00' // b'msg079'
b'P\x00Q\x00R\x00S\x00T\x00U\x00V\x00W\x00X\x00Y\x00' // b'msg080'
b'Q\x00R\x00S\x00T\x00U\x00V\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_\x00_\x00a\x00b\x00' // b'msg089'
b'Z\x00[\x00\\\x00]\x00^\x00_\x00_\x00a\x00b\x00c\x00' // b'msg090'
b'[\x00\\\x00]\x00^\x00_\x00_\x00a\x00b\x00c\x00d\x00' // b'msg091'
b'\\\x00]\x00^\x00_\x00_\x00a\x00b\x00c\x00d\x00e\x00' // b'msg092'
b']\x00^\x00_\x00_\x00a\x00b\x00c\x00d\x00e\x00f\x00' // b'msg093'
b'^\x00_\x00_\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00' // b'msg094'
b'_\x00_\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00h\x00' // b'msg095'
b'`\x00a\x00b\x00c\x00d\x00e\x00f\x00g\x00h\x00i\x00' // b'msg096'
b'a\x00b\x00c\x00d\x00e\x00f\x00g\x00h\x00i\x00j\x00' // b'msg097'
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")
        else:
            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
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

[illegible]