

Exercício 2 (BIKE) - Trabalho Prático 3

Grupo 6:

Ruben Silva - pg57900

Luís Costa - pg55970

imports

In [948...

```
import hashlib
import os
from sage.all import GF, PolynomialRing, ceil
import math
```

Paramêtros

Tamanho Polinomial $\rightarrow r = 12323$:

Row weight ($w/2 = 71$) $\rightarrow w = 142$:

Error weight $\rightarrow t = 134$:

Length of m , σ , and K . $\rightarrow \ell = 256$:

In [949...

```
# Parametros
# Tamanho do anel
r = 12323
w = 142      # Row weight
t = 134      # Error weight
ell = 256    # Shared secret size in bits

# Anel  $R = F_2[X] / (X^r - 1)$ 
F2 = GF(2)      # Campo finito com 2 elementos
P = PolynomialRing(F2, 'x') # Anel de polinômios  $F_2[x]$ 
x = P.gen()     # Gerador do anel de polinômios
R = P.quotient(x**r - 1) # Anel quociente  $F_2[x]/(x^r - 1)$ 
```

Funções Auxiliares

poly_to_bytes

1. Converte um polinômio em uma sequência de bytes:

- Garante que os coeficientes tenham o comprimento correto;
- Transforma em uma string de bits e converte em bytes.

In [950...

```
def poly_to_bytes(p, length):
    # Converter o Coeficiente do polinômio para uma string de bits
    coeffs = p.list() + [0] * (length - len(p.list()))
```

```

# Juntar os coeficientes em uma string de bits
bitstr = ''.join(str(int(c)) for c in coeffs)

# Calcular o comprimento necessário em bytes
byte_length = ceil(length / 8)

# Preencher com zeros se necessário
padded_bitstr = bitstr.ljust(byte_length * 8, '0')

# Converter a string de bits em bytes
return bytes(int(padded_bitstr[i:i+8], 2) for i in range(0, len(padded_bitstr)

```

xor_bytes

1. Realiza o XOR entre duas sequências de bytes.

```

In [951... def xor_bytes(a, b):
    return bytes(x ^ y for x, y in zip(a, b))

```

WSHAKE256_PRF

1. Gera posições distintas para polinômios esparsos usando SHAKE256:

- Utiliza hashlib.shake_256 para gerar bytes;
- Converte em inteiros de 32 bits;
- Calcula posições distintas com base na especificação.

```

In [952... def WSHAKE256_PRF(seed, length, wt):

    # Shake256
    shake = hashlib.shake_256()
    shake.update(seed)
    stream_bytes = shake.digest(wt * 4) # wt 32-bit ints

    # Converter o stream de bytes em inteiros
    s = [int.from_bytes(stream_bytes[i*4:(i+1)*4], 'big') for i in range(wt)]
    wlist = []
    present = set()

    # Gerar a lista de posições
    for i in range(wt - 1, -1, -1):
        pos = i + (length - i) * s[i] // 2**32
        if pos not in present and pos < length:
            wlist.append(pos)
            present.add(pos)
        else:
            wlist.append(i)
            present.add(i)
    return wlist

```

sample_polynomial_from_positions

1. Cria um polinômio em \mathcal{R} com coeficientes 1 nas posições indicadas

```

In [953... def sample_polynomial_from_positions(positions, length):
    # Criar um polinômio com coeficientes 0 de comprimento 'length'
    coeffs = [0] * length

```

```
# Definir os coeficientes 1 nas posições especificadas
for pos in positions:
    coeffs[pos] = 1

# Criar o polinômio a partir dos coeficientes
return R(P(coeffs))
```

Hashing Functions

H(m, r, t)

1. Mapeia uma mensagem de 256 bits para dois polinômios (e_0, e_1) com peso total t :

- Usa WSHAKE256_PRF para gerar t posições distintas;
- Distribui as posições entre e_0 e e_1 .

```
In [954... # Hash function H:  $\{0,1\}^{256} \rightarrow E_t$ 
def H(m, r, t):
    positions = WSHAKE256_PRF(m, 2 * r, t)
    e0_coeffs = [0] * r
    e1_coeffs = [0] * r
    for pos in positions:
        if pos < r:
            e0_coeffs[pos] = 1
        else:
            e1_coeffs[pos - r] = 1
    e0 = R(P(e0_coeffs))
    e1 = R(P(e1_coeffs))
    return e0, e1
```

L(e_0, e_1, r)

1. Mapeia dois polinômios para uma string de 256 bits:

- Converte os polinômios em bytes;
- Aplica SHA384 e retorna os primeiros 32 bytes.

```
In [955... def L(e0, e1, r):
    input_bytes = poly_to_bytes(e0, r) + poly_to_bytes(e1, r)
    return hashlib.sha384(input_bytes).digest()[:32] # 256 bits = 32 bytes
```

K(m, c, r)

1. Mapeia a mensagem e o ciphertext para a chave partilhada:

- Concatena m, c_0 (em bytes) e c_1 ;
- Usa SHA384 para gerar 256 bits.

```
In [956... def K(m, c, r):
    c0, c1 = c
    input_bytes = m + poly_to_bytes(c0, r) + c1
    return hashlib.sha384(input_bytes).digest()[:32]
```

BGF (Black-Gray-Flip)

getHammingWeight

1. Calcula o peso de Hamming (número de bits 1) de uma sequência binária de comprimento especificado.

```
In [957... def getHammingWeight(tmp, length):
    return sum(int(tmp[i]) for i in range(length))
```

recompute_syndrome

1. Atualiza o síndrome s após a inversão de um bit na posição pos do vetor de erro, considerando as matrizes de paridade compactadas \mathbf{h}_0 e \mathbf{h}_1 .

```
In [958... def recompute_syndrome(s, pos, h0_compact, h1_compact, r):

    # se pos < r, atualiza o síndrome usando h0_compact
    if pos < r:
        for j in range(len(h0_compact)):
            if h0_compact[j] <= pos:
                s[(pos - h0_compact[j]) % r] ^= 1
            else:
                s[(r - h0_compact[j] + pos) % r] ^= 1

    # se pos >= r, atualiza o síndrome usando h1_compact
    else:
        pos -= r
        for j in range(len(h1_compact)):
            if h1_compact[j] <= pos:
                s[(pos - h1_compact[j]) % r] ^= 1
            else:
                s[(r - h1_compact[j] + pos) % r] ^= 1
```

ctr

1. Calcula o contador de paridade insatisfeita (número de verificações de paridade violadas) para uma coluna específica da matriz de paridade, dado o síndrome.

```
In [959... def ctr(h_compact_col, position, s, r):
    count = 0
    for i in range(len(h_compact_col)):
        index = (h_compact_col[i] + position) % r
        if s[index]:
            count += 1
    return count
```

getCol

1. Converte uma representação compactada de uma linha da matriz de paridade (\mathbf{h}_0 ou \mathbf{h}_1) em uma representação compactada da coluna correspondente.

```
In [960... def getCol(h_compact_row, r):
    h_compact_col = [0] * len(h_compact_row)
```

```

if h_compact_row[0] == 0:
    h_compact_col[0] = 0
    for i in range(1, len(h_compact_row)):
        h_compact_col[i] = r - h_compact_row[len(h_compact_row) - i]
else:
    for i in range(len(h_compact_row)):
        h_compact_col[i] = r - h_compact_row[len(h_compact_row) - 1 - i]
return h_compact_col

```

flipAdjustedErrorPosition

1. Inverte um bit na posição ajustada do vetor de erro, considerando a estrutura do BIKE.

```

In [961... def flipAdjustedErrorPosition(e, position, r):
    adjustedPosition = position
    if position != 0 and position != r:
        adjustedPosition = (position > r) and ((2 * r - position) + r) or (r - p
    e[adjustedPosition] ^= 1

```

BFMaskedIter

1. Executa uma iteração mascarada do algoritmo de decodificação, invertendo bits no vetor de erro com base em uma máscara e um limiar.

```

In [962... def BFMaskedIter(e, s, mask, T, h0_compact, h1_compact, h0_compact_col, h1_compa
    pos = [0] * (2 * r)
    for j in range(r):
        counter = ctr(h0_compact_col, j, s, r)
        if counter >= T and mask[j]:
            flipAdjustedErrorPosition(e, j, r)
            pos[j] = 1
    for j in range(r, 2 * r):
        counter = ctr(h1_compact_col, j - r, s, r)
        if counter >= T and mask[j]:
            flipAdjustedErrorPosition(e, j, r)
            pos[j] = 1
    for j in range(2 * r):
        if pos[j]:
            recompute_syndrome(s, j, h0_compact, h1_compact, r)

```

BFIter

1. Executa uma iteração principal do algoritmo BGF, classificando posições como "black" ou "gray" com base em contadores de paridade e ajustando o vetor de erro.

```

In [963... def BFIter(e, black, gray, s, T, tau, h0_compact, h1_compact, h0_compact_col, h1
    pos = [0] * (2 * r)
    for j in range(r):
        counter = ctr(h0_compact_col, j, s, r)
        if counter >= T:
            flipAdjustedErrorPosition(e, j, r)
            pos[j] = 1
            black[j] = 1
        elif counter >= T - tau:
            gray[j] = 1
    for j in range(r, 2 * r):

```

```

        counter = ctr(h1_compact_col, j - r, s, r)
        if counter >= T:
            flipAdjustedErrorPosition(e, j, r)
            pos[j] = 1
            black[j] = 1
        elif counter >= T - tau:
            gray[j] = 1
    for j in range(2 * r):
        if pos[j]:
            recompute_syndrome(s, j, h0_compact, h1_compact, r)

```

BGF_decoder

1. Implementa o decodificador BGF completo, executando iterações para corrigir erros no vetor de erro com base no síndrome e nas matrizes de paridade.

In [964...

```

def BGF_decoder(e, s, h0_compact, h1_compact, r, w, t, NbIter=5, tau=3):
    e = [0] * (2 * r)
    h0_compact_col = getCol(h0_compact, r)
    h1_compact_col = getCol(h1_compact, r)
    black = [0] * (2 * r)
    gray = [0] * (2 * r)
    for i in range(1, NbIter + 1):
        black = [0] * (2 * r)
        gray = [0] * (2 * r)
        S = getHammingWeight(s, r)
        T = max(math.ceil(0.0069722 * S + 13.530), 36) # Threshold ajustado par
        BFMaskedIter(e, black, gray, s, T, tau, h0_compact, h1_compact, h0_compact_col
        if i == 1:
            T_mask = (w // 2 + 1) // 2 + 1
            BFMaskedIter(e, s, black, T_mask, h0_compact, h1_compact, h0_compact_
            BFMaskedIter(e, s, gray, T_mask, h0_compact, h1_compact, h0_compact_
        if getHammingWeight(s, r) == 0:
            print("Decodificação bem-sucedida!\n")
            return e

    return None # Falha na decodificação

```

BIKE Implementatioon

A função `KeyGen` é responsável por gerar o par de chaves pública e privada:

1. Gerar Componentes da Chave Privada:

- Criar dois polinômios esparsos, \mathbf{h}_0 e \mathbf{h}_1 , no anel \mathcal{R} ;
- Cada polinômio deve ter exatamente $w/2$ coeficientes iguais a 1, onde w é o peso da linha;
- Utilizar uma função pseudoaleatória, como `WShake256-PRF`, com uma semente, para escolher $w/2$ posições distintas para os coeficientes 1 em cada polinômio.

2. Calcular a Chave Pública:

- Calcular $\mathbf{h} = \mathbf{h}_1 \cdot \mathbf{h}_0^{-1}$ em \mathcal{R} .

- Para que \mathbf{h}_0 seja invertível, $w/2$ é definido como um número ímpar, garantindo esta propriedade no anel.

3. Gerar uma String Aleatória:

- Produzir uma string $\sigma \in \{0, 1\}^{256}$ de 256 bits, utilizando um gerador de números aleatórios seguro. Esta string é usada como recurso de reserva no desencapsulamento, caso a decodificação falhe.

In [965...

```
# Key Generation
def KeyGen(r, w):
    seed_h0 = os.urandom(32)
    positions_h0 = WSHAKE256_PRF(seed_h0, r, w // 2)
    h0 = sample_polynomial_from_positions(positions_h0, r)

    seed_h1 = os.urandom(32)
    positions_h1 = WSHAKE256_PRF(seed_h1, r, w // 2)
    h1 = sample_polynomial_from_positions(positions_h1, r)

    h = h1 * h0.inverse_of_unit() # Compute h = h1 * h0^{-1} in R
    sigma = os.urandom(32)

    sk = (h0, h1, sigma) # Private key
    pk = h                # Public key
    return sk, pk
```

A função `Encaps` é responsável por gerar uma chave secreta partilhada e o seu ciphertext utilizando a chave pública.

1. Escolher uma Mensagem Aleatória:

- Gerar uma string aleatória $m \in \{0, 1\}^{256}$ de 256 bits com um gerador seguro.

2. Gerar Vetores de Erro:

- Aplicar uma função hash \mathbf{H} (ex.: SHAKE256) a m para criar os vetores de erro $(\mathbf{e}_0, \mathbf{e}_1)$, com peso total de Hamming t (ex.: $t = 134$ para nível 1).

3. Calcular o Ciphertext:

- $c_0 = \mathbf{e}_0 + \mathbf{e}_1 \cdot \mathbf{h}$ em \mathcal{R} ;
- $c_1 = m \oplus \mathbf{L}(\mathbf{e}_0, \mathbf{e}_1)$, onde \mathbf{L} (ex.: SHA384) mapeia os vetores de erro para uma string de 256 bits;
- O ciphertext é $c = (c_0, c_1)$.

4. Calcular a Chave Secreta:

- $K = \mathbf{K}(m, c)$, onde \mathbf{K} (ex.: SHA384) faz hash de m e c .

In [966...

```
# Encapsulation
def Encaps(pk, r, t):
    h = pk
    m = os.urandom(32) # m ←$ {0,1}^{256}
    e0, e1 = H(m, r, t)
    c0 = e0 + e1 * h
    c1 = xor_bytes(m, L(e0, e1, r))
    c = (c0, c1)
```

```
K_shared = K(m, c, r)
return K_shared, c
```

A função `Decaps` é responsável por recuperar a chave secreta partilhada a partir do ciphertext usando a chave privada.

1. Decodificar o Ciphertext:

- Calcular o síndrome $s = c_0 \cdot \mathbf{h}_0$ em \mathcal{R} .
- Usar um decodificador (BGF) para recuperar os vetores de erro $\mathbf{e}' = (\mathbf{e}'_0, \mathbf{e}'_1)$.

2. Recuperar a Mensagem:

- $m' = c_1 \oplus \mathbf{L}(\mathbf{e}'_0, \mathbf{e}'_1)$, com \mathbf{L} igual à usada em `Encaps`

3. Verificar e Calcular a Chave:

- Verificar se $\mathbf{e}' = \mathbf{H}(m')$ (usando a mesma \mathbf{H} de `Encaps`)
- Se verdadeiro: $K = \mathbf{K}(m', c)$.
- Se falso (falha na decodificação): $K = \mathbf{K}(\sigma, c)$, usando σ como reserva.

In [967...

```
# Decapsulation (with simulated decoder)
def Decaps(sk, c, r, t):
    h0, h1, sigma = sk
    c0, c1 = c

    # Simulate decoder: assume it correctly recovers e0 and e1
    h0 = sk[0] # Primeira parte da chave privada
    c0 = c[0] # Primeira parte do ciphertext
    s = (c0 * h0).list() # Síndrome como lista
    s = [int(coeff) for coeff in s] # Converter para inteiros Python
    h0_list = [int(coeff) for coeff in sk[0].list()]
    h1_list = [int(coeff) for coeff in sk[1].list()]

    dec = BGF_decoder([0] * (2 * r), r * [0], h0_list, h1_list, r, w, t)
    e0_prime = R(P(dec[:r]))
    e1_prime = R(P(dec[r:2 * r]))

    m_prime = xor_bytes(c1, L(e0_prime, e1_prime, r))

    e0_check, e1_check = H(m_prime, r, t)
    c0_prime = e0_check + e1_check * (h1 * h0.inverse_of_unit())
    c1_prime = xor_bytes(m_prime, L(e0_check, e1_check, r))

    if c0 == c0_prime and c1 == c1_prime:
        return K(m_prime, c, r)
    else:
        return K(sigma, c, r)
```

Run

In [968...

```
print("==== BIKE - Key Encapsulation Mechanism ===== \n")
sk, pk = KeyGen(r, w)
print("Chave Gerada com sucesso.")
print("Chave Pública:", pk)
print("Chave Privada:", sk)
```



```
# Encapsulate
K_enc, c = Encaps(pk, r, t)
print("\nEncapsulação completa!")

# Decapsulate
print("\n===== DESCOMPACTANDO =====")
K_dec = Decaps(sk, c, r, t)
```

===== BIKE - Key Encapsulation Mechanism =====

Chave Gerada com sucesso.

Chave Pública: $xbar^{12322} + xbar^{12318} + xbar^{12315} + xbar^{12314} + xbar^{12313} + xbar^{12311} + xbar^{12309} + xbar^{12308} + xbar^{12306} + xbar^{12300} + xbar^{12299} + xbar^{12298} + xbar^{12295} + xbar^{12294} + xbar^{12293} + xbar^{12292} + xbar^{12290} + xbar^{12287} + xbar^{12285} + xbar^{12284} + xbar^{12278} + xbar^{12276} + xbar^{12275} + xbar^{12274} + xbar^{12273} + xbar^{12268} + xbar^{12266} + xbar^{12264} + xbar^{12263} + xbar^{12262} + xbar^{12260} + xbar^{12258} + xbar^{12253} + xbar^{12252} + xbar^{12251} + xbar^{12249} + xbar^{12248} + xbar^{12247} + xbar^{12246} + xbar^{12241} + xbar^{12240} + xbar^{12239} + xbar^{12230} + xbar^{12229} + xbar^{12228} + xbar^{12225} + xbar^{12223} + xbar^{12220} + xbar^{12213} + xbar^{12212} + xbar^{12210} + xbar^{12208} + xbar^{12207} + xbar^{12206} + xbar^{12204} + xbar^{12203} + xbar^{12202} + xbar^{12200} + xbar^{12199} + xbar^{12198} + xbar^{12196} + xbar^{12194} + xbar^{12191} + xbar^{12190} + xbar^{12185} + xbar^{12184} + xbar^{12183} + xbar^{12182} + xbar^{12181} + xbar^{12180} + xbar^{12179} + xbar^{12178} + xbar^{12176} + xbar^{12175} + xbar^{12174} + xbar^{12173} + xbar^{12169} + xbar^{12165} + xbar^{12159} + xbar^{12158} + xbar^{12156} + xbar^{12152} + xbar^{12151} + xbar^{12150} + xbar^{12149} + xbar^{12148} + xbar^{12147} + xbar^{12145} + xbar^{12143} + xbar^{12142} + xbar^{12141} + xbar^{12139} + xbar^{12138} + xbar^{12137} + xbar^{12136} + xbar^{12133} + xbar^{12132} + xbar^{12131} + xbar^{12127} + xbar^{12126} + xbar^{12125} + xbar^{12123} + xbar^{12121} + xbar^{12120} + xbar^{12118} + xbar^{12117} + xbar^{12110} + xbar^{12109} + xbar^{12106} + xbar^{12105} + xbar^{12104} + xbar^{12102} + xbar^{12099} + xbar^{12098} + xbar^{12097} + xbar^{12095} + xbar^{12094} + xbar^{12093} + xbar^{12091} + xbar^{12084} + xbar^{12083} + xbar^{12081} + xbar^{12079} + xbar^{12078} + xbar^{12077} + xbar^{12068} + xbar^{12065} + xbar^{12062} + xbar^{12060} + xbar^{12059} + xbar^{12057} + xbar^{12056} + xbar^{12051} + xbar^{12050} + xbar^{12048} + xbar^{12039} + xbar^{12037} + xbar^{12036} + xbar^{12030} + xbar^{12029} + xbar^{12028} + xbar^{12024} + xbar^{12023} + xbar^{12019} + xbar^{12018} + xbar^{12017} + xbar^{12014} + xbar^{12013} + xbar^{12009} + xbar^{12008} + xbar^{12002} + xbar^{11999} + xbar^{11998} + xbar^{11995} + xbar^{11994} + xbar^{11992} + xbar^{11990} + xbar^{11988} + xbar^{11987} + xbar^{11984} + xbar^{11983} + xbar^{11982} + xbar^{11980} + xbar^{11978} + xbar^{11977} + xbar^{11975} + xbar^{11973} + xbar^{11970} + xbar^{11968} + xbar^{11967} + xbar^{11963} + xbar^{11961} + xbar^{11959} + xbar^{11957} + xbar^{11956} + xbar^{11954} + xbar^{11953} + xbar^{11947} + xbar^{11946} + xbar^{11942} + xbar^{11941} + xbar^{11939} + xbar^{11937} + xbar^{11936} + xbar^{11935} + xbar^{11932} + xbar^{11929} + xbar^{11927} + xbar^{11926} + xbar^{11924} + xbar^{11919} + xbar^{11916} + xbar^{11915} + xbar^{11914} + xbar^{11911} + xbar^{11910} + xbar^{11909} + xbar^{11908} + xbar^{11907} + xbar^{11905} + xbar^{11902} + xbar^{11898} + xbar^{11895} + xbar^{11894} + xbar^{11893} + xbar^{11891} + xbar^{11889} + xbar^{11888} + xbar^{11887} + xbar^{11886} + xbar^{11885} + xbar^{11884} + xbar^{11882} + xbar^{11880} + xbar^{11878} + xbar^{11877} + xbar^{11875} + xbar^{11874} + xbar^{11873} + xbar^{11872} + xbar^{11868} + xbar^{11866} + xbar^{11865} + xbar^{11863} + xbar^{11862} + xbar^{11858} + xbar^{11857} + xbar^{11852} + xbar^{11851} + xbar^{11848} + xbar^{11842} + xbar^{11841} + xbar^{11840} + xbar^{11839} + xbar^{11837} + xbar^{11833} + xbar^{11831} + xbar^{11830} + xbar^{11826} + xbar^{11825} + xbar^{11824} + xbar^{11821} + xbar^{11820} + xbar^{11818} + xbar^{11817} + xbar^{11816} + xbar^{11813} + xbar^{11812} + xbar^{11809} + xbar^{11806} + xbar^{11805} + xbar^{11802} + xbar^{11798} + xbar^{11797} + xbar^{11794} + xbar^{11789} + xbar^{11780} + xbar^{11776} + xbar^{11775} + xbar^{11773} + xbar^{11771} + xbar^{11770} + xbar^{11767} + xbar^{11766} + xbar^{11764} + xbar^{11763} + xbar^{11758} + xbar^{11757} + xbar^{11754} + xbar^{11746} + xbar^{11745} + xbar^{11744} + xbar^{11737} + xbar^{11736} + xbar^{11735} + xbar^{11734} + xbar^{11730} + xbar^{11728} + xbar^{11723} + xbar^{11722} + xbar^{11715} + xbar^{11714} + xbar^{11713} + xbar^{11712} + xbar^{11709} + xbar^{11705} + xbar^{11704} + xbar^{11703} + xbar^{11701} + xbar^{11694} + xbar^{11690} + xbar^{11689} + xbar^{11685} + xbar^{11684} + xbar^{11682} + xbar^{11681} + xbar^{11679} + xbar^{11678} + xbar^{11675} + xbar^{11672} + xbar^{11670} + xbar^{11668} + xbar^{11665} + xbar^{11664} + xbar^{11663} + xbar^{11661} + xbar^{11660} + xbar^{11659} + xbar^{11656} + xbar^{11655} + xbar^{11654} + xbar^{11653} + xbar^{11652} + xbar^{11651} + xbar^{11650} + xbar^{11649} + xbar^{11647} + xbar^{11643} + xbar^{11641} + xbar^{11639} + xbar^{11638} + xbar^{11637} + xbar^{11636} + xbar^{11634} + xbar^{11631} + xbar^{11629} + xbar^{11625} + xbar^{11624} + xbar^{11623} + xbar^{11619} + xbar^{11618} + xbar^{11617} + xbar^{11616} + xbar^{11614} + xbar^{11609} + xbar^{11608} + xbar^{11605} + xbar^{11604} + xbar^{11602} + xbar^{11601} + xbar^{11598} + xbar^{11597} + xbar^{11594} + xbar^{11593} + xbar^{11592} + xbar^{11591} + xbar^{11590} + xbar^{11589} + xbar^{11588} + xbar^{11587} + xbar^{11586} + xbar^{11585} + xbar^{11581} + xbar^{11580} + xbar^{11576} + x$

bar¹¹⁵⁷⁵ + xbar¹¹⁵⁷⁴ + xbar¹¹⁵⁷² + xbar¹¹⁵⁷¹ + xbar¹¹⁵⁷⁰ + xbar¹¹⁵⁶⁷ + xbar¹¹⁵⁶⁵ + xbar¹¹⁵⁶³ + xbar¹¹⁵⁶² + xbar¹¹⁵⁶⁰ + xbar¹¹⁵⁵⁹ + xbar¹¹⁵⁵⁸ + xbar¹¹⁵⁵⁷ + xbar¹¹⁵⁵⁵ + xbar¹¹⁵⁵⁴ + xbar¹¹⁵⁴⁹ + xbar¹¹⁵⁴⁸ + xbar¹¹⁵⁴⁶ + xbar¹¹⁵⁴⁵ + xbar¹¹⁵⁴⁴ + xbar¹¹⁵⁴³ + xbar¹¹⁵⁴² + xbar¹¹⁵⁴⁰ + xbar¹¹⁵³⁹ + xbar¹¹⁵³⁸ + xbar¹¹⁵³⁷ + xbar¹¹⁵³⁶ + xbar¹¹⁵³⁵ + xbar¹¹⁵³⁴ + xbar¹¹⁵³³ + xbar¹¹⁵³⁰ + xbar¹¹⁵²⁹ + xbar¹¹⁵²⁷ + xbar¹¹⁵²⁶ + xbar¹¹⁵²⁴ + xbar¹¹⁵²⁰ + xbar¹¹⁵¹⁴ + xbar¹¹⁵¹³ + xbar¹¹⁵¹⁰ + xbar¹¹⁵⁰⁸ + xbar¹¹⁵⁰⁶ + xbar¹¹⁵⁰¹ + xbar¹¹⁴⁹⁸ + xbar¹¹⁴⁹⁶ + xbar¹¹⁴⁹² + xbar¹¹⁴⁹¹ + xbar¹¹⁴⁹⁰ + xbar¹¹⁴⁸⁸ + xbar¹¹⁴⁸⁵ + xbar¹¹⁴⁸³ + xbar¹¹⁴⁸¹ + xbar¹¹⁴⁷⁹ + xbar¹¹⁴⁷⁶ + xbar¹¹⁴⁷⁵ + xbar¹¹⁴⁷² + xbar¹¹⁴⁶⁷ + xbar¹¹⁴⁶⁵ + xbar¹¹⁴⁶² + xbar¹¹⁴⁶¹ + xbar¹¹⁴⁵⁷ + xbar¹¹⁴⁵⁵ + xbar¹¹⁴⁵³ + xbar¹¹⁴⁵² + xbar¹¹⁴⁵¹ + xbar¹¹⁴⁵⁰ + xbar¹¹⁴⁴⁶ + xbar¹¹⁴⁴³ + xbar¹¹⁴⁴¹ + xbar¹¹⁴⁴⁰ + xbar¹¹⁴³⁸ + xbar¹¹⁴³⁶ + xbar¹¹⁴³⁵ + xbar¹¹⁴³⁴ + xbar¹¹⁴³³ + xbar¹¹⁴³² + xbar¹¹⁴²⁹ + xbar¹¹⁴²⁸ + xbar¹¹⁴²⁷ + xbar¹¹⁴²⁵ + xbar¹¹⁴²² + xbar¹¹⁴²⁰ + xbar¹¹⁴¹⁸ + xbar¹¹⁴¹⁷ + xbar¹¹⁴¹⁴ + xbar¹¹⁴¹³ + xbar¹¹⁴¹⁰ + xbar¹¹⁴⁰⁷ + xbar¹¹⁴⁰⁴ + xbar¹¹⁴⁰² + xbar¹¹³⁹⁸ + xbar¹¹³⁹⁷ + xbar¹¹³⁹⁵ + xbar¹¹³⁹⁴ + xbar¹¹³⁹³ + xbar¹¹³⁹² + xbar¹¹³⁹⁰ + xbar¹¹³⁸⁸ + xbar¹¹³⁸³ + xbar¹¹³⁸¹ + xbar¹¹³⁸⁰ + xbar¹¹³⁷⁸ + xbar¹¹³⁷⁷ + xbar¹¹³⁷⁶ + xbar¹¹³⁷⁵ + xbar¹¹³⁷³ + xbar¹¹³⁷⁰ + xbar¹¹³⁶⁹ + xbar¹¹³⁶⁸ + xbar¹¹³⁶⁶ + xbar¹¹³⁶² + xbar¹¹³⁶¹ + xbar¹¹³⁶⁰ + xbar¹¹³⁵² + xbar¹¹³⁵¹ + xbar¹¹³⁴⁷ + xbar¹¹³⁴⁴ + xbar¹¹³⁴³ + xbar¹¹³⁴⁰ + xbar¹¹³³⁹ + xbar¹¹³³⁸ + xbar¹¹³³⁶ + xbar¹¹³³⁴ + xbar¹¹³³³ + xbar¹¹³³⁰ + xbar¹¹³²⁹ + xbar¹¹³²⁴ + xbar¹¹³²³ + xbar¹¹³²² + xbar¹¹³²⁰ + xbar¹¹³¹⁸ + xbar¹¹³¹⁵ + xbar¹¹³¹⁴ + xbar¹¹³¹¹ + xbar¹¹³¹⁰ + xbar¹¹³⁰⁹ + xbar¹¹³⁰⁸ + xbar¹¹³⁰⁶ + xbar¹¹³⁰⁴ + xbar¹¹³⁰³ + xbar¹¹²⁹⁶ + xbar¹¹²⁹⁵ + xbar¹¹²⁹⁴ + xbar¹¹²⁹¹ + xbar¹¹²⁸⁸ + xbar¹¹²⁸⁷ + xbar¹¹²⁸⁶ + xbar¹¹²⁸³ + xbar¹¹²⁸⁰ + xbar¹¹²⁷⁷ + xbar¹¹²⁷⁵ + xbar¹¹²⁷³ + xbar¹¹²⁷¹ + xbar¹¹²⁶⁹ + xbar¹¹²⁶⁸ + xbar¹¹²⁶⁷ + xbar¹¹²⁶³ + xbar¹¹²⁶² + xbar¹¹²⁶¹ + xbar¹¹²⁵⁸ + xbar¹¹²⁵⁷ + xbar¹¹²⁵⁶ + xbar¹¹²⁵⁵ + xbar¹¹²⁵⁴ + xbar¹¹²⁵³ + xbar¹¹²⁵² + xbar¹¹²⁵¹ + xbar¹¹²⁵⁰ + xbar¹¹²⁴⁶ + xbar¹¹²⁴⁵ + xbar¹¹²⁴³ + xbar¹¹²⁴² + xbar¹¹²³⁹ + xbar¹¹²³⁸ + xbar¹¹²³⁷ + xbar¹¹²³⁶ + xbar¹¹²³⁵ + xbar¹¹²³⁴ + xbar¹¹²³² + xbar¹¹²³¹ + xbar¹¹²²⁹ + xbar¹¹²²⁸ + xbar¹¹²²⁷ + xbar¹¹²²⁴ + xbar¹¹²²² + xbar¹¹²¹⁸ + xbar¹¹²¹⁵ + xbar¹¹²¹¹ + xbar¹¹²⁰⁸ + xbar¹¹²⁰⁶ + xbar¹¹²⁰⁴ + xbar¹¹¹⁹⁹ + xbar¹¹¹⁹⁷ + xbar¹¹¹⁹⁵ + xbar¹¹¹⁹³ + xbar¹¹¹⁹¹ + xbar¹¹¹⁸⁴ + xbar¹¹¹⁸³ + xbar¹¹¹⁸⁰ + xbar¹¹¹⁷⁹ + xbar¹¹¹⁷⁶ + xbar¹¹¹⁷⁴ + xbar¹¹¹⁷³ + xbar¹¹¹⁷² + xbar¹¹¹⁷⁰ + xbar¹¹¹⁶⁸ + xbar¹¹¹⁶⁷ + xbar¹¹¹⁶³ + xbar¹¹¹⁶² + xbar¹¹¹⁶⁰ + xbar¹¹¹⁵⁷ + xbar¹¹¹⁵³ + xbar¹¹¹⁵² + xbar¹¹¹⁴⁹ + xbar¹¹¹⁴⁸ + xbar¹¹¹⁴⁷ + xbar¹¹¹⁴⁶ + xbar¹¹¹⁴⁵ + xbar¹¹¹⁴⁴ + xbar¹¹¹⁴¹ + xbar¹¹¹³⁵ + xbar¹¹¹³⁴ + xbar¹¹¹³² + xbar¹¹¹³⁰ + xbar¹¹¹²⁹ + xbar¹¹¹²⁸ + xbar¹¹¹²⁷ + xbar¹¹¹²⁶ + xbar¹¹¹²⁵ + xbar¹¹¹²³ + xbar¹¹¹²⁰ + xbar¹¹¹¹⁹ + xbar¹¹¹¹⁸ + xbar¹¹¹¹³ + xbar¹¹¹¹¹ + xbar¹¹¹¹⁰ + xbar¹¹¹⁰⁹ + xbar¹¹¹⁰⁷ + xbar¹¹¹⁰⁴ + xbar¹¹¹⁰³ + xbar¹¹¹⁰² + xbar¹¹⁰⁹⁹ + xbar¹¹⁰⁹⁸ + xbar¹¹⁰⁹⁷ + xbar¹¹⁰⁹⁵ + xbar¹¹⁰⁹⁰ + xbar¹¹⁰⁸⁷ + xbar¹¹⁰⁸⁵ + xbar¹¹⁰⁸² + xbar¹¹⁰⁸⁰ + xbar¹¹⁰⁷⁵ + xbar¹¹⁰⁷⁴ + xbar¹¹⁰⁶⁸ + xbar¹¹⁰⁶³ + xbar¹¹⁰⁶¹ + xbar¹¹⁰⁵⁶ + xbar¹¹⁰⁵³ + xbar¹¹⁰⁵⁰ + xbar¹¹⁰⁴⁹ + xbar¹¹⁰⁴⁸ + xbar¹¹⁰⁴⁶ + xbar¹¹⁰⁴⁵ + xbar¹¹⁰⁴⁴ + xbar¹¹⁰⁴³ + xbar¹¹⁰³⁹ + xbar¹¹⁰³⁸ + xbar¹¹⁰³⁵ + xbar¹¹⁰³⁴ + xbar¹¹⁰³³ + xbar¹¹⁰³¹ + xbar¹¹⁰²⁸ + xbar¹¹⁰²⁶ + xbar¹¹⁰²⁰ + xbar¹¹⁰¹⁹ + xbar¹¹⁰¹⁶ + xbar¹¹⁰¹⁵ + xbar¹¹⁰¹² + xbar¹¹⁰⁰⁹ + xbar¹¹⁰⁰⁷ + xbar¹¹⁰⁰⁶ + xbar¹¹⁰⁰⁵ + xbar¹¹⁰⁰⁴ + xbar¹¹⁰⁰³ + xbar¹¹⁰⁰¹ + xbar¹¹⁰⁰⁰ + xbar¹⁰⁹⁹⁸ + xbar¹⁰⁹⁹⁶ + xbar¹⁰⁹⁹³ + xbar¹⁰⁹⁸⁷ + xbar¹⁰⁹⁸⁶ + xbar¹⁰⁹⁸⁴ + xbar¹⁰⁹⁸³ + xbar¹⁰⁹⁸² + xbar¹⁰⁹⁷⁹ + xbar¹⁰⁹⁷⁸ + xbar¹⁰⁹⁷⁷ + xbar¹⁰⁹⁷⁶ + xbar¹⁰⁹⁷⁵ + xbar¹⁰⁹⁷² + xbar¹⁰⁹⁶⁸ + xbar¹⁰⁹⁶⁴ + xbar¹⁰⁹⁶³ + xbar¹⁰⁹⁶² + xbar¹⁰⁹⁶¹ + xbar¹⁰⁹⁶⁰ + xbar¹⁰⁹⁵⁹ + xbar¹⁰⁹⁵⁶ + xbar¹⁰⁹⁵⁵ + xbar¹⁰⁹⁴⁷ + xbar¹⁰⁹⁴⁶ + xbar¹⁰⁹⁴⁵ + xbar¹⁰⁹⁴³ + xbar¹⁰⁹⁴² + xbar¹⁰⁹⁴⁰ + xbar¹⁰⁹³⁹ + xbar¹⁰⁹³⁴ + xbar¹⁰⁹³² + xbar¹⁰⁹³¹ + xbar¹⁰⁹²⁹ + xbar¹⁰⁹²⁷ + xbar¹⁰⁹²⁶ + xbar¹⁰⁹²⁴ + xbar¹⁰⁹²² + xbar¹⁰⁹²¹ + xbar¹⁰⁹²⁰ + xbar¹⁰⁹¹⁹ + xbar¹⁰⁹¹⁸ + xbar¹⁰⁹¹⁶ + xbar¹⁰⁹¹² + xbar¹⁰⁹¹¹ + xbar¹⁰⁹¹⁰ + xbar¹⁰⁹⁰⁶ + xbar¹⁰⁹⁰⁵ + xbar¹⁰⁹⁰¹ + xbar¹⁰⁹⁰⁰ + xbar¹⁰⁸⁹⁷ + xbar¹⁰⁸⁹⁶ + xbar¹⁰⁸⁸⁷ + xbar¹⁰⁸⁸⁶ + xbar¹⁰⁸⁸⁵ + xbar¹⁰⁸⁸⁴ + xbar¹⁰⁸⁸² + xbar¹⁰⁸⁸⁰ + xbar¹⁰⁸⁷⁹ + xbar¹⁰⁸⁷⁸ + xbar¹⁰⁸⁷⁷ + xbar¹⁰⁸⁷⁵ + xbar¹⁰⁸⁷⁴ + xbar¹⁰⁸⁷³ + xbar¹⁰⁸⁷⁰ + xbar¹⁰⁸⁶⁷ + xbar¹⁰⁸⁶⁶ + xbar¹⁰⁸⁶⁵ + xbar¹⁰⁸⁵⁹ + xbar¹⁰⁸⁵¹ + xbar¹⁰⁸⁴⁶ + xbar¹⁰⁸⁴³ + xbar¹⁰⁸⁴² + xbar¹⁰⁸⁴¹ + xbar¹⁰⁸³⁹ + xbar¹⁰⁸³⁸ + xbar¹⁰⁸³⁷ + xbar¹⁰⁸³⁶ + xbar¹⁰⁸³⁵ + xbar¹⁰⁸³³ + xbar¹⁰⁸³² + xbar¹⁰⁸³⁰ + xbar¹⁰⁸²⁸ + xbar¹⁰⁸²⁷ + xbar¹⁰⁸²⁶ + xbar¹⁰⁸²⁵ + xbar¹⁰⁸²⁴ + xbar¹⁰⁸²² + xbar¹⁰⁸²⁰ + xbar¹⁰⁸¹⁹ + xbar¹⁰⁸¹⁸ + x

12/26

13/26

14/26

15/26

16/26

17/26

18/26

19/26

20/26

21/26

22/26

23/26

55 + xbar¹³⁵³ + xbar¹³⁵⁰ + xbar¹³⁴⁵ + xbar¹³⁴³ + xbar¹³⁴² + xbar¹³⁴⁰ + xbar¹³³¹ + xbar¹³³⁰ + xbar¹³²⁹ + xbar¹³²⁷ + xbar¹³²⁶ + xbar¹³²⁴ + xbar¹³²³ + xbar¹³²² + xbar¹³²¹ + xbar¹³²⁰ + xbar¹³¹⁹ + xbar¹³¹⁶ + xbar¹³¹⁴ + xbar¹³¹³ + xbar¹³¹⁰ + xbar¹³⁰⁹ + xbar¹³⁰⁷ + xbar¹³⁰¹ + xbar¹³⁰⁰ + xbar¹²⁹⁹ + xbar¹²⁹⁵ + xbar¹²⁹² + xbar¹²⁹¹ + xbar¹²⁸⁹ + xbar¹²⁸⁷ + xbar¹²⁸⁵ + xbar¹²⁸⁴ + xbar¹²⁸³ + xbar¹²⁸² + xbar¹²⁷⁹ + xbar¹²⁷⁸ + xbar¹²⁷⁷ + xbar¹²⁷³ + xbar¹²⁷¹ + xbar¹²⁶⁴ + xbar¹²⁶³ + xbar¹²⁶⁰ + xbar¹²⁵⁸ + xbar¹²⁵⁶ + xbar¹²⁵⁵ + xbar¹²⁵⁴ + xbar¹²⁵² + xbar¹²⁵¹ + xbar¹²⁵⁰ + xbar¹²⁴⁹ + xbar¹²⁴⁷ + xbar¹²⁴⁶ + xbar¹²⁴⁵ + xbar¹²⁴⁴ + xbar¹²⁴³ + xbar¹²⁴² + xbar¹²⁴¹ + xbar¹²³⁴ + xbar¹²³³ + xbar¹²³² + xbar¹²³¹ + xbar¹²³⁰ + xbar¹²²⁷ + xbar¹²²³ + xbar¹²¹⁹ + xbar¹²¹⁸ + xbar¹²¹⁷ + xbar¹²¹⁶ + xbar¹²¹⁵ + xbar¹²¹³ + xbar¹²¹² + xbar¹²¹¹ + xbar¹²¹⁰ + xbar¹²⁰⁹ + xbar¹²⁰⁸ + xbar¹²⁰⁷ + xbar¹²⁰⁵ + xbar¹²⁰³ + xbar¹²⁰² + xbar¹²⁰¹ + xbar¹¹⁹⁹ + xbar¹¹⁹⁸ + xbar¹¹⁹⁶ + xbar¹¹⁹⁴ + xbar¹¹⁹³ + xbar¹¹⁸⁷ + xbar¹¹⁸³ + xbar¹¹⁸⁰ + xbar¹¹⁷⁴ + xbar¹¹⁷¹ + xbar¹¹⁷⁰ + xbar¹¹⁶⁹ + xbar¹¹⁶⁸ + xbar¹¹⁶⁵ + xbar¹¹⁶⁴ + xbar¹¹⁶² + xbar¹¹⁶¹ + xbar¹¹⁵⁸ + xbar¹¹⁵⁵ + xbar¹¹⁵³ + xbar¹¹⁵¹ + xbar¹¹⁴⁹ + xbar¹¹⁴⁸ + xbar¹¹⁴⁷ + xbar¹¹⁴⁶ + xbar¹¹⁴⁵ + xbar¹¹⁴⁴ + xbar¹¹⁴³ + xbar¹¹⁴² + xbar¹¹³⁹ + xbar¹¹³³ + xbar¹¹³⁰ + xbar¹¹²⁷ + xbar¹¹²⁶ + xbar¹¹²⁴ + xbar¹¹²³ + xbar¹¹²² + xbar¹¹²¹ + xbar¹¹¹⁴ + xbar¹¹¹³ + xbar¹¹¹¹ + xbar¹¹¹⁰ + xbar¹¹⁰⁷ + xbar¹¹⁰⁴ + xbar¹¹⁰³ + xbar¹¹⁰² + xbar¹¹⁰¹ + xbar¹⁰⁹⁸ + xbar¹⁰⁹⁴ + xbar¹⁰⁹³ + xbar¹⁰⁹¹ + xbar¹⁰⁸⁹ + xbar¹⁰⁸⁷ + xbar¹⁰⁸⁶ + xbar¹⁰⁸³ + xbar¹⁰⁷⁸ + xbar¹⁰⁷⁰ + xbar¹⁰⁶⁹ + xbar¹⁰⁶⁸ + xbar¹⁰⁶⁷ + xbar¹⁰⁶⁶ + xbar¹⁰⁶² + xbar¹⁰⁶⁰ + xbar¹⁰⁵⁹ + xbar¹⁰⁵⁸ + xbar¹⁰⁵⁷ + xbar¹⁰⁵⁵ + xbar¹⁰⁵³ + xbar¹⁰⁵² + xbar¹⁰⁵¹ + xbar¹⁰⁴⁹ + xbar¹⁰⁴⁷ + xbar¹⁰⁴⁵ + xbar¹⁰⁴¹ + xbar¹⁰³⁸ + xbar¹⁰³⁵ + xbar¹⁰³³ + xbar¹⁰³² + xbar¹⁰³¹ + xbar¹⁰²⁵ + xbar¹⁰²⁴ + xbar¹⁰²³ + xbar¹⁰²⁰ + xbar¹⁰¹⁷ + xbar¹⁰¹⁴ + xbar¹⁰¹⁰ + xbar¹⁰⁰⁹ + xbar¹⁰⁰⁷ + xbar¹⁰⁰⁴ + xbar¹⁰⁰¹ + xbar¹⁰⁰⁰ + xbar⁹⁹⁷ + xbar⁹⁹⁵ + xbar⁹⁹⁴ + xbar⁹⁹³ + xbar⁹⁹² + xbar⁹⁸⁸ + xbar⁹⁸⁷ + xbar⁹⁸⁴ + xbar⁹⁷⁹ + xbar⁹⁷⁸ + xbar⁹⁷⁷ + xbar⁹⁷⁶ + xbar⁹⁷⁴ + xbar⁹⁶⁹ + xbar⁹⁶⁶ + xbar⁹⁶⁴ + xbar⁹⁶² + xbar⁹⁶⁰ + xbar⁹⁵⁹ + xbar⁹⁵⁷ + xbar⁹⁵⁶ + xbar⁹⁵⁴ + xbar⁹⁴⁹ + xbar⁹⁴⁸ + xbar⁹⁴⁶ + xbar⁹⁴⁵ + xbar⁹³⁷ + xbar⁹²⁷ + xbar⁹²⁶ + xbar⁹²⁵ + xbar⁹²⁴ + xbar⁹²² + xbar⁹²¹ + xbar⁹²⁰ + xbar⁹¹⁸ + xbar⁹¹⁶ + xbar⁹¹⁵ + xbar⁹¹⁴ + xbar⁹¹³ + xbar⁹¹⁰ + xbar⁹⁰⁸ + xbar⁹⁰⁷ + xbar⁹⁰⁵ + xbar⁹⁰³ + xbar⁹⁰⁰ + xbar⁸⁹⁹ + xbar⁸⁹⁸ + xbar⁸⁹⁷ + xbar⁸⁹⁶ + xbar⁸⁹⁵ + xbar⁸⁹⁴ + xbar⁸⁹² + xbar⁸⁹¹ + xbar⁸⁹⁰ + xbar⁸⁸⁷ + xbar⁸⁸⁶ + xbar⁸⁸⁵ + xbar⁸⁸⁴ + xbar⁸⁸³ + xbar⁸⁸¹ + xbar⁸⁸⁰ + xbar⁸⁷⁵ + xbar⁸⁷⁴ + xbar⁸⁷³ + xbar⁸⁷⁰ + xbar⁸⁶⁶ + xbar⁸⁶⁴ + xbar⁸⁶³ + xbar⁸⁶⁰ + xbar⁸⁵⁵ + xbar⁸⁵⁴ + xbar⁸⁵² + xbar⁸⁵¹ + xbar⁸⁴⁸ + xbar⁸⁴⁶ + xbar⁸⁴⁵ + xbar⁸⁴⁰ + xbar⁸³⁹ + xbar⁸³⁸ + xbar⁸³⁷ + xbar⁸³⁵ + xbar⁸³⁴ + xbar⁸³¹ + xbar⁸³⁰ + xbar⁸²⁹ + xbar⁸²⁸ + xbar⁸²⁷ + xbar⁸²⁴ + xbar⁸²³ + xbar⁸¹⁹ + xbar⁸¹⁸ + xbar⁸¹⁷ + xbar⁸¹⁶ + xbar⁸¹⁴ + xbar⁸¹² + xbar⁸⁰⁸ + xbar⁸⁰⁷ + xbar⁸⁰⁵ + xbar⁸⁰⁴ + xbar⁸⁰³ + xbar⁸⁰⁰ + xbar⁷⁹⁹ + xbar⁷⁹⁸ + xbar⁷⁹⁷ + xbar⁷⁹⁵ + xbar⁷⁹⁴ + xbar⁷⁹¹ + xbar⁷⁹⁰ + xbar⁷⁸⁸ + xbar⁷⁸⁷ + xbar⁷⁸⁵ + xbar⁷⁸³ + xbar⁷⁸¹ + xbar⁷⁷⁹ + xbar⁷⁷⁶ + xbar⁷⁷⁵ + xbar⁷⁷⁴ + xbar⁷⁷³ + xbar⁷⁷² + xbar⁷⁷⁰ + xbar⁷⁶⁶ + xbar⁷⁶² + xbar⁷⁶¹ + xbar⁷⁵⁹ + xbar⁷⁵⁸ + xbar⁷⁵⁴ + xbar⁷⁵³ + xbar⁷⁵² + xbar⁷⁵¹ + xbar⁷⁴⁵ + xbar⁷⁴⁴ + xbar⁷⁴³ + xbar⁷⁴¹ + xbar⁷³⁷ + xbar⁷³⁶ + xbar⁷³⁴ + xbar⁷³² + xbar⁷³¹ + xbar⁷²⁹ + xbar⁷²⁸ + xbar⁷²⁷ + xbar⁷²⁵ + xbar⁷²³ + xbar⁷²⁰ + xbar⁷¹⁹ + xbar⁷¹⁷ + xbar⁷¹⁶ + xbar⁷¹⁵ + xbar⁷¹⁰ + xbar⁷⁰⁹ + xbar⁷⁰⁸ + xbar⁷⁰³ + xbar⁷⁰² + xbar⁶⁹⁹ + xbar⁶⁹⁸ + xbar⁶⁹⁷ + xbar⁶⁹⁶ + xbar⁶⁹⁵ + xbar⁶⁹² + xbar⁶⁹¹ + xbar⁶⁹⁰ + xbar⁶⁸⁸ + xbar⁶⁸⁷ + xbar⁶⁸⁴ + xbar⁶⁷⁹ + xbar⁶⁷⁴ + xbar⁶⁷² + xbar⁶⁶⁸ + xbar⁶⁶⁴ + xbar⁶⁶¹ + xbar⁶⁵⁹ + xbar⁶⁵⁷ + xbar⁶⁵⁴ + xbar⁶⁵² + xbar⁶⁵⁰ + xbar⁶⁴⁵ + xbar⁶⁴⁴ + xbar⁶⁴³ + xbar⁶⁴² + xbar⁶⁴⁰ + xbar⁶³⁹ + xbar⁶³⁸ + xbar⁶³⁷ + xbar⁶³³ + xbar⁶³² + xbar⁶³¹ + xbar⁶²⁹ + xbar⁶²⁸ + xbar⁶²⁶ + xbar⁶²⁵ + xbar⁶²² + xbar⁶²¹ + xbar⁶²⁰ + xbar⁶¹⁹ + xbar⁶¹⁶ + xbar⁶¹³ + xbar⁶¹¹ + xbar⁶⁰⁹ + xbar⁶⁰⁸ + xbar⁶⁰⁷ + xbar⁶⁰⁶ + xbar⁶⁰¹ + xbar⁶⁰⁰ + xbar⁵⁹⁷ + xbar⁵⁹⁶ + xbar⁵⁹³ + xbar⁵⁹² + xbar⁵⁹¹ + xbar⁵⁸⁹ + xbar⁵⁸⁷ + xbar⁵⁸⁵ + xbar⁵⁸³ + xbar⁵⁸² + xbar⁵⁸⁰ + xbar⁵⁷⁹ + xbar⁵⁷⁸ + xbar⁵⁷⁵ + xbar⁵⁷⁴ + xbar⁵⁷¹ + xbar⁵⁷⁰ + xbar⁵⁶⁹ + xbar⁵⁶⁷ + xbar⁵⁶⁴ + xbar⁵⁶³ + xbar⁵⁶² + xbar⁵⁶¹ + xbar⁵⁶⁰ + xbar⁵⁵⁹ + xbar⁵⁵⁷ + xbar⁵⁵⁶ + xbar⁵⁵⁴ + xbar⁵⁵² + xbar⁵⁴⁹ + xbar⁵⁴⁸ + xbar⁵⁴⁷ + xbar⁵⁴⁶ + xbar⁵⁴⁵ + xbar⁵³⁷ + xbar⁵³⁶ + xbar⁵³³ + xbar⁵³² + xbar⁵³¹ + xbar⁵²⁴ + xbar⁵²³ + xbar⁵²⁰ + xbar⁵¹⁷ + xbar⁵¹³ + xbar⁵¹¹ + xbar⁵¹⁰ + xbar⁵⁰⁹ + xbar⁵⁰⁸ + xbar⁵⁰⁷ + xbar⁵⁰⁶ + xbar⁵⁰⁴ + xbar⁵⁰³ +

$xbar^{498} + xbar^{497} + xbar^{496} + xbar^{494} + xbar^{493} + xbar^{492} + xbar^{491} + xbar^{489} + xbar^{487} + xbar^{486} + xbar^{483} + xbar^{479} + xbar^{476} + xbar^{474} + xbar^{473} + xbar^{472} + xbar^{470} + xbar^{469} + xbar^{468} + xbar^{467} + xbar^{466} + xbar^{465} + xbar^{464} + xbar^{461} + xbar^{458} + xbar^{456} + xbar^{453} + xbar^{445} + xbar^{444} + xbar^{443} + xbar^{442} + xbar^{439} + xbar^{436} + xbar^{435} + xbar^{434} + xbar^{430} + xbar^{428} + xbar^{427} + xbar^{426} + xbar^{425} + xbar^{423} + xbar^{419} + xbar^{416} + xbar^{415} + xbar^{413} + xbar^{411} + xbar^{410} + xbar^{406} + xbar^{404} + xbar^{402} + xbar^{401} + xbar^{397} + xbar^{395} + xbar^{394} + xbar^{393} + xbar^{392} + xbar^{391} + xbar^{390} + xbar^{389} + xbar^{387} + xbar^{386} + xbar^{382} + xbar^{380} + xbar^{378} + xbar^{375} + xbar^{372} + xbar^{371} + xbar^{370} + xbar^{367} + xbar^{366} + xbar^{364} + xbar^{363} + xbar^{362} + xbar^{361} + xbar^{359} + xbar^{358} + xbar^{357} + xbar^{354} + xbar^{352} + xbar^{351} + xbar^{350} + xbar^{348} + xbar^{346} + xbar^{345} + xbar^{344} + xbar^{343} + xbar^{342} + xbar^{341} + xbar^{340} + xbar^{338} + xbar^{334} + xbar^{331} + xbar^{329} + xbar^{327} + xbar^{326} + xbar^{325} + xbar^{322} + xbar^{317} + xbar^{316} + xbar^{315} + xbar^{314} + xbar^{311} + xbar^{308} + xbar^{306} + xbar^{305} + xbar^{303} + xbar^{302} + xbar^{301} + xbar^{299} + xbar^{297} + xbar^{295} + xbar^{293} + xbar^{290} + xbar^{289} + xbar^{288} + xbar^{287} + xbar^{286} + xbar^{284} + xbar^{283} + xbar^{281} + xbar^{280} + xbar^{279} + xbar^{278} + xbar^{277} + xbar^{276} + xbar^{274} + xbar^{273} + xbar^{271} + xbar^{270} + xbar^{268} + xbar^{267} + xbar^{263} + xbar^{262} + xbar^{259} + xbar^{258} + xbar^{257} + xbar^{256} + xbar^{254} + xbar^{253} + xbar^{251} + xbar^{250} + xbar^{248} + xbar^{246} + xbar^{244} + xbar^{243} + xbar^{242} + xbar^{237} + xbar^{232} + xbar^{229} + xbar^{227} + xbar^{226} + xbar^{223} + xbar^{222} + xbar^{220} + xbar^{219} + xbar^{217} + xbar^{211} + xbar^{210} + xbar^{207} + xbar^{198} + xbar^{191} + xbar^{187} + xbar^{185} + xbar^{184} + xbar^{182} + xbar^{179} + xbar^{178} + xbar^{175} + xbar^{173} + xbar^{171} + xbar^{167} + xbar^{165} + xbar^{163} + xbar^{162} + xbar^{161} + xbar^{159} + xbar^{157} + xbar^{155} + xbar^{154} + xbar^{152} + xbar^{145} + xbar^{142} + xbar^{141} + xbar^{140} + xbar^{138} + xbar^{134} + xbar^{132} + xbar^{131} + xbar^{129} + xbar^{128} + xbar^{125} + xbar^{124} + xbar^{122} + xbar^{121} + xbar^{119} + xbar^{118} + xbar^{116} + xbar^{115} + xbar^{111} + xbar^{110} + xbar^{106} + xbar^{105} + xbar^{104} + xbar^{102} + xbar^{101} + xbar^{100} + xbar^{99} + xbar^{97} + xbar^{95} + xbar^{94} + xbar^{93} + xbar^{91} + xbar^{88} + xbar^{85} + xbar^{84} + xbar^{83} + xbar^{82} + xbar^{81} + xbar^{78} + xbar^{77} + xbar^{76} + xbar^{74} + xbar^{73} + xbar^{72} + xbar^{70} + xbar^{69} + xbar^{68} + xbar^{67} + xbar^{66} + xbar^{65} + xbar^{64} + xbar^{63} + xbar^{62} + xbar^{60} + xbar^{56} + xbar^{55} + xbar^{54} + xbar^{53} + xbar^{48} + xbar^{46} + xbar^{43} + xbar^{42} + xbar^{41} + xbar^{39} + xbar^{38} + xbar^{37} + xbar^{34} + xbar^{24} + xbar^{23} + xbar^{19} + xbar^{18} + xbar^{12} + xbar^{7} + xbar^{5} + xbar^{4} + xbar^{3} + xbar^{1}$

Chave Privada: $(xbar^{12188} + xbar^{11882} + xbar^{11852} + xbar^{11351} + xbar^{11331} + xbar^{11246} + xbar^{11078} + xbar^{10860} + xbar^{10731} + xbar^{10175} + xbar^{10025} + xbar^{9930} + xbar^{9906} + xbar^{9748} + xbar^{9400} + xbar^{9387} + xbar^{9258} + xbar^{9180} + xbar^{9088} + xbar^{8861} + xbar^{8404} + xbar^{8391} + xbar^{8337} + xbar^{8238} + xbar^{8233} + xbar^{8144} + xbar^{7985} + xbar^{7939} + xbar^{7906} + xbar^{7736} + xbar^{7467} + xbar^{7316} + xbar^{7080} + xbar^{6769} + xbar^{6723} + xbar^{6683} + xbar^{6642} + xbar^{6561} + xbar^{6400} + xbar^{5841} + xbar^{5635} + xbar^{5595} + xbar^{5559} + xbar^{5499} + xbar^{4908} + xbar^{4627} + xbar^{4417} + xbar^{4177} + xbar^{4148} + xbar^{4020} + xbar^{4000} + xbar^{3359} + xbar^{3023} + xbar^{2579} + xbar^{2398} + xbar^{2060} + xbar^{2059} + xbar^{1913} + xbar^{1890} + xbar^{1667} + xbar^{1224} + xbar^{1059} + xbar^{1005} + xbar^{985} + xbar^{668} + xbar^{528} + xbar^{289} + xbar^{169} + xbar^{81} + xbar^{25} + xbar^{11}, xbar^{12281} + xbar^{12043} + xbar^{11835} + xbar^{11702} + xbar^{11572} + xbar^{11468} + xbar^{11385} + xbar^{11136} + xbar^{10658} + xbar^{10540} + xbar^{10259} + xbar^{10190} + xbar^{9938} + xbar^{9718} + xbar^{9602} + xbar^{9320} + xbar^{9210} + xbar^{9191} + xbar^{8732} + xbar^{8730} + xbar^{8172} + xbar^{7898} + xbar^{7609} + xbar^{7550} + xbar^{7187} + xbar^{7063} + xbar^{6738} + xbar^{6518} + xbar^{6324} + xbar^{6116} + xbar^{6078} + xbar^{5579} + xbar^{5402} + xbar^{5400} + xbar^{5259} + xbar^{5248} + xbar^{5247} + xbar^{5073} + xbar^{4970} + xbar^{4939} + xbar^{4718} + xbar^{4647} + xbar^{4620} + xbar^{4495} + xbar^{4362} + xbar^{4175} + xbar^{4128} + xbar^{4034} + xbar^{3964} + xbar^{3954} + xbar^{3933} + xbar^{3925} + xbar^{3888} + xbar^{3647} + xbar^{2962} + xbar^{2882} + xbar^{2794} + xbar^{2193} + xbar^{2021} + xbar^{1735} + xbar^{1673} + xbar^{1454} + xbar^{1369} + xbar^{1236} + xbar^{774} + xbar^{771} + xbar^{520} + xbar^{512} + xbar^{200} + xbar^{193} + xbar^{184}, b'\backslash xee\&\backslash x18\backslash x10\backslash xdd\backslash xc3\backslash x01m\backslash xdeg\backslash xcc,\backslash xb9k\backslash x074\backslash xc0\backslash x9fDq\backslash xf0\backslash x94\backslash x98\backslash xdfd\backslash xdb\backslash x1f\backslash xc3\backslash x8c-+X')$

Encapsulação completa!

===== DESCOMPACTANDO =====
Decodificação bem-sucedida!