Instituto Superior de Engenharia de Lisboa
MEIC, MEIM, MEETC
Cibersegurança
Exame Tipo

Grupo 1 - Mecanismos para proteção da informação [6 valores]

1. [2,0] Considere uma cifra *round* por blocos de 2 bytes definida pela composição das cifras: C_1, cifra por blocos de 2 bytes definida pela troca de posição do byte esquerdo e direito; C_2, cifra de substituição que consiste em identificar cada byte com um par de elementos (x,y) de Z_{16} e realizar a transformação (x,y)->(5x,x+y) em Z_{16}. Determine o texto cifrado com esta cifra *round,* usando um modo de operação ECB e, caso necessário, um *padding* de tipo *OneAndZeroes*, obtido a partir do texto em claro F1FB33A0.
2. [1,0] Cifre o texto em claro

   `boasorte`

   usando a cifra de auto-chave de Vigenere com chave inicial A.
3. [2,0] (Cifra ElGalmal) Considere o primo p=11.
   a. Verifique que 6 é um gerador multiplicativo de Z_{11}^*.
   b. Determine uma chave pública e uma chave privada para cifra El Gamal com p=11 e alpha=6
   c. Cifre o texto em claro x=3 com a chave pública obtida e verifique, a partir do texto cifrado, que a chave privada o decifra adequadamente. []
4. [1,0] Considere a relação de recorrência $k_i=k_{i-1}+k_{i-2}$ e os valores iniciais $k_0=0$ e $k_1=1$. Determine os primeiros 5 termos da *keystream* definida por este LFSR e use-a para cifrar, através da cifra ONE-PAD, o texto em claro 00011.

Grupo 2 - Segurança no Software [6 valores]

1. No contexto de vulnerabilidades de segurança:
   a. [1,5] Descreva os dois fatores principais que determinam o cálculo de risco numa aplicação.
   b. [1,5] Distinga entre vulnerabilidades de projeto e de programação.
   c. [1,5] Uma das vulnerabilidades mais comuns é não separar corretamente dados de instruções de controlo. Dê exemplo de duas vulnerabilidades que tenham por base este problema.
2. [1,5] De que forma o uso de engenharia reversa pode contribuir para encontrar superfícies de ataque em aplicações móveis e nos serviços web que lhes dão suporte.
3. [1,5] Distinga entre análise estática de código e análise de fluxo de dados.

Grupo 3 - Segurança no Hardware [4 valores]

1. [2,0] Indique as vantagens da utilização de um circuito TPM no processo de verificação da integridade de um computador do tipo PC durante o seu arranque (*secure boot*).
2. [2,0] Explique como é garantida a confidencialidade e a integridade dos dados de um enclave na tecnologia Intel SGX.

Grupo 4 - Regulamentos e Segurança das Comunicações [4 valores]

1. [2,0] Qual a diferença entre um Sistema de Deteção de Intrusões e um Sistema de Prevenção de Intrusões?
2. [2,0] Quais as principais diferenças entre um Quadro Normativo (por exemplo, o Quadro Nacional de Referência para a Cibersegurança) e um Regulamento (por exemplo, o Regulamento Geral da Proteção de Dados)?