**Primeiro teste de Criptografia Aplicada**

**3 de novembro de 2022** **18h00m – 19h30m**

---

**1.0** **1:** Explique qual é a diferença entre uma cifra segura sob o ponto de vista da teoria da informação (*information-theoretic security*) e uma cifra segura sob o ponto de vista computacional (*computational security*).

**1.0** **2:** O conceito de difusão, ou efeito de avalanche, é fundamental para a concretização de funções de cifra simétricas e para o desenho de funções de síntese (*digest*). Em relação a estas últimas funções, explique de que forma esse conceito se revela na sua utilização prática.

**1.0** **3:** As máquinas de rotores, como a Enigma, concretizam cifras polialfabéticas que tipicamente não permitem a sua criptanálise usando o teste de Kasiski ou o índice de coincidência. Explique porquê.

**1.0** **4:** A máquina de cifra contínua (*stream*) Lorenz foi criptanalizada graças a um erro de um operador, que fez algo que nunca se deve fazer com a maioria das cifras contínuas. Explique que erro foi esse, e que o mesmo permite (e permitiu).

**1.0** **5:** Considere os modos de cifra ECB (*Electronic Code Book*) e CTR (*Counter*). Tendo em conta o seu uso em ambiente real, indique duas características que os diferenciam sob o ponto de vista de um observador externo (ou seja, sem considerar as diferenças do seu modo interno de funcionamento).

**1.0** **6:** O protocolo Diffie-Hellman pode ser implementado usando curvas elípticas. Explique como e indique qual é o problema matemático que o torna "seguro".

**1.0** **7:** O sistema criptográfico RSA pode ser usado para cifrar uma mensagem. Explique como. Qual é o problema matemático que o torna criptograficamente "seguro"?

**1.0** **8:** O sistema criptográfico RSA também pode ser usado para assinar uma mensagem, isto é, para atestar, desde que sejam tomadas as precauções devidas, que uma messagem não foi forjada por outro que não o remetente. Explique como.

**1.0** **9:** Num sistema RSA em que o expoente usado para cifrar uma mensagem é sempre 3 e em que não se usa *padding* aleatório, enviar a mesma mensagem $m$ para três destinatários diferentes, com chaves públicas $(n_1, 3)$, $(n_2, 3)$ e $n_3, 3)$, é altamente desaconselhado, já que se as três mensagens cifradas, $m^3 \bmod n_1$, $m^3 \bmod n_2$ e $m^3 \bmod n_3$, forem intercetadas é possível recuperar a mensagem original. Explique como. [Pista: lembre-se do Chinês...]

**1.0** **10:** Explique como se pode multiplicar eficientemente um ponto de uma curva elíptica por um número inteiro positivo.