Mestrado Matemática e Aplicações, Universidade Agostinho Neto			
2020/2021	**Introdução à Criptografia**	**Exame Normal**	**2/8/2021**

1. Os sistemas de chave pública distinguem-se dos sistemas de chave privada na forma como fazem a gestão das suas chaves de cifração.

   Aparentemente os sistemas de chave pública resolvem completamente o problema da troca de chaves entre entidades. Infelizmente isso não é totalmente correcto dado que estes sistemas permitem um tipo de ataque designado por **personificação**, o qual permite quebrar o protocolo.

   Explique de forma breve o ataque de personificação ao protocolo de troca de chaves de cifração para uma cifra de chave pública.

2. Um dos ataques possíveis, para uma qualquer cifra, é o ataque por procura exaustiva no espaço das chaves. Ou seja tenta-se, de forma exaustiva, todas as chaves possíveis.

   Calcule para as cifras seguintes a dimensão do espaço das chaves (com $\mathcal{A}$, $|\mathcal{A}| = 43$, o alfabeto e $K \in \mathcal{K}$ a chave usada na encriptação):

   (a) $E_K^1(x) = (x + K) \mod |\mathcal{A}|$.
   (b) $E_K^2(x) = (ax + b) \mod |\mathcal{A}|, \quad K = (a, b)$.

Resolução

1. Dado que para se encriptar uma mensagem, para um dado destinatário, é necessário obter a sua chave pública, a validação da origem da chave é crucial, se alguém se interpuser entre o emissor e o destinatário pode-se fazer passar pelo destinatário, ataque de personificação, e enviar ao emissor a sua chave pública, em vez da chave pública do destinatário, comprometendo deste modo a comunicação entre o emissor e o destinatário.

2. Dimensão do espaço das chaves.

   (a) A dimensão do espaço das chaves é $|\mathcal{A}| - 1$, isto é o número de classes de congruência módulo a dimensão do alfabeto. Embora se possa considerar que qualquer número natural é uma potencial chave, só há $|\mathcal{A}|$ chaves diferentes, isto é o número de classes de congruência módulo $|\mathcal{A}|$.

   Resp: $|\mathcal{A}| = 43$ (slide 88), ou 42, se se considerar que o zero não é uma chave significativa.

   (b) Dado que $|\mathcal{A}| = 43$ é um número primo, isto é, $(\mathbb{Z}_{43} \setminus \{[0]_{43}\}, \cdot)$ é um grupo, isto é para todos os a é possível ter o seu inverso.

   A dimensão do espaço das chaves é dada por: $\phi(|\mathcal{A}|) \times |\mathcal{A}| + |\mathcal{A}|$, como $\phi(|\mathcal{A}|) = n - 1$, temos: $(|\mathcal{A}| - 1) \times |\mathcal{A}| + |\mathcal{A}|$.

   Resp: $(|\mathcal{A}| - 1) \times |\mathcal{A}| + |\mathcal{A}| = 42 \times 43 + 43 = 1849$ (slide 88). ou $42 \times 42 + 42 = 1806$, se se considerar que o zero não é uma chave significativa.