Teste Modelo

1. No contexto das cifras simétricas clássicas, comente a seguinte frase: “resistência a um ataque por procura exaustiva não é condição suficiente para obter segurança”.

2. No caso da cifra Vigenère, explique porque é que o crescimento do espaço de chaves usualmente implica o acesso a uma maior quantidade de informação cifrada.

3. Explique o porquê da seguinte frase: nenhuma cifra simétrica determinística pode, num cenário de ataque que contemple múltiplas mensagens, ser segura contra adversários passivos.

4. Recorde a definição de One-Time Pad, e gerador de números pseudoaleatórios (PRNG). Se na primeira, se substituir a chave (perfeitamente aleatória, e de tamanho igual à mensagem), por uma sequência pseudo-aleatória, acha que se continua a ter segurança perfeita? Justifique.

5. Os Message Authentication Codes são suficientes para evitar ataques por repetição? Se respondeu que não, como faria para, em conjunto com um MAC, os evitar?

6. Considere o ataque “padding oracle”. Como sabe, este ataque consiste no facto de ser possível quebrar o modo mac-then-encrypt, se for possível distinguir entre dois tipos de erros (erros de padding (i.e. um erro de decifragem) vs. erros de verificação do MAC). Como alteraria o protocolo, de modo a tornar este ataque inviável?

7. Comente a seguinte afirmação: no mundo da criptografia assimétrica, o adversário tem sempre acesso a um oráculo de cifragem.

Nota 1: este documento meramente pretende esboçar o tipo questões que serão colocadas. *Mas não tem em conta a duração do teste.*

Nota 2: para desencorajar os alunos de guiarem o seu estudo pelas questões acima colocadas, o docente terá bastantes reticências em responder a dúvidas sobre as mesmas…