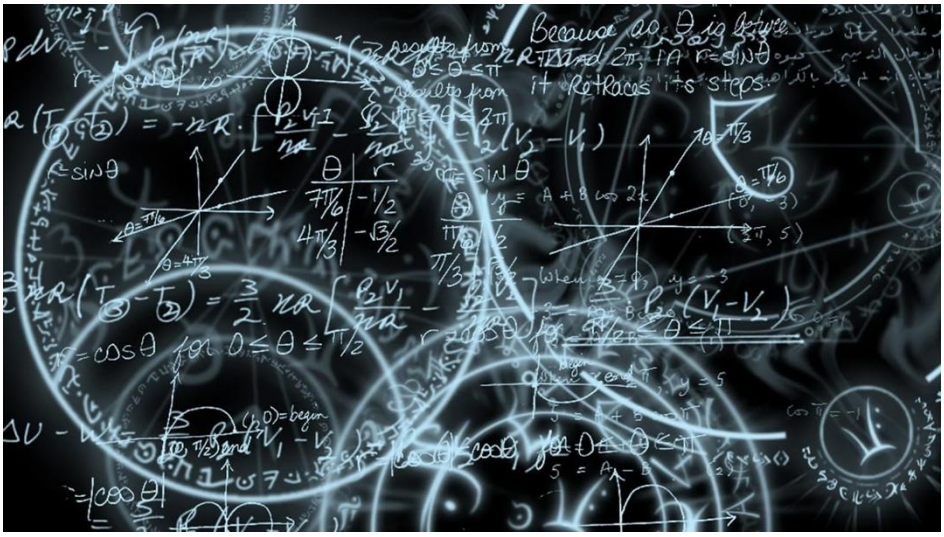
Universidade do Minho
Escola de Engenharia

Criptografia

TP3



João Miguel da Silva Alves (83624)

Paulo Jorge Alves (84480)

MESTRADO INTEGRADO EM ENGENHARIA BIOMÉDICA

INFORMÁTICA MÉDICA 2020/2021

O objetivo deste trabalho prático é encriptar uma imagem recorrendo a dois métodos diferentes de cifra por blocos (ECB e CBC).

Uma cifra de blocos cifra sempre o mesmo conteúdo da mesma maneira, dada a mesma chave. Um bom exemplo disto, é, por exemplo, a imagem do pinguim da Linux (figura 1), pois tem regiões em que todas as cores são iguais, e por isso, criptografarão da mesma forma ao usar uma cifra de blocos.

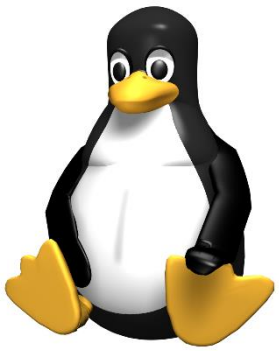


Figura 1 - Figura original: pinguim da Linux

Começamos por cifrar a imagem usando a AES no modo ECB (Electronic Code Book).

A cifra de blocos é aplicada diretamente à imagem, e assim, não se podem ocultar padrões de dados. Este modo produz protocolos de criptografia sem garantia de integridade e bastante suscetíveis a ataques de repetição, pois cada bloco é cifrado exatamente da mesma forma. Na figura 2, está o pinguim da figura anterior cifrado pelo modo descrito.

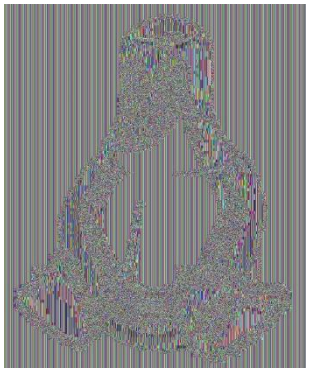


Figura 2 - Figura cifrada pelo modo ECB

Comparando o que se consegue ver nas duas imagens, verifica-se que o resultado da encriptação não é muito diferente da imagem original. Na figura 2, consegue-se perceber perfeitamente qual a imagem que está a ser cifrada. Isto porque, como foi dito anteriormente, a imagem usada tem blocos que se repetem, o que faz com que a imagem cifrada tenha os mesmos padrões da imagem original.

Desta forma, verifica-se que o modo ECB não é seguro para imagens que tenham blocos de cores. Quanto mais aleatória for a imagem (em geometria e cor), mais segura é cifrar com este modo.

É então necessário recorrer a um método mais eficaz, de modo a que a imagem cifrada não seja percetível nem fácil de decifrar.

O modo alternativo usado foi o modo CBC (Cipher Block Chaining). Este modo, em comparação com o usado anteriormente, inclui a encriptação usando operações com vetores.

Primeiro, a imagem é processada por vetores de inicialização (IV). Este IV é um meio de aumentar a segurança da cifra através da introdução de um grau de aleatoriedade, sendo único, mas igual tanto na cifragem como decifragem. A integridade destes vetores tem de ser protegida, independentemente de serem secretos ou não.

Só depois de realizado este processo, é que a imagem é cifrada. Na figura 3, temos a figura 1 cifrada por este modo.

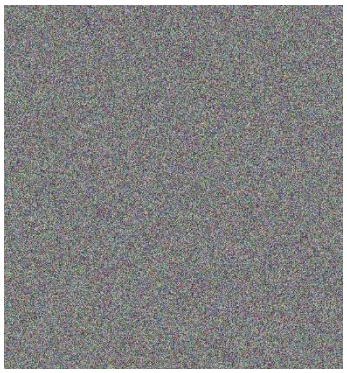


Figura 3 - Figura cifrada pelo modo CBC

Comparando o que se consegue ver em relação às imagens anteriores, verifica-se que o resultado da encriptação é aleatório, o que permite que não haja qualquer padrão na imagem cifrada. Independentemente das cores ou geometrias da imagem, o resultado é sempre aleatório, sendo mais difícil o ataque.

Com isto, verifica-se que blocos de dados idênticos não devem ser criptografados de maneira a que o resultado seja semelhante. Como consequência, o modo ECB é considerado de fraca segurança, ao contrário do modo CBC, que por usar um fator aleatório, o resultado torna-se indecifrável.