Mestrado Matemática e Aplicações, Universidade Agostinho Neto			
2020/2021	**Introdução à Criptografia**	**Exame Normal**	**11/8/2021**

Nota: Identifique correctamente a sua prova.

1. Os dois sistemas de encriptação actualmente usados são designados por *Cifras de Chave Secreta* e *Cifras de Chave Pública*.

   (a) Quais são os pontos positivos e negativos de ambas as aproximações?

   (b) Como é que se poderão combinar para melhor aproveitar os pontos positivos de ambos os sistemas?

2. Demonstre que as cifras de *Deslocamento Simples* e de *Vigenère* são na verdade cifras.

Resolução

1. (a) **Vantagens e Desvantagens das Cifras de Chaves Simétricas (slide 17)**

   - **Podem ser concebidas para terem uma velocidade de processamento de dados elevada.**
   - As chaves são relativamente pequenas.
   - Cifras deste tipo podem ser usadas como primitivas em vários tipos de ferramentas criptográficas
   - São facilmente componíveis de forma a construir sistemas criptográficos mais seguros.
   - Têm um largo historial, e como tal já foram muito, e extensivamente, estudadas.

   Desvantagens das Cifras de Chaves Simétricas

   - **As chaves entre todas as entidades envolvidas numa comunicação têm de ser mantidas secretas.**
   - Se o número de entidades envolvidas for elevado o número de pares de chaves a considerar é também elevado.
   - As chaves têm de ser mudadas muito frequentemente.

   Vantagens e Desvantagens das Cifras de Chaves Públicas (slide 24)

   Vantagens das Cifras de Chaves Públicas

   - **Só a chave privada deve permanecer secreta.**
   - As chaves podem ser mantidas por largos períodos de tempo.
   - Mesmo que o número de entidades envolvidas seja elevado o número de chaves permanece baixo (comparado com as chaves simétricas).

   Desvantagens das Cifras de Chaves Públicas

   - A autenticidade das chaves públicas tem de ser, de alguma forma, assegurado.
   - **São consideravelmente mais lentos que os sistemas de chaves simétricas no que diz respeito ao processamento da informação.**
   - O comprimento das chaves é em geral bastante maior do que nos sistemas de chaves simétricas.
   - A segurança destes sistemas é baseada em assumpções (ainda não demonstradas) sobre dificuldade computacional de certo tipo de problemas.
   - O seu historial é recente (década de 1970).

   (b) A utilização de uma cifra de chave pública (boa gestão de chaves) como passo inicial para estabelecer a comunicação e fazer a geração e troca de chaves simétricas, passando depois a utilizar uma cifra de chaves simétricas (eficiente), permite combinar os pontos positivos de ambos os tipos de cifras.

2. Ambas as cifras baseam-se em operações aditivas em aritmética modular. Dado que para qualquer $m \in \mathbb{N}$, $(\mathbb{Z}_m, +)$ é um grupo Abeliano, então tem-se que todos os elementos têm inverso, o simétrico de $[a]_m$ é $[-a]_m = [m-a]_m$ (slide 48). Conclui-se então que $D_k(E_k(x)) = E_k(D_k(x)) = x$