Criptografia

MIETI

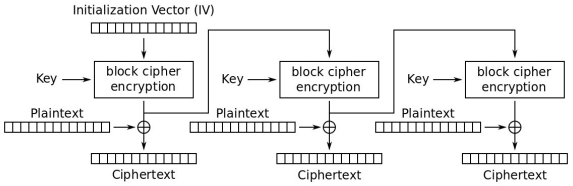
Teste intermédio – 9 de Novembro 2017

Questão 1

1. A cifra *one-time-pad* exibe segurança absoluta. Qual é o significado desta afirmação e porque é que esse facto não se traduz numa utilização generalizada dessa cifra?

2. As cifras sequenciais acabam por aproximar a cifra *one-time-pad*. É então legítimo afirmar-se que essas cifras exibem o mesmo nível de segurança? Justifique.

3. A operação de cifra no modo de operação *Output Feedback (OFB)* consiste em:



Output Feedback (OFB) mode encryption

   (a) Este modo de operação permite emular uma cifra sequencial a partir de uma cifra por blocos. Explique porquê e quais as características da cifra resultante.

   (b) Como deve ser realizada a operação de decifrar neste mesmo modo?

   (c) Parece-lhe que neste modo de operação, o vector de inicialização deve ser aleatório ou basta que não se repita (e.g. utilizando um contador)? Justifique.

   (d) Por vezes, o último bloco do criptograma pode ser usado como MAC. Parece-lhe ser esse o caso neste modo de operação? Justifique.

Questão 2 Suponha que pretende transmitir de forma segura um ficheiro com 20 byte de comprimento.

1. Descreva um procedimento apropriado para transmitir a mensagem de forma a garantir a confidencialidade da mensagem. Considere para o efeito que se fará uso da cidra AES, e detalhe em particular qual o tamanho da informação transmitida.

2. A solução proposta garante a integridade da informação? Em caso negativo, adapte o procedimento proposto por forma a acomodar também esse requisito.

Questão 3

1. No curso foram estudadas *Funções de Hash Criptográficas* e *Message Authentication Codes (MACs)*. Quais as semelhanças e diferenças entre essas técnicas criptográficas?

2. As *Key Derivation Functions (KDF)* constituem um exemplo de aplicação das funções de hash criptográficas. Quais os objectivos e as principais características dessa técnica (concretize com exemplos concretos, se entender conveniente).