**Licenciatura segurança informática em redes de computadores**

**Trabalho Prático**

**Relatório**

**Realizado por:**

**Hugo Martins (8230273),**

**Pedro Antunes (8230068),**

**Rúben Pereira (8230168),**

**João Ribeiro (8230157);**

**Unidade Curricular: Matemática Discreta**

Junho 2024

Índice

[1. Indução Matemática 4](#_Toc170132382)

[1.1. Introdução á Indução Matemática 4](#_Toc170132383)

[1.2. Resolução e exemplificação de um exercício 4](#_Toc170132384)

[1.2.1. Resolução 4](#_Toc170132385)

[1.2.1.1. Passo base 4](#_Toc170132386)

[1.2.1.2. Passo indutivo 5](#_Toc170132387)

[1.3.Conclusão 5](#_Toc170132388)

[2. Rota do Românico 6](#_Toc170132389)

[2.1. Monumentos 6](#_Toc170132390)

[2.2. Alojamento 6](#_Toc170132391)

[2.3. Construção do grafo 6](#_Toc170132392)

[2.4. Classificação do grafo 7](#_Toc170132393)

[2.6. Matriz de adjacências 9](#_Toc170132394)

[2.7. Matriz de Custo 10](#_Toc170132395)

[2.7.1. Matriz de custo para o critério de tempo em Minutos 10](#_Toc170132396)

[2.7.2. Matriz de custo para o critério de distância em Km 11](#_Toc170132397)

[2.7.3. Tabela de custo tempo 12](#_Toc170132398)

[2.7.4. Tempo de custo de distância 13](#_Toc170132399)

[2.3. Exercício 2.b) do trabalho 15](#_Toc170132400)

[2.4. Exercício 2.c) do trabalho 17](#_Toc170132401)

[3. Criptografia 18](#_Toc170132402)

[3.1.1. Alfabeto Cifrado 18](#_Toc170132403)

[3.1.2. Alfabeto Original 19](#_Toc170132404)

[3.1.3. Alfabeto definido pela fórmula 19](#_Toc170132405)

[3.1.4. Inversão da Cifra de César 21](#_Toc170132406)

[3.1.5. Alfabeto definido pela inversa da fórmula 22](#_Toc170132407)

[3.2 Resolução do problema 23](#_Toc170132408)

[4. Conclusão 24](#_Toc170132409)

[5.Bibliografia 25](#_Toc170132410)

Índice de Figuras

[Figura 1 - Mapa que representa todos os monumentos, intersecções e o alojamento escolhido 6](#_Toc169995930)

[Figura 2 - Grafo representativo dos monumentos, intersecções e do alojamento escolhido 7](#_Toc169995931)

[Figura 3 - Grafo que representa os vários percursos possíveis e respetivo custo (minutos) 11](#_Toc169995932)

[Figura 4 - Grafo que representa os vários percursos possíveis e respetivo custo (kms) 12](#_Toc169995933)

[Figura 5 – Tabela de dijkstra (tempo) 13](#_Toc169995934)

[Figura 6 – Tabela de dijkstra (distância) 14](#_Toc169995935)

# 1. Indução Matemática

## 1.1. Introdução á Indução Matemática

A indução matemática é uma técnica de prova utilizada em matemática para demonstrar a veracidade de uma proposição para todos os números naturais. Ela é especialmente útil para provar propriedades que se aplicam a uma sequência de casos, como somas, desigualdades ou propriedades algébricas que envolvem números naturais.

A prova por indução matemática consiste em dois passos principais:

* **Passo Base**: Verificar que a proposição é verdadeira para o menor valor de , geralmente é , pois é em muitos casos o primeiro termo de uma sequência.
* **Passo Indutivo**: Neste passo afirmamos que como também , ou seja, assumimos que a proposição é verdadeira para (hipótese de indução) e mostramos que isso implica que a proposição é verdadeira para(tese).

A indução matemática tem por base estes dois passos para demonstrar a veracidade de uma proposição de números. Poderemos ver no seguinte exercício, como a indução matemática pode ser utilizada.

## 1.2. Resolução e exemplificação de um exercício

Prove por indução matemática que

**, .**

Exercício retirado da Lista de Exercícios 4 da Universidade Federal de Minas Gerais, Curso Ciências Exatas e Engenharias do ano de 2018 página 3.

### 1.2.1. Resolução

### 1.2.1.1. Passo base

Primeiramente, temos de seguir o passo base como já foi referido, utilizaremos o n=1 para verificar se o primeiro termo da sucessão corresponde ao resultado final. Então:

De facto, para a primeira sucessão verificamos a veracidade do passo base. 1 é igual a 1.

### 1.2.1.2. Passo indutivo

Passemos agora para o passo indutivo, queremos demonstrar que através da preposição de veracidade que n=k, diremos também que n=k+1. E como podemos demonstrar esta situação? Então,

Agora, assumimos que a fórmula é verdadeira para um . Esta é a hipótese de indução:

Queremos provar que a fórmula é verdadeira para . Ou seja, queremos mostrar que:

Vamos começar com a soma dos primeiros k termos e adicionar o próximo número ímpar :

Usando a hipótese de indução, sabemos que:

Então, a soma torna-se:

Simplificamos :

Agora substituímos na soma:

Reconhecemos que isso é uma expansão do quadrado perfeito:

Assim, mostramos que se a fórmula é verdadeira para , ela também é verdadeira para .

## 1.3.Conclusão

Pela indução matemática, como a fórmula é verdadeira para e mostramos que, se é verdadeira para , então é verdadeira para , concluímos que a fórmula:

é verdadeira para todo .

# 2. Rota do Românico

## 2.1. Monumentos

Para este exercício, foi pedido para escolhermos 6 monumentos da rota do românico, entre os quais selecionamos os seguintes:

* Mosteiro de Santa Maria Pombeiro
* Igreja do Salvador de Aveleda
* Igreja de Santo André de Vila Boa de Quires
* Igreja do Salvador de Tabuado
* Igreja de Santo André de Telões
* Castelo de Arnoia

## 2.2. Alojamento

Foi também nos requisitado a escolha de um alojamento contido na rota do românico ao qual selecionamos A Casa da Cachada.

## 2.3. Construção do grafo

Após a escolha dos monumentos e alojamento, procedemos á construção do nosso grafo para melhor organização e planeamento das próximas etapas que nos foram requeridas.

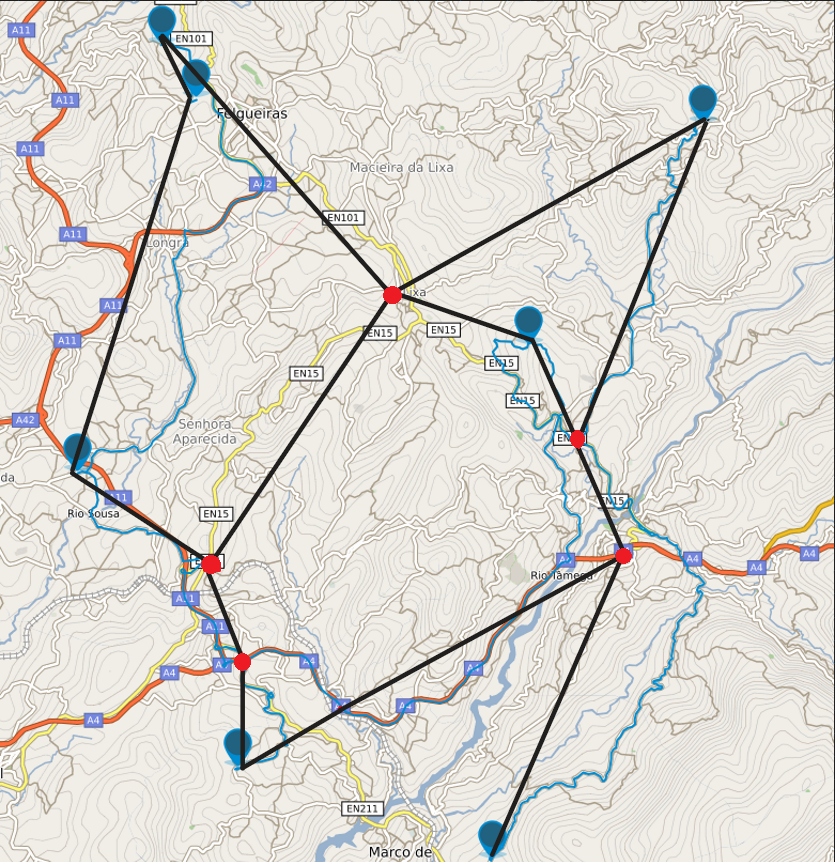


Figura 1 - Mapa que representa todos os monumentos, intersecções e o alojamento escolhido

Os pontos azuis referem-se aos monumentos e alojamento.

Os pontos vermelhos referem-se a interseções/cruzamentos que inserimos para que não fosse um grafo completo.

## 2.4. Classificação do grafo

Então, definimos que os nossos conjuntos dos vértices e das arestas do nosso grafo são:

Gv = {1 , 2 , 3 , 4 , 5 , 6 , ALO , Inter1 , Inter2 , Inter3 , Inter4 , Inter5}

Constituído por 6 monumentos, 5 interseções e 1 alojamento.

Ga = {[1,ALO];[ALO,2];[2,INTER1];[INTER1,INTER2];[INTER2,3];[3,INTER3];[INTER3,4]; [INTER3,INTER4];[INTER4,6];[INTER4,5][INTER5,5];[INTER5,6];[INTER5,INTER1]; [INTER5,1]}

Constituído por 14 arestas entre os monumentos, interseções e o alojamento.

Graus dos vértices: V1=2, V2=2, V3=2, V4=1, V5=2, V6=2, ALO=2, INTER1=3, INTER2=2, INTER3=3, INTER4=3, INTER5=4.

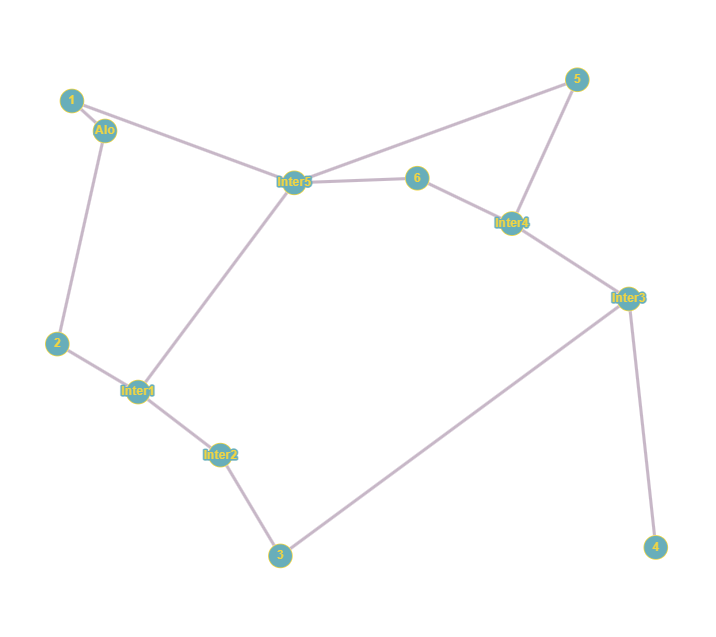


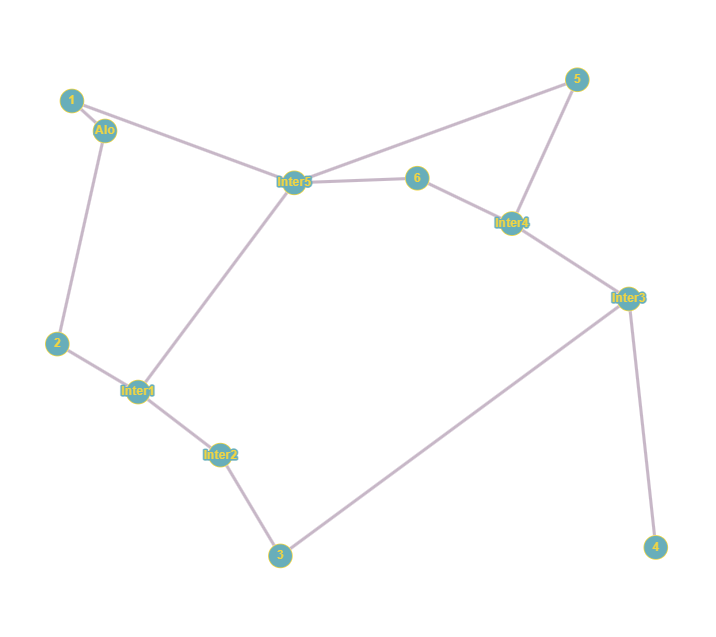
Figura 2 - Grafo representativo dos monumentos, intersecções e do alojamento escolhido

Por classificação, o nosso grafo é:

* Não orientado, pois nenhuma aresta tem direção especifica uma vez que apresentam uma matriz de adjacência simétrica.
* Grafo Simples, pois não existem arestas múltiplas nem lacetes no grafo.
* Grafo Conexo, pois todos os vértices têm ligação entre si através de um caminho que os une.
* Grafo não é completo, pois nem todos os vértices são adjacentes entre si.
* Grafo não é Euleriano pois embora seja um grafo conexo, nem todos os vértices têm grau par.
* Grafo não é Hamiltoniano pois segundo o teorema de Dirac, neste grafo nâo é possivel de ser executado pois não segue uma das suas regras (O Teorema de Dirac afirma que um grafo simples com vértices é hamiltoniano se o grau de cada vértice é pelo menos **)**. Neste caso todos os vértices teriam de ter pelo menos grau 6 o que não se verifica. No Teorema de Ore afirma-se que um grafo simples com vértices () é hamiltoniano se, para cada par de vértices não adjacentes e , a soma dos graus o que não se verifica neste grafo.

## 2.6. Matriz de adjacências

A matriz de adjacências é uma forma de representar grafos em matemática e ciência da computação. Ela é especialmente útil para trabalhar com grafos de forma algorítmica e é uma das várias formas de representar grafos, cada uma com suas próprias vantagens e desvantagens dependendo do contexto e do tipo de grafo em questão.



A matriz de adjacências do nosso grafo é representada da seguinte forma:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **ALO** | **INTER1** | **INTER2** | **INTER3** | **INTER4** | **INTER5** |
| **1** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **0** | **0** | **0** | **0** | **1** |
| **2** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **1** | **0** | **0** | **0** | **0** |
| **3** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **1** | **0** | **0** |
| **4** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **0** | **0** |
| **5** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **1** |
| **6** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **1** |
| **ALO** | **1** | **1** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **INTER1** | **0** | **1** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **0** | **0** | **1** |
| **INTER2** | **0** | **0** | **1** | **0** | **0** | **0** | **0** | **1** | **0** | **0** | **0** | **0** |
| **INTER3** | **0** | **0** | **1** | **1** | **0** | **0** | **0** | **0** | **0** | **0** | **1** | **0** |
| **INTER4** | **0** | **0** | **0** | **0** | **1** | **1** | **0** | **0** | **0** | **1** | **0** | **0** |
| **INTER5** | **1** | **0** | **0** | **0** | **1** | **1** | **0** | **1** | **0** | **0** | **0** | **0** |

## 2.7. Matriz de Custo

A matriz de custo em grafos, também conhecida como matriz de pesos, é uma forma de representar os custos (ou valores) associados às arestas de um grafo. Em um grafo orientado (ou dígrafo), os custos indicam o "preço" ou "distância" para se mover de um nó (vértice) a outro. Em um grafo não dirigido, os custos são simétricos e a matriz é simétrica.

A matriz de custo fornece uma representação compacta e eficiente dos custos de navegação entre os vértices, facilitando a implementação de algoritmos que solucionam problemas de roteamento e conectividade.

### 2.7.1. Matriz de custo para o critério de tempo em Minutos

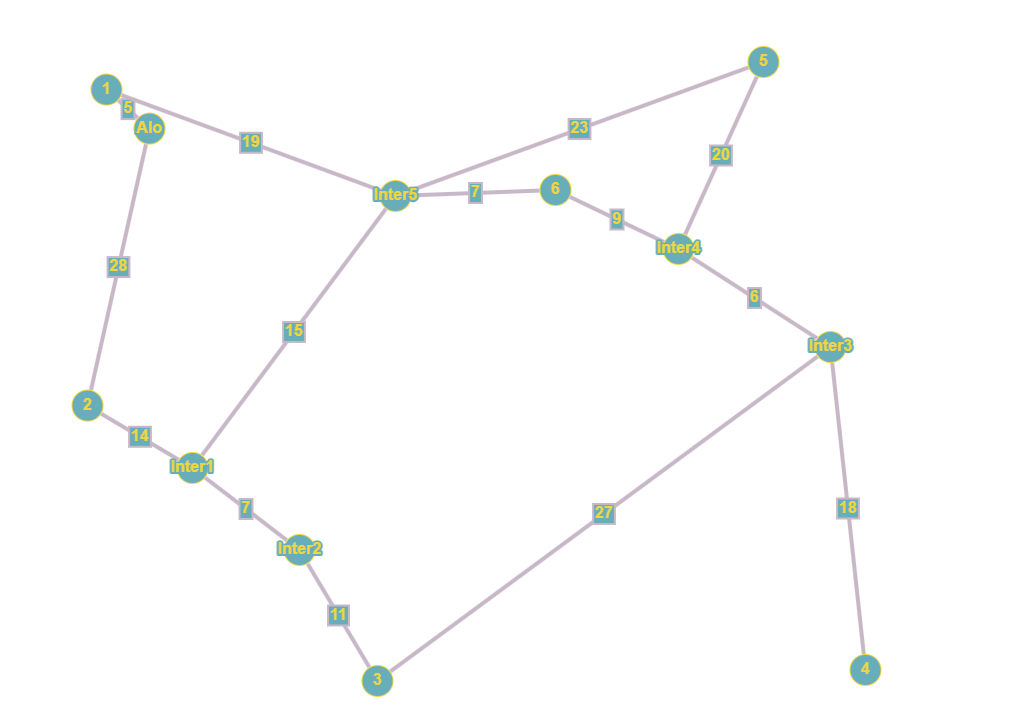


Figura 3 - Grafo que representa os vários percursos possíveis e respetivo custo (minutos)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **ALO** | **INTER1** | **INTER2** | **INTER3** | **INTER4** | **INTER5** |
| **1** | **0** | **0** | **0** | **0** | **0** | **0** | **5** | **0** | **0** | **0** | **0** | **19** |
| **2** | **0** | **0** | **0** | **0** | **0** | **0** | **28** | **14** | **0** | **0** | **0** | **0** |
| **3** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **11** | **27** | **0** | **0** |
| **4** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **18** | **0** | **0** |
| **5** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **20** | **23** |
| **6** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **9** | **7** |
| **ALO** | **5** | **28** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **INTER1** | **0** | **14** | **0** | **0** | **0** | **0** | **0** | **0** | **7** | **0** | **0** | **15** |
| **INTER2** | **0** | **0** | **11** | **0** | **0** | **0** | **0** | **7** | **0** | **0** | **0** | **0** |
| **INTER3** | **0** | **0** | **27** | **18** | **0** | **0** | **0** | **0** | **0** | **0** | **6** | **0** |
| **INTER4** | **0** | **0** | **0** | **0** | **20** | **9** | **0** | **0** | **0** | **6** | **0** | **0** |
| **INTER5** | **19** | **0** | **0** | **0** | **23** | **7** | **0** | **15** | **0** | **0** | **0** | **0** |

### 2.7.2. Matriz de custo para o critério de distância em Kms

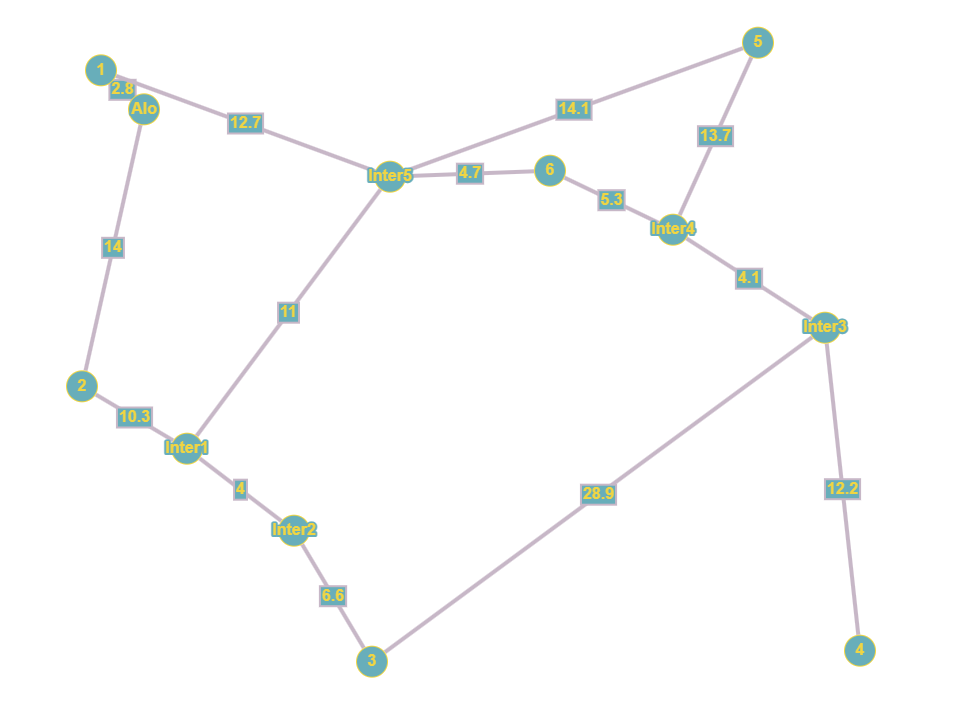


Figura 4 - Grafo que representa os vários percursos possíveis e respetivo custo (kms)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **ALO** | **INTER1** | **INTER2** | **INTER3** | **INTER4** | **INTER5** |
| **1** | **0** | **0** | **0** | **0** | **0** | **0** | **2.8** | **0** | **0** | **0** | **0** | **12.7** |
| **2** | **0** | **0** | **0** | **0** | **0** | **0** | **14** | **10.3** | **0** | **0** | **0** | **0** |
| **3** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **6.6** | **28.9** | **0** | **0** |
| **4** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **12.2** | **0** | **0** |
| **5** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **13.7** | **14.1** |
| **6** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **5.3** | **4.7** |
| **ALO** | **2.8** | **14** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **INTER1** | **0** | **10.3** | **0** | **0** | **0** | **0** | **0** | **0** | **4** | **0** | **0** | **11** |
| **INTER2** | **0** | **0** | **6.6** | **0** | **0** | **0** | **0** | **4** | **0** | **0** | **0** | **0** |
| **INTER3** | **0** | **0** | **28.9** | **12.2** | **0** | **0** | **0** | **0** | **0** | **0** | **4.1** | **0** |
| **INTER4** | **0** | **0** | **0** | **0** | **13.7** | **5.3** | **0** | **0** | **0** | **4.1** | **0** | **0** |
| **INTER5** | **12.7** | **0** | **0** | **0** | **14.1** | **4.7** | **0** | **11** | **0** | **0** | **0** | **0** |

As nossas matrizes de custo baseiam-se apenas nos dois critérios anteriormente selecionados: tempo e distância, pois para conhecermos novas rotas e planear-lhas da melhor forma, o tempo e as distâncias são cruciais na organização das mesmas.

### 2.7.3. Tabela de custo tempo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| It. | (M) | Mc | A | e | X e | R: Caminhos mínimos |
| 0 | - | ALO | {1,2} | ALO,1 -> 5  ALO, 2 -> 28 | {1,2}  {5,28} | ALO,1  ALO,2 |
| 1 | 1 | ALO, 1 | {inter5} | ALO,1, inter5 -> 24 | {inter5}  {19} | ALO,1, inter5 |
| 2 | Inter5 | ALO,1,inter5 | {inter1, 5, 6} | ALO,1, inter5, inter1 -> 39  ALO,1, inter5, 5 ->47  ALO,1, inter5, 6 ->31 | {inter1, 5, 6}  {15,23,7} | ALO,1, inter5, inter1  ALO,1, inter5, 5  ALO,1, inter5, 6 |
| 3 | 2 | ALO,2 | {inter1} | ALO,2, inter1->42 | {inter1 }  {14} | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 4 | 6 | ALO,1, inter5,6 | {inter4} | ALO,1, inter5,6, inter4 -> 40 | {inter4}  {9} | ALO,1, inter5,6, inter4 |
| 5 | Inter1 | ALO,1, inter5, inter1 | {2, inter2} | ALO,1, inter5, inter1,2 -> 53  ALO,1, inter5, inter1, inter2 -> 46 | {2, inter2 }  {14, 7} | ALO,1, inter5, inter1, inter2 |
| 6 | Inter4 | ALO,1, inter5,6, inter4 | {5, inter3} | ALO,1, inter5,6, inter4,5 -> 60  ALO,1, inter5,6, inter4, inter3 -> 46 | {5, inter3}  {20,6} | ALO,1, inter5, inter4, inter3 |
| 7 | Inter1 | ALO,2,inter1 | {inter5,inter2} | ALO,2,inter1, inter5 ->57  ALO,2,inter1, inter2 ->49 | {inter2,inter5}  {7,15} | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 8 | Inter2 | ALO,1, inter5, inter1, inter2 | {3} | ALO,1, inter5, inter1,inter2, 3 -> 57 | {3}  {11} | ALO,1, inter5, inter1,inter2, 3 |
| 9 | inter3 | ALO,1, inter5,6, inter4, inter3 | {3,4} | ALO,1, inter5,6, inter4, inter3, 3-> 73  ALO,1, inter5,6, inter4, inter3, 4 -> 64 | {3,4}  {27,18} | ALO,1, inter5,6, inter4, inter3, 4 |

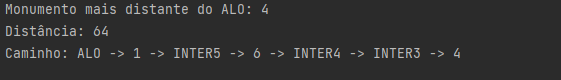
Figura 5 – Tabela de dijkstra (tempo)

### 2.7.4. Tempo de custo de distância

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| It. | (M) | Mc | A | e | X e | R: Caminhos mínimos |
| 0 | - | ALO | {1,2} | ALO,1 -> 2.8  ALO, 2 -> 14 | {1,2}  {2.8,14} | ALO,1  ALO,2 |
| 1 | 1 | ALO, 1 | {Inter5} | ALO,1, Inter5 -> 15.5 | {Inter5}  {12.7} | ALO,1, Inter5 |
| 2 | 2 | ALO,2, Inter1 | {Inter1} | ALO,2, Inter1->24.3 | {Inter1}  {10.3} | ALO,2, Inter1 |
| 3 | Inter5 | ALO,1, Inter5 | {5, 6, Inter1} | ALO,1, Inter5, 5->29.6  ALO,1, Inter5, 6->20.2  ALO,1, Inter5, Inter1->26.5 | {5, 6, Inter1}  {14.1, 4.7, 11} | ALO,1, Inter5, 5  ALO,1, Inter5, 6 |
| 4 | 6 | ALO,1, Inter5, 6 | {Inter4} | ALO,1, Inter5, 6, Inter4->25.5 | {Inter4}  {5.3} | ALO,1, Inter5, 6, Inter4 |
| 5 | Inter1 | ALO,2, Inter1 | {Inter5, Inter2} | ALO,2, Inter1, Inter2->28.3  ALO,2, Inter1, Inter5->35.3 | {Inter2, Inter5}  {4, 11} | ALO,2, Inter1, Inter2 |
| 6 | Inter4 | ALO,1, Inter5, 6, Inter4 | {5, Inter3} | ALO,1, Inter5, 6, Inter4, 5->39.2  ALO,1, Inter5, 6, Inter4, inter3->29.6 | {5, inter3}  {13.7, 4.1} | ALO,1, Inter5, 6, Inter4, inter3 |
| 7 | Inter1 | ALO,1, Inter5, Inter1 | {2,inter2} | ALO,1, Inter5, Inter1, 2->36.8  ALO,1, Inter5, Inter1, inter2->30.5 | {2, inter2}  {10.3, 4} | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 8 | Inter2 | ALO,2, Inter1, Inter2 | {3} | ALO,2, Inter1, Inter2, 3->34.9 | {3}  {6.6} | ALO,2, Inter1, Inter2, 3 |
| 9 | 5 | ALO,1, Inter5, 5 | {inter4} | ALO,1, Inter5, 5, inter4->43.3 | {inter4}  {13.7} | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 10 | Inter3 | ALO,1, Inter5, 6, Inter4, inter3 | {3, 4} | ALO,1, Inter5, 6, Inter4, inter3, 3->58.5  ALO,1, Inter5, 6, Inter4, inter3, 4->41.8 | {3, 4}  {28.9, 12.2} | ALO,1, Inter5, 6, Inter4, inter3, 4 |

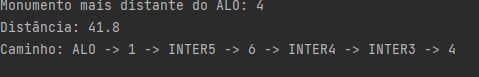
Figura 6 – Tabela de dijkstra (distância)

Verificando nas duas tabelas de dijkstra podemos afirmar que o percurso com menor custo entre a origem no alojamento e o monumento mais distante para o custo tempo é: {ALO,1, inter5,6, inter4, inter3,4 -> 64}



Para a tabela de custo de distância, podemos verificar que é:

{ALO,1, inter5,6, inter4, inter3,4 -> 41.8}



## 2.3. Exercício 2.b) do trabalho

Neste exercício foi utilizado um programa da linguagem java para vermos o percurso com menor custo entre cada dois locais.

Como não é possível no programa usado colocar nomes, salienta-se que:

* O número 7 refere-se ao ALO;
* O número 8 refere-se ao inter1;
* O número 9 refere-se ao inter2;
* O número 10 refere-se ao inter3;
* O número 11 refere-se ao inter4;
* O número 12 refere-se ao inter5.

O caminho com menor custo entre 1 e 2:



O caminho com menor custo entre 1 e 3:



O caminho com menor custo entre 1 e 4:



O caminho com menor custo entre 1 e 5:



O caminho com menor custo entre 1 e 6:



O caminho com menor custo entre 1 e 7:

Uma imagem com texto, Tipo de letra, captura de ecrã, tipografia

Descrição gerada automaticamente

O caminho com menor custo entre 2 e 3:



O caminho com menor custo entre 2 e 4:



O caminho com menor custo entre 2 e 5:



O caminho com menor custo entre 2 e 6:



O caminho com menor custo entre 2 e 7:

Uma imagem com texto, Tipo de letra, captura de ecrã, tipografia

Descrição gerada automaticamente

O caminho com menor custo entre 3 e 4:



O caminho com menor custo entre 3 e 5:



O caminho com menor custo entre 3 e 6:



O caminho com menor custo entre 3 e 7:

Uma imagem com texto, Tipo de letra, captura de ecrã

Descrição gerada automaticamente

O caminho com menor custo entre 4 e 5:



O caminho com menor custo entre 4 e 6:



O caminho com menor custo entre 4 e 7:



O caminho com menor custo entre 5 e 6:



O caminho com menor custo entre 5 e 7:

Uma imagem com texto, Tipo de letra, captura de ecrã

Descrição gerada automaticamente

O caminho com menor custo entre 6 e 7:

Uma imagem com texto, Tipo de letra, captura de ecrã

Descrição gerada automaticamente

## 2.4. Exercício 2.c) do trabalho

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **1** | **0** | **33** | **65** | **59** | **42** | **26** | **5** |
| **2** | **33** | **0** | **32** | **69** | **52** | **36** | **28** |
| **3** | **65** | **32** | **0** | **45** | **53** | **40** | **57** |
| **4** | **59** | **69** | **45** | **0** | **44** | **33** | **64** |
| **5** | **42** | **52** | **53** | **44** | **0** | **29** | **47** |
| **6** | **26** | **36** | **40** | **33** | **29** | **0** | **31** |
| **7** | **5** | **28** | **57** | **64** | **47** | **31** | **0** |

Partindo do ponto 7 (ALO), podemos verificar que caminho com menor custo é para o vértice 1, do vértice 1 o caminho com menor custo é o vértice 6, do vértice 6 o caminho com menor custo é o 5, do vértice 5 o caminho com menor custo é o 4, do vértice 4 o caminho com menor custo é o 3, do vértice 3 o caminho com menor custo é o 2, do vértice 2 o caminho com menor custo é o 7(ALO) construindo-se o seguinte circuito:

7 -> 1 -> 6 -> 5 -> 4 -> 3 -> 2 -> 7 = 5 + 26 + 29 + 44 + 45 + 32 + 28 = 209

Com isto podemos concluir que se trata de um circuito que parte do alojamento passando por todos os monumentos e voltando ao alojamento, tendo em conta que pode passar pela mesma interceção mais que uma vez.

Logo com isto podemos verificar que não é um circuito hamiltoniano porque não passa pelo mesmo vértice uma única vez, visto que tem de passar mais que uma vez pela mesma interceção.

Também não se trata de um circuito de Euler porque não transita em todas as arestas uma única vez.

# 3. Criptografia

A criptografia é a ciência e prática de proteger informações ao transformá-las em uma forma ilegível para aqueles que não possuem a chave adequada para decifrá-las. Essa transformação é realizada por meio de algoritmos matemáticos que convertem o texto original (também conhecido como texto plano) em um texto cifrado, que é incompreensível sem o conhecimento necessário para reverter o processo. A criptografia é uma ferramenta crucial para a segurança da informação, proporcionando uma camada essencial de proteção contra o acesso não autorizado e garantindo a privacidade dos dados.

Para este exercício, foi-nos requisitado para considerarmos uma fórmula  **mod 29 com 0**

com a ser o último número de aluno de um dos 4 elementos do nosso grupo. Escolhemos o número 8230162 para o efeito, o que faz com que **.**

Após uma primeira analise do problema, achamos a questão muito parecida com a cifra de César, então optamos por utilizar a mesma para a solução do problema em questão. Criamos o nosso próprio alfabeto com a fórmula que nos foi dada, tendo esta resultado no seguinte alfabeto.

### 3.1.1. Alfabeto Cifrado

|  |  |
| --- | --- |
| **A- f(0)=(2\*0+2) mod 29 = 2** | **P- f(15)=(2\*15+2) mod 29 = 3** |
| **B- f(1)=(2\*1+2) mod 29 = 4** | **Q- f(16)=(2\*16+2) mod 29 = 5** |
| **C- f(2)=(2\*2+2) mod 29 = 6** | **R- f(17)=(2\*17+2) mod 29 = 7** |
| **D- f(3)=(2\*3+2) mod 29 = 8** | **S- f(18)=(2\*18+2) mod 29 = 9** |
| **E- f(4)=(2\*4+2) mod 29 = 10** | **T- f(19)=(2\*19+2) mod 29 = 11** |
| **F- f(5)=(2\*5+2) mod 29 = 12** | **U- f(20)=(2\*20+2) mod 29 = 13** |
| **G- f(6)=(2\*6+2) mod 29 = 14** | **V- f(21)=(2\*21+2) mod 29 = 15** |
| **H- f(7)=(2\*7+2) mod 29 = 16** | **W- f(22)=(2\*22+2) mod 29 = 17** |
| **I- f(8)=(2\*8+2) mod 29 = 18** | **X- f(23)=(2\*23+2) mod 29 = 19** |
| **J- f(9)=(2\*9+2) mod 29 = 20** | **Y- f(24)=(2\*24+2) mod 29 = 21** |
| **K- f(10)=(2\*10+2) mod 29 = 22** | **Z- f(25)=(2\*25+2) mod 29 = 23** |
| **L- f(11)=(2\*11+2) mod 29 = 24** | **.- f(26)=(2\*26+2) mod 29 = 25** |
| **M- f(12)=(2\*12+2) mod 29 = 26** | **,- f(27)=(2\*27+2) mod 29 = 27** |
| **N- f(13)=(2\*13+2) mod 29 = 28** | **!- f(28)=(2\*28+2) mod 29 = 0** |
| **O- f(14)=(2\*14+2) mod 29 = 1** |  |

Para a definição de cada valor temos de calcular os mod de certos números definidos pela função de

A função é:

Agora, vamos exemplificar com :

Como 2 já é menor que 29, ele permanece 2 quando dividido pelo módulo 29. Portanto. Seguimos estes cálculos até obter o alfabeto todo.

Após a realização desde processo, podemos substituir a frase que queremos criptografar, substituindo as respetivas letras pelos respetivos resultados numéricos que obtivemos.

### 3.1.2. Alfabeto Original

|  |  |
| --- | --- |
| **A- 0** | **P- 15** |
| **B- 1** | **Q- 16** |
| **C- 2** | **R- 17** |
| **D- 3** | **S- 18** |
| **E- 4** | **T- 19** |
| **F- 5** | **U- 20** |
| **G- 6** | **V- 21** |
| **H- 7** | **W- 22** |
| **I- 8** | **X- 23** |
| **J- 9** | **Y- 24** |
| **K- 10** | **Z- 25** |
| **L- 11** | **.- 26** |
| **M- 12** | **,- 27** |
| **N- 13** | **!- 28** |
| **O- 14** |  |

### 3.1.3. Alfabeto definido pela fórmula

|  |  |
| --- | --- |
| **A- f(0)=(2\*0+2) mod 29 = 2** | **P- f(15)=(2\*15+2) mod 29 = 3** |
| **B- f(1)=(2\*1+2) mod 29 = 4** | **Q- f(16)=(2\*16+2) mod 29 = 5** |
| **C- f(2)=(2\*2+2) mod 29 = 6** | **R- f(17)=(2\*17+2) mod 29 = 7** |
| **D- f(3)=(2\*3+2) mod 29 = 8** | **S- f(18)=(2\*18+2) mod 29 = 9** |
| **E- f(4)=(2\*4+2) mod 29 = 10** | **T- f(19)=(2\*19+2) mod 29 = 11** |
| **F- f(5)=(2\*5+2) mod 29 = 12** | **U- f(20)=(2\*20+2) mod 29 = 13** |
| **G- f(6)=(2\*6+2) mod 29 = 14** | **V- f(21)=(2\*21+2) mod 29 = 15** |
| **H- f(7)=(2\*7+2) mod 29 = 16** | **W- f(22)=(2\*22+2) mod 29 = 17** |
| **I- f(8)=(2\*8+2) mod 29 = 18** | **X- f(23)=(2\*23+2) mod 29 = 19** |
| **J- f(9)=(2\*9+2) mod 29 = 20** | **Y- f(24)=(2\*24+2) mod 29 = 21** |
| **K- f(10)=(2\*10+2) mod 29 = 22** | **Z- f(25)=(2\*25+2) mod 29 = 23** |
| **L- f(11)=(2\*11+2) mod 29 = 24** | **.- f(26)=(2\*26+2) mod 29 = 25** |
| **M- f(12)=(2\*12+2) mod 29 = 26** | **,- f(27)=(2\*27+2) mod 29 = 27** |
| **N- f(13)=(2\*13+2) mod 29 = 28** | **!- f(28)=(2\*28+2) mod 29 = 0** |
| **O- f(14)=(2\*14+2) mod 29 = 1** |  |

A seguinte frase:

Os estudantes da ESTG: Ruben, Pedro, Hugo, João, sugerem uma visita a Felgueiras

Torna-se em:

“19 1091113822811109 82 1091114: 7134102827 31087127 161314127 2012127 913141071026 13262 1518918112 2 12102414131018729”

Mas o processo não acaba aqui, ainda temos de encriptar os respetivos números que obtivemos através da fórmula com o alfabeto original, ou seja, o atual número alfabético terá de ser substituído pela letra do alfabeto original. Resultando na seguinte frase:

“Bj kjlnic!lkj ic KJLO: Hnek!, Dkihb, Qnob, Ubcb, jnokhk. n.c psjslc c Mkyonkshcj”

Para a seguinte frase:

As opções de visita incluem: Ver, Escapar, Saborear, Inspirar, Meditar, Encontrar e Viver!

Torna-se em:

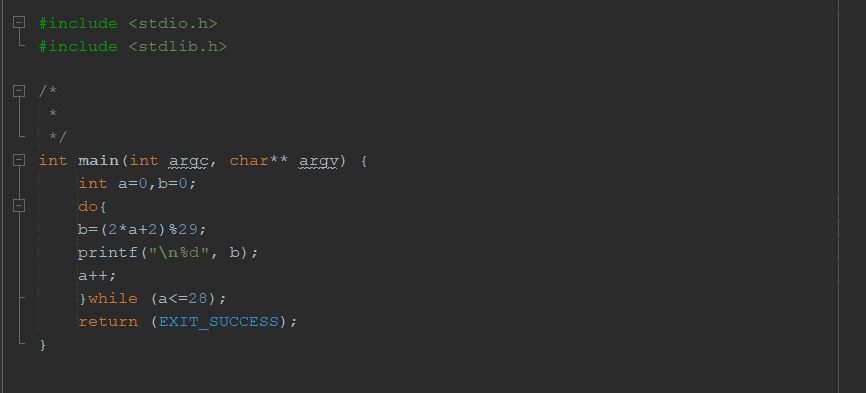
“29 1361109 810 1518918112 1828624131026: 1510727 1096232727 92417102727 1828931872727 2610818112727 102861281172727 10 151815107 0”

E mais uma vez, continuamos o processo fazendo a alteração numérica dos números obtidos na nossa nova frase, por letras do alfabeto original.

“Cj bdgbkj ik psjslc s!gynk.: Pkh, Kjgcdch, Jcebhkch, S!jdshch, .kislch, K!gb!lhch, k Pspkh a “

Por fim, obtemos finalmente as nossas duas frases desejadas encriptadas pela cifra de César, o que resulta numa cifra que à primeira vista é impossível de ser decifrada, tirando o facto que podemos reverter a cifra tendo acesso através dos cálculos matemáticos da inversa da nossa função.

Para chegar aos resultados obtidos usamos este script:





### 3.1.4. Inversão da Cifra de César

Sabendo que precisamos encontrar a inversa da nossa função, seguimos os seguintes passos para calcular a mesma e descobrir a função inversa.

1. Definir a função e a inversa

Dada a função , queremos encontrar uma função tal que

2. Escrever a equação

Queremos resolver para x na equação .

3. Isolar x

Primeiro, isolamos x:

Subtraímos 2 de ambos os lados:

4. Encontrar o inverso multiplicativo de 2 módulo 29

Para resolver x, precisamos dividir ambos os lados por 2. Em aritmética modular, isso significa multiplicar pelo inverso multiplicativo de 2 módulo 29. O inverso multiplicativo de a módulo m é um número b tal que:

Precisamos encontrar b tal que:

5. ()Usar o algoritmo de Euclides

Para encontrar o inverso multiplicativo de 2 módulo 29, usamos o algoritmo de Euclides:

O algoritmo de Euclides:

Rearranjamos para encontrar 1:

Aqui, vemos que o inverso multiplicativo de 2 é -14. Como trabalhamos com módulo 29, -14 é equivalente a 15 (pois ).

Portanto, o inverso multiplicativo de 2 módulo 29 é 15.

6. Multiplicar ambos os lados da equação pelo inverso

Agora multiplicamos ambos os lados da equação por 15:

Como , a equação se simplifica para:

7. Expressão final para a inversa

Portanto, a expressão final para a inversa da função é:

8. Verificação

Para confirmar que esta é a função inversa correta, substituímos na função original :

Substituindo na função :

Como :

E como :

Portanto, confirmando que é realmente a inversa correta de .

Para chegar ao resultado da inversão da cifra de césar utilizamos este script:

Uma imagem com texto, captura de ecrã, software, ecrã

Descrição gerada automaticamente



### 3.1.5. Alfabeto definido pela inversa da fórmula

Tendo a função , procedemos a criação do nosso alfabeto decifrador para a cifra criada.

|  |  |
| --- | --- |
| **0- = 28** | **15- = 21** |
| **1- = 14** | **16- = 7** |
| **2- = 0** | **17- = 22** |
| **3- = 15** | **18- = 8** |
| **4- = 1** | **19- = 23** |
| **5- = 16** | **20- = 9** |
| **6- = 2** | **21- = 24** |
| **7- = 17** | **22- = 10** |
| **8- = 3** | **23- = 25** |
| **9- = 18** | **24- = 11** |
| **10- = 4** | **25- = 26** |
| **11- = 19** | **26- = 12** |
| **12- = 5** | **27- = 27** |
| **13- = 20** | **28- = 13** |
| **14- = 6** |  |

## 3.2 Resolução do problema

A seguinte frase:

“Bj kjlnic!lkj ic KJLO: Hnek!, Dkihb, Qnob, Ubcb, jnokhk. n.c psjslc c Mkyonkshcj”

Convertemos os caracteres da frase encriptada pelos números da nossa função encriptador para começarmos a decifrar a cripta. Fazendo a conversão ficamos com o seguinte resultado.

“19 1091113822811109 82 1091114: 7134102827 31087127 161314127 2012127 913141071026 13262 1518918112 2 12102414131018729”

Utilizando agora a nossa função desencriptador, a inversa da nossa fórmula de encriptação, trocamos os números da frase anterior pelos novos números resultantes das fórmulas expostas na tabela anterior. Após isso, basta acedermos a tabela do Alfabeto Original e substituir os resultados das funções pelas letras obtendo assim o seguinte resultado:

Os estudantes da ESTG: Ruben, Pedro, Hugo, João, sugerem uma visita a Felgueiras

Para a segunda frase procedemos exatamente aos mesmos passos.

A seguinte frase:

“Cj bdgbkj ik psjslc s!gynk.: Pkh, Kjgcdch, Jcebhkch, S!jdshch, .kislch, K!gb!lhch, k Pspkh a “

Torna-se primeiramente:

“29 1361109 810 1518918112 1828624131026: 1510727 1096232727 92417102727 1828931872727 2610818112727 102861281172727 10 151815107 0”

E depois torna-se:

As opções de visita incluem: Ver, Escapar, Saborear, Inspirar, Meditar, Encontrar e Viver!

# 4. Conclusão

Neste trabalho de Matemática Discreta, explorámos três tópicos fundamentais: indução matemática, grafos e encriptação/desencriptação. Cada um destes tópicos desempenha um papel crucial em várias aplicações práticas e teóricas dentro da matemática.

Exercício 1:

A indução matemática é uma ferramenta poderosa para a prova de proposições. Este exercício é essencial para a validação de algoritmos e propriedades em diversas áreas da matemática.

Exercício 2:

A utilização da teoria de grafos na rota do Românico permitiu analisar os conceitos sobre os grafos não direcionados, caminhos, ciclos, arestas, vértices e a importância dos algoritmos de busca e otimização em grafos, principalmente o algoritmo dijkstra.

Exercício 3:

Por fim, abordámos os princípios de encriptação e desencriptação, fundamentais para a segurança da informação. Analisámos as técnicas de criptografia que asseguram a confidencialidade, integridade e autenticidade dos dados em ambientes digitais.

Em suma, este relatório destacou que não são apenas os fundamentos teóricos da indução matemática, dos grafos e do algoritmo de Dijkstra, e da cifra de César, mas também as suas aplicações práticas que abundam diversas áreas do conhecimento e da tecnologia. A Matemática Discreta, não é apenas um campo de estudo abstrato nem uma matemática básica, mas sim, é uma disciplina com profundas implicações práticas que moldam o nosso mundo moderno principalmente nas áreas tecnológicas que hoje estudamos no nosso curso.

# 5.Bibliografia

*chat gpt*. (s.d.). Obtido de chat gpt: https://chatgpt.com/

*Elemar JR*. (s.d.). Obtido de Elemar JR: https://elemarjr.com/clube-de-estudos/artigos/algoritmo-de-dijkstra-entendendo-o-caminho-minimo-em-grafos-ponderados/

*Google maps*. (s.d.). Obtido de Google maps: https://www.google.com/maps/@41.1787792,-8.5562968,12.92z?entry=ttu

*online gdb beta*. (s.d.). Obtido de online gdb beta: https://onlinegdb.com/nI6XH5oxQ