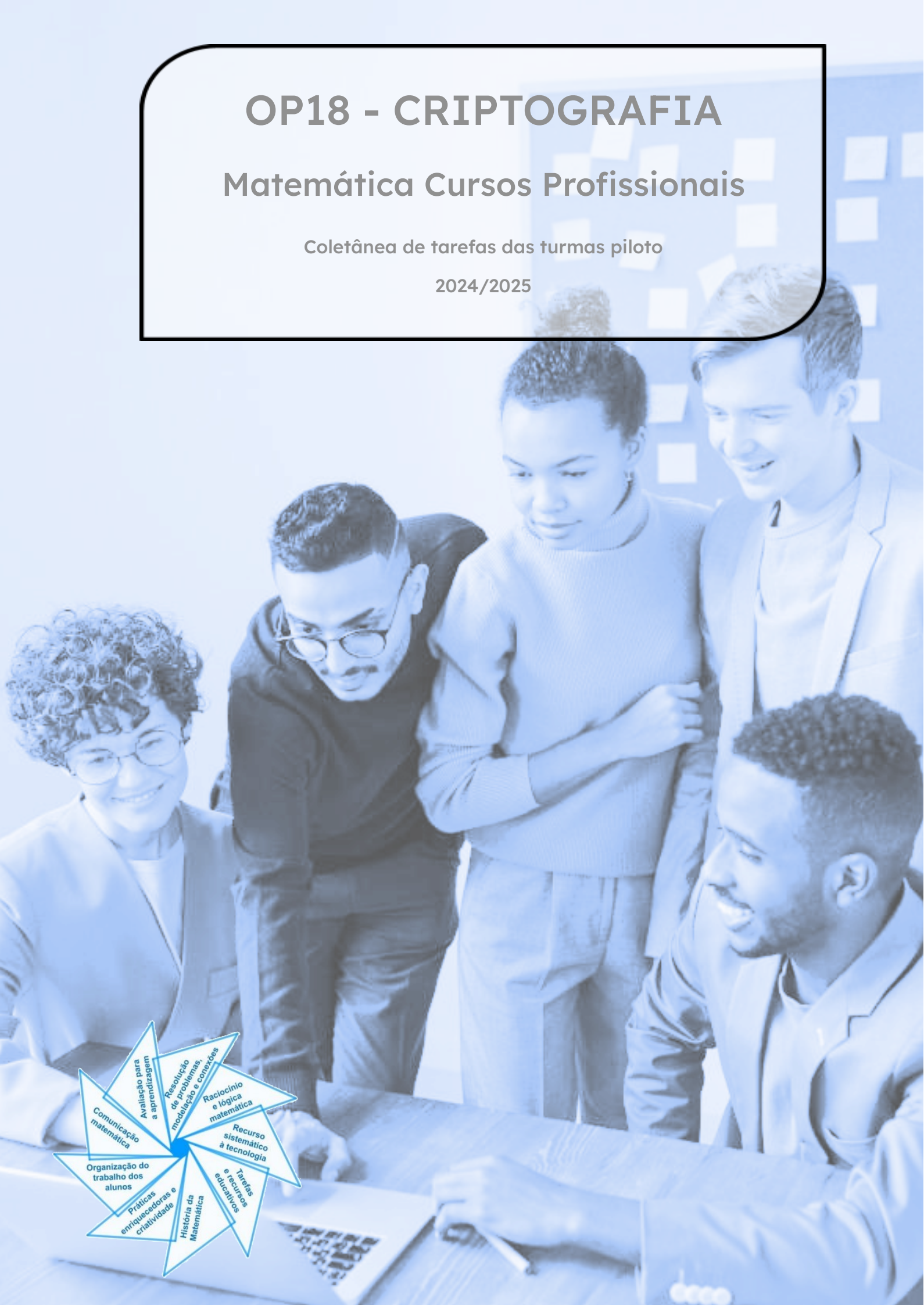
OP18 - CRIPTOGRAFIA

Matemática Cursos Profissionais

Coletânea de tarefas das turmas piloto

2024/2025



Ficha técnica

Título:

Coletânea de tarefas das turmas piloto - Criptografia (Matemática Cursos Profissionais)

Autoria e adaptação:

Professores das turmas piloto de Matemática Cursos Profissionais

Revisão:

Grupo de Trabalho de Desenvolvimento Curricular e Profissional de Matemática do Ensino Secundário

Imagem da capa:

Adaptada de imagem de utilização livre para fins não comerciais, disponível em https://www.pexels.com/pt-br/foto/foto-de-pessoas-olhando-no-laptop-3182750/

Data:

Lisboa, agosto de 2025

Nota de apresentação

A Direção-Geral da Educação (DGE) tem vindo a conceber e a concretizar um conjunto de atividades destinadas a apoiar a generalização dos programas (Aprendizagens Essenciais) de Matemática para os 10.°, 11.° e 12.° anos de escolaridade, designadamente nas disciplinas de Matemática A, Matemática B (Matemática Aplicada às Artes Visuais) e nos módulos de Matemática dos Cursos Profissionais.

É essencialmente no âmbito do **Grupo de Trabalho (GT) do Desenvolvimento Curricular e Profissional em Matemática para o Ensino Secundário (DCPMES)** que tais atividades têm sido apresentadas, pensadas, discutidas e planeadas. Integram este GT os docentes e investigadores Jaime Carvalho e Silva (Coordenador), Alexandra Rodrigues, Ana Breda, António Cardoso, António Domingos, Carlos Albuquerque, Cristina Cruchinho, Cristina Negra, Emanuel Martinho, Helder Manuel Martins, Hélia Jacinto, João Almiro, Luís Gabriel, Maria Eugénia Graça Martins, Maria Manuel Torres, Maria Teresa Santos, Nélia Amado, Nélida Filipe, Paulo Correia, Pedro Freitas, Pedro Macias Marques, Raúl Gonçalves, Rui Gonçalo Espadeiro e Susana Carreira.

As Coletâneas de Tarefas destinam-se a apoiar a implementação dos programas de Matemática já referidos. São materiais que foram na sua grande maioria testados em turmas piloto que se iniciaram no ano letivo de 2023/2024 e são acompanhados de alguns dos comentários motivados pela sua aplicação em sala de aula. Contudo, não substituem outros elementos de estudo e de consulta, mas constituem certamente referências de qualidade que, com certeza, ajudarão os professores de Matemática a aprofundar os seus conhecimentos sobre a natureza e as finalidades dos programas, sobre questões matemáticas, pedagógicas e didáticas ou sobre a conceção e o desenvolvimento de projetos. Neste sentido, são materiais que, passados pela prova essencial da realidade da sala de aula, podem apoiar os professores na seleção e na planificação de tarefas que mais facilmente concretizem as ideias inovadoras do currículo e envolvam os alunos em atividades matemáticas relevantes, empreendendo uma formação matemática abrangente e inovadora.

A aprendizagem de conceitos estruturantes e de competências essenciais dos alunos no âmbito da cidadania, implica disponibilizar aos alunos um conjunto variado de ferramentas matemáticas. Assim, aposta-se na diversificação de temas matemáticos, e das abordagens a cada tema, valorizando competências algébricas em paralelo com métodos numéricos e o raciocínio dedutivo a par do recurso à tecnologia. Estas Coletâneas de Tarefas pretendem oferecer exemplos muito concretos de forma a contribuir para esse objetivo.

Os professores das Turmas Piloto e os restantes elementos do GT DCPMES são professores, formadores e investigadores com percursos académicos e profissionais diversificados e significativos. Estas Coletâneas de Tarefas foram aplicadas num conjunto de turmas em escolas de Portugal Continental que aceitaram integrar a antecipação da aplicação das novas Aprendizagens Essenciais, com a preocupação de encontrar uma grande diversidade regional, com escolas localizadas em grandes centros urbanos e localizadas no interior, com turmas grandes e turmas pequenas, com alunos com condições socioeconómicas muito diferentes, dando garantia de uma melhor adequação aos alunos das escolas de hoje.

A testagem das tarefas agora publicadas é uma característica essencial do trabalho presente ao permitir uma reflexão sobre a aplicação prática das tarefas em salas de aula reais e um posterior refinamento dessas mesmas tarefas. Além do mais irão permitir, mais facilmente, uma aplicação a diferentes ambientes escolares e adaptações em diferentes direções, atendendo aos detalhes que emergiram da sua aplicação concreta. Os professores das turmas piloto e respetivas escolas/agrupamentos de escolas em 2024/2025 foram: Alexandra Ferrão (Agrupamento de Escolas Poeta António Aleixo), Ana Catarina Lopes (Escola Secundária Cacilhas Tejo), Ana Cristina Gomes (Agrupamento de Escolas Soares Basto), Cristina Cruchinho (Escola Secundária Filipa de Vilhena), Cristina Fernandes (Agrupamento de Escolas de Sampaio), Elisabete Sousa (Agrupamento de Escolas de Trancoso), Elisabete Sousa Almeida (Agrupamento de Escolas de Sátão), Elsa Gomes (Escola Secundária de Paços de Ferreira), Eunice Tavares Pita (Agrupamento de Escolas Gabriel Pereira), Hélder Manuel Martins (Escola Secundária António Damásio), Joaquim Rosa (Escola Secundária Luís de Freitas Branco), Maria Teresa Santos (Escola Profissional de Agricultura e Desenvolvimento Rural de Vagos), Marília Rosário (Escola Secundária de Tomaz Pelayo), Marisabel Antunes (Escola Secundária D. Dinis, Coimbra), Nélida Filipe (Agrupamento de Escolas Dra. Laura Ayres), Paula Teixeira (Escola Secundária João de Barros), Paulo Correia (Agrupamento de Escolas de Alcácer do Sal), Raul Aparício Gonçalves (Agrupamento de Escolas de Ermesinde), Rui Gonçalo Espadeiro (Agrupamento de Escolas de Redondo), Sandra Afonso (Escola Secundária José Saramago), Sara Faria Monteiro (Escola Secundária Pedro Nunes), Verónica Lopes (Agrupamento de Escolas Poeta António Aleixo).

A DGE tem vindo a desenvolver um processo de apoio sistemático e persistente aos professores de Matemática que iniciam em 2024/2025 a generalização dos novos programas de Matemática do Ensino Secundário, e que inclui, entre outras iniciativas: a dinamização de Turmas Piloto em mais de uma vintena de escolas; a edição de várias Coletâneas de Tarefas e outras brochuras; a formação de professores formadores que determina uma rede nacional de professores que, localmente, apoiam os seus colegas e desenvolvem ações de formação para todas as escolas; uma base de dados de tarefas novas ou já anteriormente publicadas e adequadas aos novos programas; e um conjunto de seminários a distância (*webinars*) dedicados a temas relevantes suscitados pelos novos programas.

Os desafios dos tempos modernos são significativos e por isso é fundamental que o currículo na escolaridade obrigatória dê resposta a todos os alunos, tendo em vista a sua formação matemática enquanto cidadãos, proporcionando-lhes uma experiência rica, adequada ao seu nível etário e ao alcance de todos, tendo o cuidado dos formalismos e dos níveis de abstração serem adequados ao trabalho a desenvolver em cada tema. A matemática deve ser um importante contributo para a resolução de problemas, possibilitando que os alunos mobilizem e desenvolvam o seu raciocínio com vista à tomada de decisões e à construção e uso de estratégias adequadas a cada contexto.

Finalmente, esperamos que as professoras e os professores de Matemática do ensino Secundário, bem como toda a comunidade, possam reconhecer utilidade nos materiais agora disponibilizados, quer no âmbito da planificação das suas atividades de ensino quer ainda como referências e instrumentos de reflexão, de autoformação e de desenvolvimento profissional. A DGE e o GT DCPMES, como lhes compete, não deixarão de continuar a

desenvolver esforços para apoiar e melhorar o desenvolvimento curricular na disciplina de Matemática. Para tal, continuamos a contar com os professores e com o seu profissionalismo empenhado, informado e consciente, elemento essencial e decisivo no processo de efetiva melhoria do ensino e da aprendizagem da Matemática.

Pelo GT DCPMES

Jaime Carvalho e Silva
Coordenador

MÓDULO OP18 - Criptografia

Aulas (Horas)	Nome da Tarefa	Tópicos/ Subtópicos	Objetivos de Aprendizagem	Tipo de trabalho	Ideias chave das AE	Áreas de Competência do PASEO
2	Tarefa 1 Importância da Criptografia no mundo atual	**Importância na criptografia no mundo atual** Usos atuais da criptografia. Perigos e dificuldades colocados pelo uso da criptografia	• Identificar alguns usos atuais da Criptografia. • Conhecer alguns problemas relacionados com as fragilidades/ dificuldades da Criptografia.	Trabalho de pares, com discussão em turma	• Comunicação matemática • Organização do trabalho dos alunos • Tarefas e recursos educativos	• Recorre à informação disponível em fontes documentais físicas e digitais; avalia, valida e organiza a informação recolhida (B) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)
2	Tarefa 2 O método de Júlio César	**O método de Júlio César** Funcionamento prático do método de Júlio César. Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens.	• Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens; referir o caso particular do método ROT - 13.	Trabalho de pares, com discussão em turma	• Comunicação matemática • Práticas enriquecedoras e criatividade • Tarefas e recursos educativos • História da Matemática	• Recorre à informação disponível em fontes documentais físicas e digitais; avalia, valida e organiza a informação recolhida (B) • Gere projetos e toma decisões na resolução de problemas e analisa criticamente as conclusões a que chega, reformulando, se necessário, as estratégias adotadas (C) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)

4	Tarefa 3 Variantes do método de Júlio César	**O método de Júlio César** Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens. Método ROT-13. Estratégias para decifrar uma mensagem cifrada pelo método de Júlio César quando não se conhece o valor da transposição alfabética.	• Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens; referir o caso particular do método ROT - 13. • Discutir possíveis estratégias para descodificar uma mensagem criptografada com o método de Júlio César, incluindo o uso da frequência das letras da língua usada na mensagem.	Trabalho em pequenos grupos, com discussão em turma	• Comunicação matemática • Recurso sistemático à tecnologia • Raciocínio e lógica matemática • Avaliação para a aprendizagem • História da Matemática	• Compreende, interpreta e comunica, utilizando linguagem matemática (A) • Gere projetos e toma decisões na resolução de problemas e analisa criticamente as conclusões a que chega, reformulando, se necessário, as estratégias adotadas (C) • Usa critérios para apreciar ideias, processos ou produtos, construindo argumentos para a fundamentação das tomadas de posição (D) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)
3	Tarefa 4 Método de Júlio César com Python	**O método de Júlio César** Estratégias para decifrar uma mensagem cifrada pelo método de Júlio César quando não se conhece o valor da transposição alfabética.	• Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens; referir o caso particular do método ROT - 13.	Trabalho em pequenos grupos, com discussão em turma	• Recurso sistemático à tecnologia • Tarefas e recursos educativos • Comunicação matemática • Avaliação para a aprendizagem	• Usa modelos para explicar um determinado sistema, para estudar os efeitos das variáveis e para fazer previsões acerca do comportamento do sistema em estudo (C) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E)

3	Tarefa 5 A Estatística decifra os métodos de Júlio César	**O método de Júlio César** Estratégias para decifrar uma mensagem cifrada pelo método de Júlio César quando não se conhece o valor da transposição alfabética.	• Discutir possíveis estratégias para descodificar uma mensagem criptografada com o método de Júlio César, incluindo o uso da frequência das letras na língua usada na mensagem.	Trabalho em pequenos grupos, com discussão em turma	• Resolução de problemas, modelação e conexões • Raciocínio e lógica matemática • Recurso sistemático à tecnologia • Organização do trabalho dos alunos • Comunicação matemática	• Compreende, interpreta e comunica, utilizando linguagem matemática (A) • Usa modelos para explicar um determinado sistema, para estudar os efeitos das variáveis e para fazer previsões acerca do comportamento do sistema em estudo (C) • Usa critérios para apreciar ideias, processos ou produtos, construindo argumentos para a fundamentação das tomadas de posição (D) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E)
2	Tarefa 6 O inseto dourado	**O método de Júlio César** Vantagens e fraquezas do método de Júlio César. Estratégias para decifrar uma mensagem cifrada pelo método de Júlio César quando não se conhece o valor da transposição alfabética.	• Conhecer a aplicar o método de Júlio César para codificar e descodificar mensagens; referir o caso particular do método ROT-13. • Discutir possíveis estratégias para descodificar uma mensagem criptografada com o método de Júlio César, incluindo o uso da frequência das letras na língua usada na mensagem.	Trabalho em pequenos grupos, com discussão em turma	• Resolução de problemas, modelação e conexões • Raciocínio e lógica matemática • Recurso sistemático à tecnologia • Organização do trabalho dos alunos • Comunicação matemática • História da Matemática	• Compreende, interpreta e comunica, utilizando linguagem matemática (A) • Gere projetos e toma decisões na resolução de problemas e analisa criticamente as conclusões a que chega, reformulando, se necessário, as estratégias adotadas (C) • Usa critérios para apreciar ideias, processos ou produtos, construindo argumentos para a fundamentação das tomadas de posição (D) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)

3	Tarefa 7 O Bastão de Licurgo	**Método de transposição** Estudo do bastão de Licurgo.	• Codificar e descodificar mensagens usando o método do Bastão de Licurgo.	Trabalho em pequenos grupos, com discussão em turma	• Resolução de problemas, modelação e conexões • Raciocínio e lógica matemática • Recurso sistemático à tecnologia • Tarefas e recursos educativos • Organização do trabalho dos alunos • Comunicação matemática	• Gere projetos e toma decisões na resolução de problemas e analisa criticamente as conclusões a que chega, reformulando, se necessário, as estratégias adotadas (C) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)
3	Tarefa 8 Método das Cercas de Linha de Comboio	**Método de transposição** Estudo do método de transposição usando cercas de linha de comboio (Rail Fenoe Cipher).	• Codificar e descodificar mensagens usando o método das Cercas de Linha de Comboio com 2 linhas.	Trabalho em pequenos grupos, com discussão em turma	• Resolução de problemas, modelação e conexões • Raciocínio e lógica matemática • Recurso sistemático à tecnologia • Tarefas e recursos educativos • Organização do trabalho dos alunos • Comunicação matemática	• Gere projetos e toma decisões na resolução de problemas e analisa criticamente as conclusões a que chega, reformulando, se necessário, as estratégias adotada (C) • Usa critérios para apreciar ideias, processos ou produtos, construindo argumentos para a fundamentação das tomadas de posição (D) • Trabalha em equipa e aprende a considerar diversas perspetivas e a construir consensos (E) • Compreende processos e fenómenos científicos que permitam a tomada de decisão (I)

Ao longo do módulo	Trabalho de Projeto Peddy Digital ou Exposição de Criptografia	Todos os tópicos	• Identificar alguns usos atuais da Criptografia. • Conhecer alguns problemas relacionados com as fragilidades/ dificuldades da Criptografia. • Conhecer e aplicar o método de Júlio César para codificar e descodificar mensagens; referir o caso particular do método ROT - 13 • Codificar e descodificar mensagens usando o método do Bastão de Licurgo. • Codificar e descodificar mensagens usando o método das Cercas de Linha de Comboio com 2 linhas.	Trabalho de grupo com apresentação final	• Raciocínio e lógica matemática • História da Matemática • Comunicação matemática • Organização do trabalho dos alunos • Avaliação para a aprendizagem	• Apresenta e explica conceitos em grupos, ideias e projetos dante de audiências reais, presenciais ou à distância (B) • Resolve problemas de natureza relacional de forma pacífica, com empatia e consentido crítico (E) • Domina a capacidade percetivo-motora (imagem corporal, direcionalidade, afinamento percetivo e estruturação espacial e temporal (J)

Tarefa 1

Importância da Criptografia no mundo atual

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa introduz-se o tema da criptografia com recurso a várias publicações de fácil acesso.

Conhecimentos prévios dos alunos: Noções de cibersegurança.

Materiais e recursos: Equipamento digital com acesso à internet.

Notas e sugestões:
Sugere-se que a aula inicie com a explicação do que se entende por criptografia solicitando que os alunos consultem, por exemplo, o dicionário *Priberam* e o *Infopédia* da Língua Portuguesa. Após uma breve introdução ao tema, os alunos devem aceder ao texto publicado pelo projeto "Público na Escola", na página da internet do jornal "Público" e visualizar o vídeo do Eng. José Eduardo Pina Miranda que se encontra no fim desse mesmo texto.
Seguidamente devem ler a notícia de 10 de outubro de 2024 da *Rádio Renascença* "Ataque informático afeta serviços do Estado" e explicar o que sucedeu.
É importante que no final da aula/tarefa o professor faça uma discussão em grande grupo para que os alunos percebam em que consiste a criptografia e a importância desta no mundo atual, bem como os perigos/riscos!!! e as dificuldades. Além disso, deve perceber se estes se apropriaram dos conceitos "criptografia", "ransomware" e "cibersegurança".

Tarefa 1

Importância da Criptografia no mundo atual

Segundo o dicionário Priberam e o Infopédia da Língua Portuguesa, a Criptografia é:

> Escrita secreta, em cifra, isto é, por meio de abreviaturas ou sinais convencionais.
>
> "criptografia", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2024, https://dicionario.priberam.org/criptografia.
>
> Surgiu da junção das palavras gregas “kryptós” (secreto) + “gráphé” (escrita) +-ia.

1. Consulta o texto publicado pelo projeto “Público na Escola”, na página da internet do jornal “Público” *https://www.publico.pt/publico-na-escola/interactivo-criptografia* e tenta responder às seguintes questões:

   1.1. Em que consiste a criptografia?

   1.2. Indica uma aplicação prática da criptografia.

   1.3. O que poderás fazer quando um pirata (“hacker”) está a espiar a linha de comunicação e a ler as tuas mensagens?

2. Visualiza o vídeo que está no final da notícia, do Eng. José Eduardo Pina Miranda, um reconhecido especialista em segurança de informação e criptografia, e indica algumas aplicações práticas da criptografia.

   A criptografia pode ser bem ou mal utilizada, conforme as intenções de quem a utiliza, como todas as ferramentas informáticas. Um dos maiores perigos atuais é o do “*Ransomware*”, em que o acesso aos dados de uma instituição ou empresa é bloqueado por piratas usando a criptografia baseada numa cifra que os piratas só cedem contra o pagamento de um resgate (“ransom”).

3. Lê a notícia de 10 de outubro de 2024 da Rádio Renascença “Ataque informático afeta serviços do Estado” e explica por palavras tuas o que aconteceu:

   https://rr.sapo.pt/noticia/pais/2024/10/10/ataque-informatico-afeta-servicos-do-estado/397028/

4. Procura num jornal português outra notícia recente sobre o mesmo tema, usando os termos de pesquisa: “criptografia”, “ransomware” ou “cibersegurança”.

Tarefa 2

O método de Júlio César

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa aborda-se o método de Júlio César numa perspectiva histórica e a sua importância na codificação e descodificação de mensagens. Pretende-se que os alunos apliquem este método na codificação e descodificação de mensagens.

Conhecimentos prévios dos alunos: Conhecimentos elementares da linguagem python.

Materiais e recursos: Equipamento digital com acesso à internet.

Notas e sugestões:
Sugere-se que a tarefa seja resolvida a pares ou em pequenos grupos e, que no final, em grande grupo, sejam discutidas as conclusões.
Caso os alunos não percebam o método de Júlio César sugere-se que o professor ilustre o mesmo recorrendo à figura 1 que se encontra na tarefa.

Tarefa 2

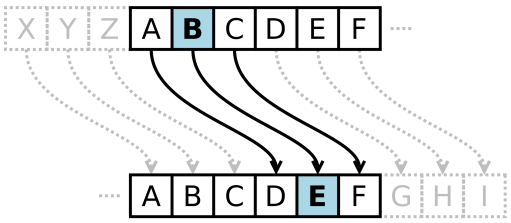
O método de Júlio César

O imperador romano Júlio César viveu entre os anos 100 a.C. e 44 a.C. e foi o responsável pela conquista da Gália (hoje França), de uma parte da Britânia (hoje Inglaterra) e uma parte da atual Alemanha. Para saber mais sobre este imperador podes ver o vídeo da RTP Ensina: https://ensina.rtp.pt/artigo/julio-cesar/

Para poder comunicar com os seus generais, Júlio César inventou um método para esconder as mensagens aos seus inimigos (embora possa ter usado ou adaptado um método já antes utilizado). Segundo um historiador romano antigo:

> Se ele tinha qualquer coisa confidencial a dizer, ele escrevia cifrado, isto é, mudando a ordem das letras do alfabeto, para que nenhuma palavra pudesse ser compreendida. Se alguém deseja decifrar a mensagem e entender o seu significado, deve substituir a quarta letra do alfabeto, a saber 'D', por 'A', e assim por diante com as outras.
>
> Suetónio, (2007). Os doze Césares. Lisboa, Assírio & Alvim.
> Wikipedia: https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar

Vejamos como funciona na prática o método de Júlio César. Podemos descrever o método como transformando cada letra da mensagem a codificar numa letra que esteja três posições mais à direita no alfabeto.



Suponhamos que queremos cifrar (codificar) a palavra CADA. Codificamos cada letra separadamente. Em vez da letra C escrevemos a letra F (três posições à direita), depois em vez da letra A escrevemos a letra D, em vez da letra D escrevemos a letra G e por fim a letra A já estava codificada como D. Assim, a codificação de CADA será FDGD e obtemos uma palavra que é, claramente, incompreensível.

1. Codifica a frase: “ATACAMOS DE NOITE” recorrendo ao método de Júlio César.
2. Se intersetarmos uma mensagem dos nossos adversários que tenha sido codificada usando o método de Júlio César, como poderemos tentar descodificar a mensagem?
3. Supõe que os nossos adversários aplicaram o método de Júlio César para enviar a mensagem secreta R QRYR OLGHU YDL VHU R ZDJQHU. Escreve a mensagem descodificada.
4. Inventa uma mensagem codificada pelo método de Júlio César, envia a um colega e pede-lhe que a descodifique.

Tarefa 3

Variantes do método de Júlio César

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa pretende-se dar a conhecer aos alunos variantes simples do método de Júlio César para codificar e descodificar mensagens, com especial ênfase no caso particular do método ROT-13, utilizando a apliqueta https://cryptii.com/pipes/caesar-cipher .

Conhecimentos prévios dos alunos: Método de Júlio César.

Materiais e recursos: Equipamento digital com acesso à internet.

Notas e sugestões:
Sugere-se que os alunos, em pares, iniciem a tarefa com a exploração da apliqueta https://cryptii.com/pipes/caesar-cipher e realizem o item 1.
Depois de perceberem bem o método de Júlio César, devem explorar a variante do método de Júlio César, o **método ROT-13**, e resolver o item 2. Podem não conseguir chegar à explicação da popularidade do método, mas o professor poderá sugerir aos alunos que experimentem o método ROT-13 duas vezes seguidas, o que provavelmente levará a que encontrem uma explicação.
Antes de passarem aos itens 3. e 4. o professor deverá, em grande grupo, discutir a exploração feita relativamente ao método de Júlio César e à sua variante.
A questão 4. pode ser realizada, como aprofundamento, com a utilização das 26 letras e dos 10 algarismos como base da codificação, caso em que a mensagem a decifrar poderia ser, por exemplo, uma destas:
`q pqxq nkfgt xck ugt q ycipgt` ou `x wx4x urmn0 4jr 1n0 x 5jpwn0`
Pode-se questionar os alunos acerca da razão pela qual não aparecem algarismos na primeira mensagem codificada apesar de usarmos 36 símbolos e não 26. Neste caso convém usar um descodificador que permita esta variante como https://planetcalc.com/8572/ .
No final da tarefa esta deverá ser apresentada e discutida em grande grupo ou, se se verificarem muitas dificuldades, no final de cada item.

Tarefa 3

Variantes do método de Júlio César

Ao longo da história foram desenvolvidos muitos métodos para codificar (cifrar) e descodificar (decifrar) mensagens secretas. Um dos métodos usados foi uma variação do método de Júlio de César em que as letras não eram deslocadas três posições mais adiante no alfabeto, mas um número diferente de posições.
Na apliqueta https://cryptii.com/pipes/caesar-cipher pode-se codificar e descodificar com facilidade uma mensagem usando o método de Júlio César com uma deslocação com qualquer número de deslocação de posições no alfabeto.

1. Usando a apliqueta https://cryptii.com/pipes/caesar-cipher, escolhe o número:

   1.1. 5 (na segunda quadrícula na coluna do meio) para o número de deslocações das letras no alfabeto e codifica a mensagem "ATACAMOS DE NOITE".

   1.2. 11 (na segunda quadrícula na coluna do meio) para o número de deslocações das letras no alfabeto e codifica a mensagem "ATACAMOS DE NOITE".

2. Uma variante muito popular do método de Júlio César é o chamado **método ROT-13**, em que as letras são deslocadas 13 posições no alfabeto. Acede à apliqueta https://rot13.com/ e codifica a palavra "MATEMATICA". Explica o resultado obtido e conjetura uma razão pela qual este método será tão popular.

3. O método de Júlio César e todas as suas variantes pertencem à categoria dos **métodos de substituição monoalfabética** em que cada letra do texto original é substituída por uma outra letra no texto codificado, sendo que em ambos os textos se usa o mesmo alfabeto.
   Os métodos de substituição podem não ser alfabéticos, sendo as letras substituídas por símbolos escolhidos previamente. Um código secreto célebre é o que foi decifrado por Sherlock Holmes na obra "The Dancing Men" (escrita por Sir Arthur Conan Doyle em 1903).

O código dos homens a dançar decifrado por Sherlock Holmes

Esta mensagem não é fácil de decifrar pois temos poucos carateres disponíveis. Consulta a página https://commons.wikimedia.org/w/index.php?curid=20287664, (em “abrir no visualizador dos media”) e descobre a mensagem que o Sherlock Holmes decifrou. Depois, poderás ler o livro com a aventura de Sherlock Holmes.

4. Supõe que os nossos adversários usaram uma variante do método de Júlio César, onde usamos as 26 letras do alfabeto e colocamos alguns algarismos como distratores para dificultar a decifração.
   Desta vez não sabemos quantas posições as letras estarão deslocadas no alfabeto. Como poderemos fazer para descodificar esta mensagem?

   V UV3V SPKLY 3HP ZLY V 4HNULY.

Tarefa 4

Método de Júlio César com Python

Notas pedagógicas para a ação do professor

Resumo:
Com esta tarefa pretende-se que os alunos usem a linguagem Python para programar o método de Júlio César e o método ROT-13.

Conhecimentos prévios dos alunos: Método de Júlio César e o método ROT-13.

Materiais e recursos: Calculadora gráfica ou computador e software Colab ou equivalente.

Notas e sugestões:
O professor deve iniciar a tarefa discutindo com os alunos de modo que estes interpretem, em linguagem corrente, e percebam os diversos passos descritos nos programas/códigos em Python, para que depois, de forma autónoma, resolvam os itens.
Os alunos deverão em pequenos grupos resolver a tarefa e o professor deve fomentar a discussão a partir da participação de todos os alunos, que explicarão as suas resoluções.
Podem surgir dificuldades na interpretação das linhas de comando do programa Python e em aceder à plataforma Colab, bem como na realização do item 2.3..

Tarefa 4

Método de Júlio César com Python

1. O programa seguinte encripta uma letra de cada vez. Podes aceder ao código em rot13.ipynb.

```
letra=input("Introduza uma letra para a encriptar: ")
c = ord(letra)  # obter o código numérico do carater
d=c+13
if d>122: # Verifica se o código ultrapassa 'z'
  d=d-26
e=chr(d) # Obter o carater correspondente a 'c'
print(e)
```

Descreve por palavras tuas o que faz este programa.

Nota: Podes consultar uma tabela com os códigos numéricos de cada carater em https://www.w3schools.com/charsets/ref_html_ascii.asp

2. Considera o seguinte programa em python:

```
texto=input("Utilizando apenas letras minúsculas, introduza a frase a encriptar: ")
def rot13(texto):
    l = len(texto)  # Obter o número de carateres
    code = ""
    for i in range(l):
        c = ord(texto[i])
        c = c + 13
        if c > 122:
            c = c - 26
        m = chr(c)
        code = code + m # Reconstrói a frase com os novos carateres
    return code
print(rot13(texto))
```

Copia o programa acima para a plataforma COLAB para responder às seguintes questões:

2.1. Descreve por palavras tuas o que faz este programa.

2.2. Modifica-o de modo a usar outro dos métodos do tipo de Júlio César.

2.3. Quais as modificações que terias de fazer ao programa para que pudesse descodificar mensagens em vez de codificar mensagens?

2.4. Usa o programa alterado para descodificar a seguinte mensagem

graf-dhr-rfghqne-zngrzngvpn

TAREFA 5

A Estatística decifra os métodos de Júlio César

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa os alunos terão que recorrer a métodos estatísticos para decifrar mensagens codificadas.

Conhecimentos prévios dos alunos: Frequência absoluta e frequência relativa. Método de Júlio César.

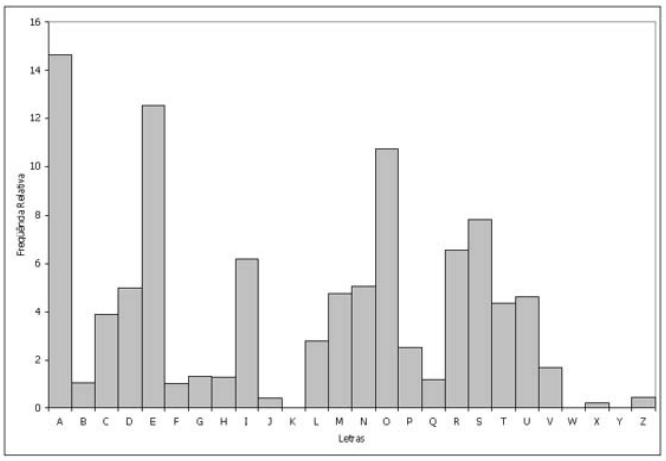
Materiais e recursos: Equipamento digital com acesso à internet.

Notas e sugestões:
O professor deve explicar a importância da Estatística para decifrar mensagens codificadas. Por exemplo, quando estamos perante um texto cifrado usando uma variante do método de Júlio César e não sabemos quantos lugares as letras foram deslocadas no alfabeto, a Estatística pode ajudar-nos, percebendo quantos lugares as letras foram deslocadas no alfabeto e recorrendo às estatísticas da frequência das letras perceber quais poderão ser algumas das letras originais do texto codificado.
É importante que o professor ajude a interpretar o item 1. de modo a que os alunos percebam que após descobrirem quais as duas letras mais prováveis escolham a melhor estratégia a seguir para decifrar os grupos de duas letras (digramas) e de três letras (trigramas) que são mais frequentes aparecerem combinados.
No item 2. os alunos devem decifrar o texto para que entendam a estratégia mais simples que é a de contar a frequência das palavras mais curtas no texto e comparar com a frequência das mesmas na língua portuguesa.
As conclusões dos itens 1. e 2. deverão ser apresentadas e discutidas em grande grupo.

TAREFA 5

A Estatística decifra os métodos de Júlio César

Quando estamos perante um texto cifrado usando uma variante do método de Júlio César e não sabemos quantos lugares as letras foram deslocadas no alfabeto, a Estatística pode ajudar-nos. Se for um texto escrito em língua portuguesa, então podemos recorrer às estatísticas da frequência das letras, para determinar quais poderão ser algumas das letras originais do texto codificado. Uma estatística que está disponível na Wikipedia é a indicada na figura seguinte.



Frequência das letras de um texto comum em língua portuguesa

https://commons.wikimedia.org/w/index.php?curid=553560

Observamos que as letras mais frequentes são o A, o E e o O e que as letras que mais aparecem a seguir são S, R e I.

Suponhamos que queremos descodificar o texto seguinte:

sl elyezd mfcczd xlyolyoz px szxpyd op tyepwtrpyntl bfp ld gpkpd qtnz apydlyoz bfp l mfcctnp p fxl ntpyntl alcl yãz qlkpcpd zqpydld p epcpd otld qpwtkpd ylz otrld efoz z bfp apydld xld apydl efoz z bfp otkpd otk lyezytz lwptiz

Podemos contar diretamente a frequência de cada letra, mas podemos também usar uma ferramenta na internet para o fazer.

1. Acede à apliqueta seguinte: decifrar mensagem

   Copia o texto anterior e cola-o no retângulo azul, escolhendo a opção “Calculate Letter Frequency!”.

   1.1. Quais as duas letras mais frequentes no texto?

   1.2. Em função dos dados obtidos, quais deverão ser as letras originais correspondentes a essas duas letras mais frequentes?

Nota: Observa que não conseguimos dizer exatamente quais são as letras originais. Apenas temos as duas letras mais prováveis. Assim, podemos seguir várias estratégias. Uma delas tem a ver com os grupos de duas letras (digramas) e de três letras (trigramas) que são mais frequentes aparecerem combinados. A página https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html fornece alguns dados para a língua portuguesa.

2. Vamos usar uma estratégia mais simples que é a de contar a frequência das palavras mais curtas no texto e comparar com a frequência das mesmas na língua portuguesa. A página que indicamos mostra a frequência das palavras com uma, duas e três letras na língua portuguesa. Há várias ferramentas, na internet, para fazer a contagem das palavras no nosso texto. Para simplificar vamos usar uma apliqueta idêntica à indicada/apresentada anteriormente: frequência das palavras.

   2.1. Usa a ferramenta dada para contar as palavras de uma, duas e três letras no texto dado. Qual é a letra mais frequente? Qual é a palavra de duas letras mais frequente? E a de três?

   2.2. Como o texto é pequeno, a maior parte das palavras só aparece uma vez, tornando-se complicado comparar com as frequências das mesmas na língua portuguesa. No texto, há uma palavra que aparece quatro vezes e que é também a mais frequente na língua portuguesa. Qual é essa palavra?

   2.3. A conclusão a que chegaste em 2.2. é compatível com a conclusão de 1.2.? O que podes concluir?

   2.4. A partir do que concluíste em 2.3., consegues decifrar o texto dado? Se sim, decifra-o.

TAREFA 6

O inseto dourado

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa pretende-se que os alunos, com recurso à linguagem Python, descodifiquem mensagens, pelo Método de Júlio César, quando se conhece ou desconhece a rotação introduzida no alfabeto e percebam também que a criptografia é utilizada na literatura.
É uma tarefa que pode se tornar interdisciplinar e servirá de consolidação.

Conhecimentos prévios dos alunos: Método de Júlio César e linguagem Python.

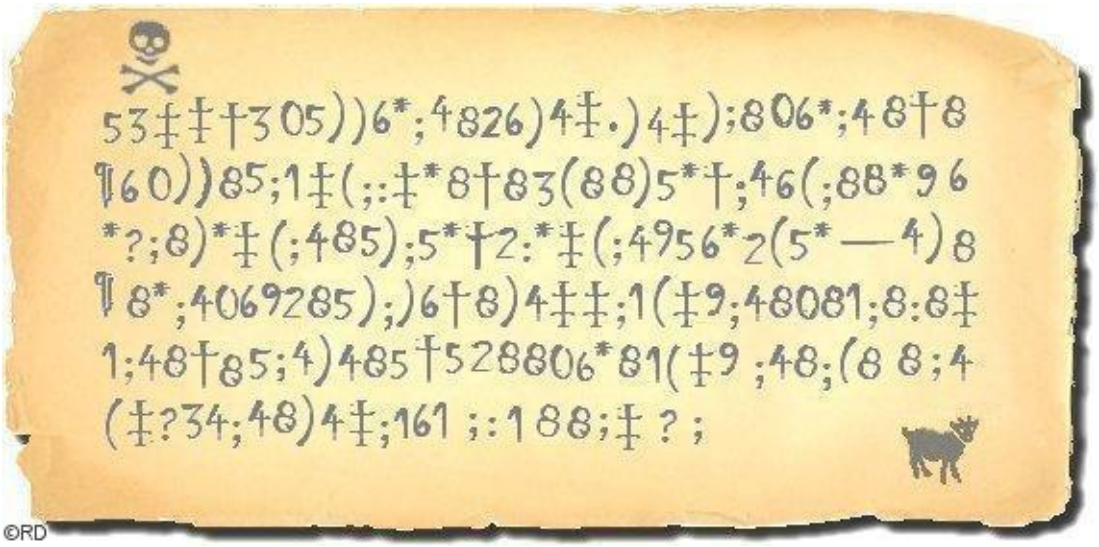
Materiais e recursos: Equipamento digital com acesso à internet. Calculadora gráfica ou computador com acesso ao Colab ou equivalente.

Notas e sugestões:
Esta tarefa deverá ser resolvida em pequenos grupos.
Poderá haver a necessidade de o professor apoiar a interpretação do programa Python do item 4.1..

TAREFA 6

O inseto dourado

Durante o século XIX, Edgar Allen Poe aproveitou a popularidade da criptografia e escreveu o conto "The Gold Bug", publicado em 1843. Neste, o personagem principal, William Legrand, acidentalmente descobre uma mensagem secreta, escrita em tinta invisível, num pedaço de papel que tinha utilizado para ilustrar o inseto dourado ao seu amigo, o narrador. Legrand acaba por mostrar ao amigo a mensagem e explica como a conseguiu decifrar.



A mensagem encriptada encontrada por Legrand

Fonte: https://www.ciphermachinesandcryptology.com/en/goldbug.htm

1. Decifra a mensagem anterior. Podes recorrer a pesquisas na Internet.

2. Visualiza os vídeos: "Xiu ... é segredo" e "A Matemática das Letras" e descreve a estratégia utilizada tanto no conto como nos vídeos para decifrar mensagens encriptados por métodos de substituição?

3. De acordo com os métodos de substituição que estudaste até ao momento, apresenta algumas fragilidades destes métodos, como por exemplo o de Júlio César, na encriptação de mensagens?

4. Os alunos do 11.º ano após estudarem o método de Júlio César decidiram usar este método para comunicarem entre si. No entanto, um dos alunos, o Santiago, reparou que os seus amigos andavam a comportar-se de uma forma estranha e

que lhe estavam a esconder algo. Um dia ele descobriu uma mensagem encriptada que um dos amigos deixou cair.
A mensagem era a seguinte:

xwklskmjhjwkshsjsgsfanwjksjagvgesjughgflgvwwfugfljgksts vgsknaflwwvmskwljaflsfsusksvsbgsfstjmfgwfusjjwymwvwljsr wjgesjug

Como tinham acabado de estudar o método de Júlio César na aula de Matemática, o Santiago pensou que a mensagem tinha sido encriptada por este método, mas não sabe qual foi a rotação do alfabeto utilizada.

4.1. O Santiago lembrou-se que numa aula de Matemática tinha criado um programa em linguagem Python, no Colab para descodificar mensagens que tinham sido encriptadas pelo Método de Júlio César, com uma rotação fixa do alfabeto.
O Programa é o seguinte:

```
texto=input("Utilizando apenas letras minúsculas, introduza o texto encriptado. Não utilizes pontuação, acentos nem espaços entre as palavras. ")
n=len(texto)
code=""
for i in range(n):
  c=ord(texto[i])
  c=c-3
  if c<97:
    c=c+26
  m=chr(c)
  code=code+m
print(code)
```

Altera o programa do Santiago para que possa ser utilizado para qualquer rotação do alfabeto.

4.2. O Santiago tentou descobrir a rotação do alfabeto utilizada por tentativa e erro e rapidamente chegou à conclusão de que não é muito prático. Decidiu então contar a frequência absoluta de cada letra no texto, utilizando para o efeito a seguinte aplicação http://www.writewords.org.uk/word_count.asp para descobrir qual é a rotação do alfabeto utilizada.

4.3. Utiliza o programa de descodificação do item 4.1. para verificar a chave e decifrar a mensagem.

4.4. Codifica uma mensagem, usando a rotação do alfabeto que quiseres. Troca a tua mensagem com outro grupo. Utiliza os programas construídos anteriormente para descobrires qual é a rotação do alfabeto utilizada e decifrares a mensagem que recebeste de outro grupo.

TAREFA 7

O Bastão de Licurgo

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa pretende-se apresentar aos alunos a história do Bastão de Licurgo, as suas vantagens e desvantagens. Além disso, os alunos serão incentivados a descodificar/codificar usando este método de transposição.

Conhecimentos prévios dos alunos: Posicionamento das 26 letras do alfabeto português.

Materiais e recursos: Equipamento digital com acesso à internet e alguns cilindros para exemplificar o método do Bastão de Licurgo.

Notas e sugestões:
Esta tarefa é a primeira com um novo método de codificação, o de transposição, em que os carateres da mensagem original são apenas recolocados em diferentes posições (transpostos).
O professor deve levar vários cilindros para exemplificar o método do Bastão de Licurgo.
Após os alunos consultarem a página sobre os Métodos Manuais de Substituição e Transposição o professor pode passar o pequeno vídeo do episódio "Isto é Matemática" que se encontra em https://www.youtube.com/watch?v=5W8iHMKFAoc. Desta forma a resolução dos itens 1. e 2. será mais fácil.
As conclusões dos itens 1. e 2. deverão ser apresentadas e discutidas em grande grupo.

TAREFA 7

O Bastão de Licurgo

O método para impedir os inimigos de ler as mensagens, usado em Esparta, Grécia, há centenas de anos atrás é muito curioso: à volta de um bastão de diâmetro dado, enrola-se uma fita de material de escrita (pergaminho ou couro, por exemplo) e a escrita é feita longitudinalmente, ao longo do bastão.

Bastão de Licurgo

Fonte: CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1698345

1. Descodifica a seguinte mensagem onde foi o usado o método do Bastão de Licurgo:

AEVBIEDLAA

Podes usar um esquema como o seguinte, tendo de determinar se, de acordo com o raio do cilindro do bastão (que desconheces), conseguirás colocar duas, três ou quatro letras de cada vez à volta do cilindro:

	I	a	m	h	u	
__	r	t	v	e	r	__
	y	b	a	d	l	
	y	h	e	l	p	

Um esquema do bastão de Licurgo com quatro letras transversais ao bastão e cinco longitudinais.

2. Codifica a seguinte mensagem, aplicando o método do Bastão de Licurgo:

"eu sou um detetive"

TAREFA 8

Método das Cercas de Linha de Comboio

Notas pedagógicas para a ação do professor

Resumo:
Nesta tarefa os alunos serão incentivados a descodificar/codificar usando o método de transposição das Cercas de Linha de Comboio.

Conhecimentos prévios dos alunos: Posicionamento das 26 letras do alfabeto português.

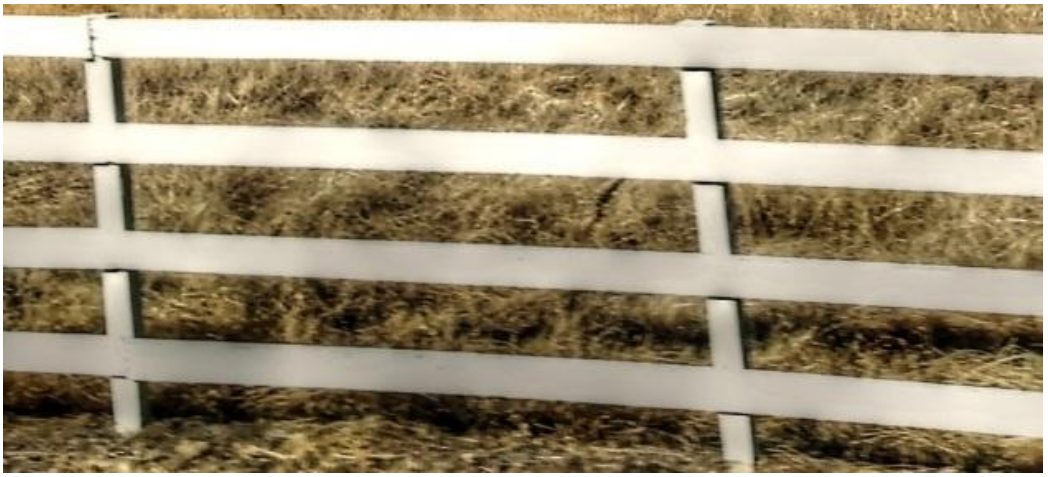
Materiais e recursos: Equipamento digital com acesso à internet.

Notas e sugestões:
Este é um método relativamente simples pelo que é expectável que os alunos consigam realizar a tarefa sem grande ajuda do professor.
O método e as conclusões dos itens 1. e 2. deverão ser apresentadas e discutidas em grande grupo.

TAREFA 8

Método das Cercas de Linha de Comboio

Este é um método de transposição em que se altera a ordem das letras para esconder a mensagem. Este método foi buscar o nome às cercas comuns junto a linhas de comboio e explorações agrícolas onde o gado anda livremente.



Cerca By Linnaea Mallette

Fonte: https://commons.wikimedia.org/w/index.php?curid=120894457

O Método das Cercas de Linha de Comboio, também chamado de método Zig Zag, é usado escrevendo o texto que se quer esconder diagonalmente num certo número de linhas horizontais ora para baixo ora para cima. Por exemplo, se quisermos esconder a mensagem VAMOS FUGIR NA SEXTA À MEIA NOITE escrevemos o seguinte, numa cerca com quatro linhas horizontais:

V . . . . . U . . . . . S . . . . . M . . . . . I . .
. A . . . . F . G . . A . E . . . A . E . . . O . T .
. . M . S . . . I . N . . . X . A . . . I . N . . . E
. . . O . . . . . R . . . . . T . . . . . A

- **Decifra** a mensagem seguinte que foi codificada com o Método das Cercas de Linha de comboio com três linhas horizontais:

  NODOTU OFMSECBROFJM SOSESA

- Codifica a mensagem seguinte utilizando uma cerca de três linhas horizontais.

  O PRESIDENTE VAI CHEGAR ANTES DAS DOZE

Trabalho de Projeto

Peddy Digital ou Exposição de Criptografia

Notas pedagógicas para a ação do professor

Resumo:
Pretende-se desafiar os alunos a organizarem um Peddy Digital na sua escola ou a fazer um póster sobre criptografia para uma exposição a realizar na escola com todos os pósteres.

Conhecimentos prévios dos alunos: Tópicos abordados ao longo do módulo.

Materiais e recursos: Internet.

Notas e sugestões:
Esta tarefa pode ser proposta no início da lecionação deste módulo. O professor pode propor aos alunos dois trabalhos distintos: I) organizarem um peddy digital, tendo em conta os tópicos estudados ou outros de outras disciplinas ou II) criarem um póster.
O professor deve apresentar a tarefa e explicar todas as etapas e prazos a cumprir, assim como critérios de avaliação. Ao longo das aulas, o professor deve acompanhar o trabalho que os alunos estão a desenvolver, dando-lhes feedback de aspetos a melhorar.
No final do módulo, o professor deve, na sua planificação modular, contemplar tempos de aulas destinados à apresentação do trabalho desenvolvido, ou para a preparação e organização do dia do peddy digital que se irá realizar na escola ou ainda para a apresentação pública da exposição dos pósteres.

Trabalho de Projeto

Peddy Digital ou Exposição de Criptografia

Ao longo deste módulo vais ter ou tiveste a oportunidade de conhecer o tópico da criptografia, a sua importância, bem como vários métodos para codificar ou decifrar enigmas, sozinho ou com os teus colegas.

Assim, são propostos dois desafios:

I) Organizares um peddy digital na tua escola;

II) Preparares uma exposição de Criptografia (Cria o teu póster).

Para que consigas concretizar um dos desafios propostos, tem em conta as seguintes sugestões:

I) Peddy Digital

Sugestões para a organização do Peddy Digital:

Primeira fase:

- Seleciona os pontos da escola onde devem ser colocados os postos com os desafios.
- Para cada posto cria um desafio utilizando os métodos de criptografia estudados.
- No Google Apps cria o Peddy Digital.
- Cria para cada posto um QR code onde os participantes poderão ver os desafios.
- Caso não disponhas dos materiais que considerares necessários na tua escola, deves construí-los.

Segunda fase:

Organiza o peddy digital.

- Deves divulgar as regras do peddy digital, assim como a sua descrição.
- Define e divulga as datas para as inscrições e para a realização do peddy digital.
- Cada grupo de alunos participantes não deve exceder os 4 elementos.
- Em cada posto deve estar alguém para facultar o QR code e validar as respostas.

- No final, podes organizar uma cerimónia para divulgação do grupo vencedor.
- Podes divulgar o evento nas redes sociais da tua escola.

II) Exposição de Criptografia (Criares o teu póster).

Neste projeto deverás estudar outros métodos de criptografia.

Atenção: o trabalho tem de ser original. Quando escreveres algo que não seja da tua autoria, deves referir sempre a fonte de onde foi retirado.
A tarefa atribuída a cada grupo é a elaboração de um póster onde deverá constar:

1. Identificação
   - Título do projeto;
   - Nome dos elementos do grupo (2 a 3 elementos).

2. Contextualização
   - Enquadramento histórico: breve descrição da época em que o método surgiu e do inventor do método;
   - Apresentação e breve descrição do método;

3. Enquadramento Matemático
   - Descrição matemática, concisa e compreensível, do método.
   - Demonstração concreta do método, codificando e decodificando mensagens;
   - Explicação dos conceitos matemáticos que intervêm para obter os resultados;
   - Uso de vocabulário matemático adequado.

   Nota importante: Esta secção (Enquadramento Matemático) é obrigatória pois é a que terá um peso maior na avaliação do projeto.

4. Curiosidades (opcional)
   - Factos interessantes sobre o método e o seu criador.

Não podem existir grupos que escolham o mesmo método.
Cada grupo apresentará o trabalho final à turma.

Nota:

Em ambos os desafios (I ou II) deverás elaborar uma pequena reflexão individual sobre o trabalho que realizaste. Tópicos a abordar:

- o que aprendeste com este projeto;
- o que mais gostaste;
- quais foram as dificuldades que enfrentaste e como as superaste;
- qual foi o teu contributo no trabalho de grupo;
- como foi a distribuição do trabalho pelos elementos do grupo e a respetiva participação no desenvolvimento do projeto;
- faz uma apreciação global do projeto;
- qual foi o teu grau de satisfação com o trabalho realizado.