

**1ª Série de Exercícios**

**Licenciatura em Engenharia Informática e de Computadores**

## Segurança Informática

# *Prof. Eng. José Manuel Simão*

# *Grupo 7:*

*Hugo Fora A42121*

*Luana Silva A42189*

*Rui Lima A42200*

*Bruno Lourenço A42400*

*Lisboa, 22 de Maio de 2017*

1) Este esquema não cumpre os requisitos, uma vez que a chave vai incluída no criptograma, como tal não garante a confidencialidade. Outra razão advém do facto de no caso de o T(k)(m) ser alterado, a mensagem será visualizada como não autêntica, apesar do facto de o ser. Por outro lado, caso o criptograma seja alterado no esquema simétrico de cifra, Es(k)(m), a autenticação mantém a sua validade, apesar de a mensagem já não ser autêntica.

2) A função de hash é usada para converter um input arbitrário num valor de tamanho fixo, que é normalmente muito menor, e garante as propriedades da assinatura. A primitiva da assinatura serve para assinar e misturar a chave com a mensagem.

3) Em E(k)(m1||m2), é cifrada a concatenação das mensagens, e em E(k)(m1)||E(k)(m2), é cifrada cada mensagem em separado sendo os seus resultados concatenados, e uma vez que o esquema de cifra simétrico usa padding, quer seja para preencher os bits do bloco em falta, quer seja para indicar que o tamanho da cifra é múltiplo do número de bits do bloco, a quantidade de bits de padding será sempre diferente, criando assim um resultado sempre diferente para as cifras.

4) Os ataques de Vaudenay, consistem em modificar os bits de padding usados numa cifra, e uma vez que Galois Counter Mode, não necessita de padding pois usa vectores de dimensão variável, tornando-o invulnerável aos ataques de Vaudenay.