

# Trabalho 2 - Teoria da Codificação e Criptografia

---

Déborah Mendes Ferreira  
09/0042735

24 de junho de 2013

## 1 COMPILAÇÃO

Para compilar execute o seguinte:

**gcc cifraimagem.c ppm.c -o cifraimagem**

## 2 EXECUÇÃO

### CIFRA DE HILL

Cifração:

**./cifraimagem -e -h entrada.ppm saida.ppm**

Decifração:

**./cifraimagem -d -h saida.ppm entrada.ppm**

### TEA - ECB

Cifração:

**./cifraimagem -e -t1 entrada.ppm saida.ppm**

Decifração:

**./cifraimagem -d -t1 saida.ppm entrada.ppm**

### TEA - CBC

Cifração:

**./cifraimagem -e -t2 entrada.ppm saida.ppm**

Decifração:

**./cifraimagem -d -t2 saida.ppm entrada.ppm**

### 3 COMPARAÇÃO

Chave utilizada na Cifra de Vigenére: 40 67 23 200 56.

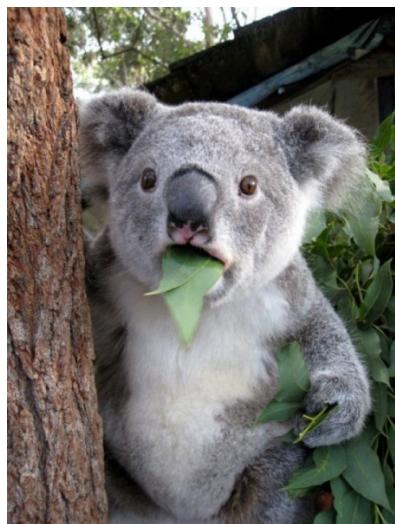
Chave utilizada na Cifra de Hill: $\begin{pmatrix} 99 & 78 \\ 91 & 77 \end{pmatrix}$

Chave utilizada na TEA ECB e CBC: 0x11223344 0x22334411 0x33441122 0x44112233.

Nas imagens cifradas com a Cifra de Vigenére é possível observar claramente qual a imagem original, com apenas algumas alterações na cor. Para a chave utilizada com 5 números, fica claro que já uma sequência de 5 tonalidades que se repetem, dando a dica para o adversário que quiser obter a imagem original.

A cifra de Hill e a TEA em modo ECB não conseguem esconder imagens que possuam blocos de uma só cor, na imagem 3.2 isso é observado. Porém para imagens com cores mais dispersas, estas cifras não revelam muitos detalhes da imagem original, como na imagem 3.1. Mesmo para as figuras com grandes blocos concentrados de cores, é possível perceber que a TEA em modo ECB gera um melhor resultado que a Cifra de Hill, ela gera uma maior variação de cores mesmo para blocos da mesma cor.

Para melhorar o uso da TEA, foi utilizado o modo de operação *cipher block chaining*. Pelos exemplos, há uma melhora perceptível em relação ao modo ECB, em todos os exemplos é impossível identificar qual era a imagem original apenas observando a imagem cifrada.



(a) Imagem Original



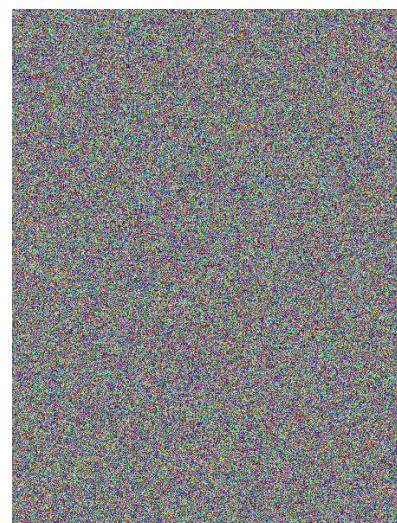
(b) Cifrada com Vigenére



(c) Cifrada com Cifra de Hill



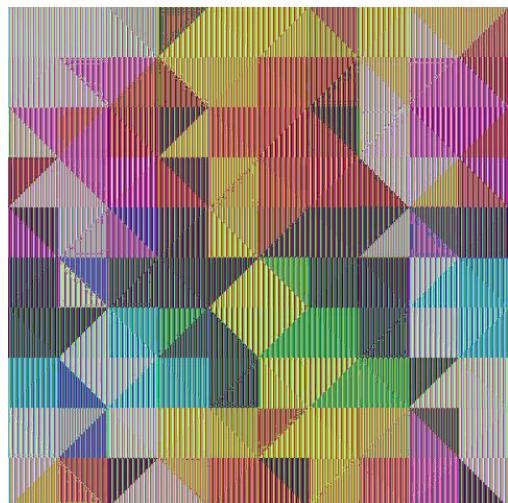
(d) Cifrada com TEA em modo ECB



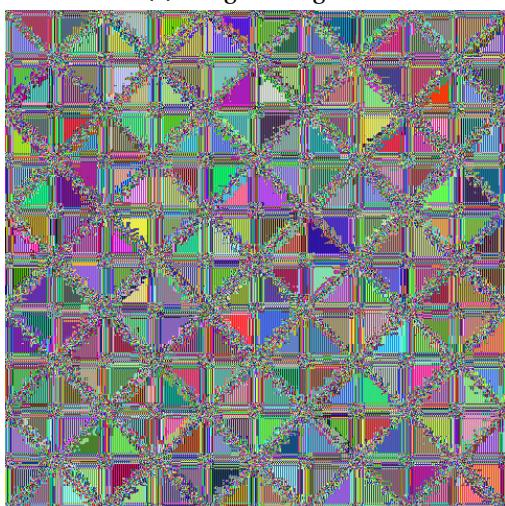
(e) Cifrada com TEA em modo CBC



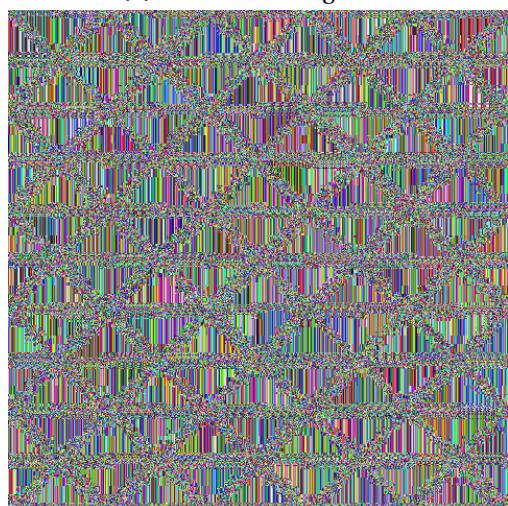
(a) Imagem Original



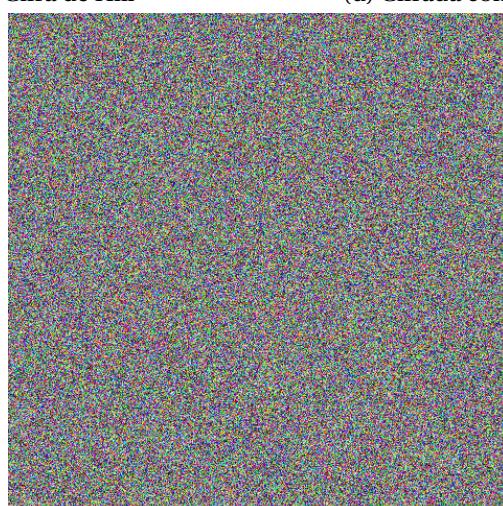
(b) Cifrada com Vigenére



(c) Cifrada com Cifra de Hill



(d) Cifrada com TEA em modo ECB

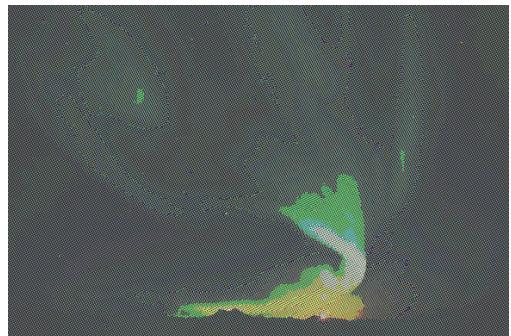


(e) Cifrada com TEA em modo CBC

Figure 3.2: Imagem 2



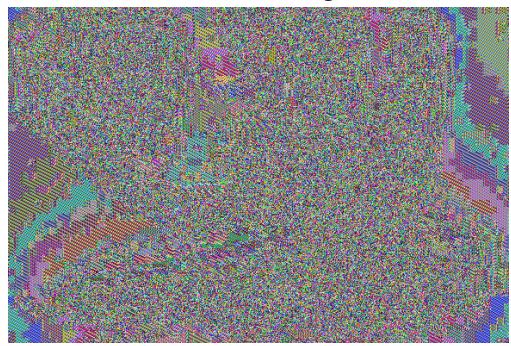
(a) Imagem Original



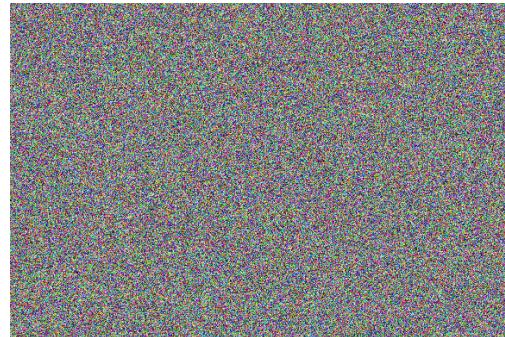
(b) Cifrada com Vigenére



(c) Cifrada com Cifra de Hill

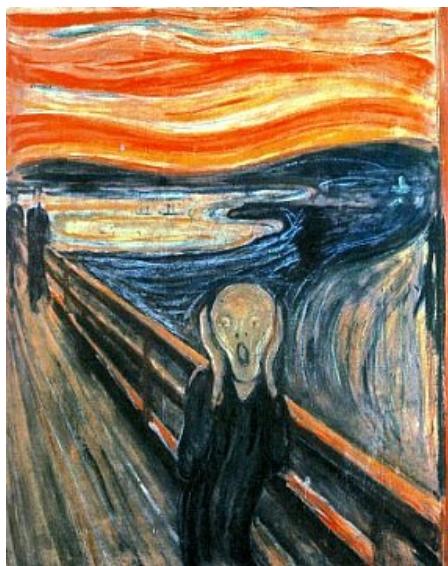


(d) Cifrada com TEA em modo ECB

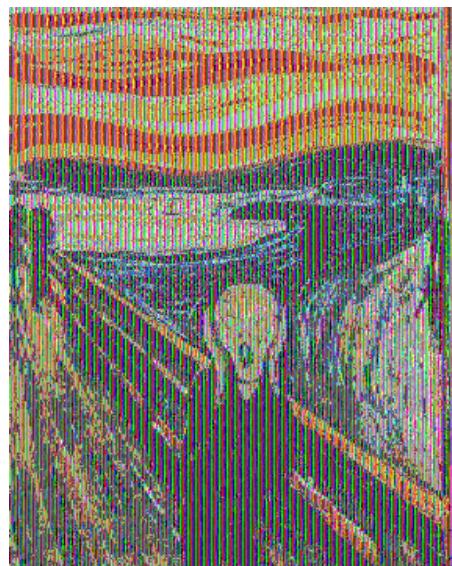


(e) Cifrada com TEA em modo CBC

Figure 3.3: Imagem 3



(a) Imagem Original



(b) Cifrada com Vigenére



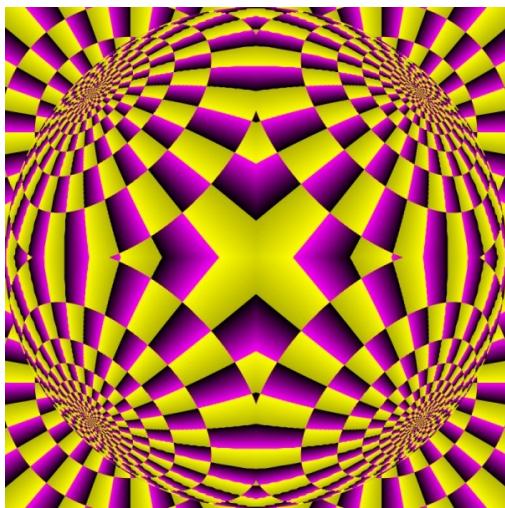
(c) Cifrada com Cifra de Hill



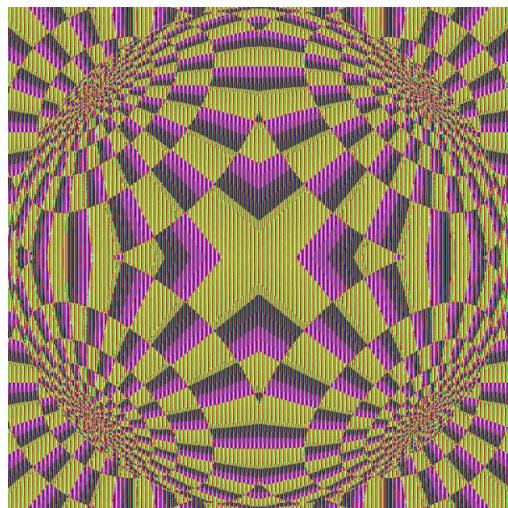
(d) Cifrada com TEA em modo ECB



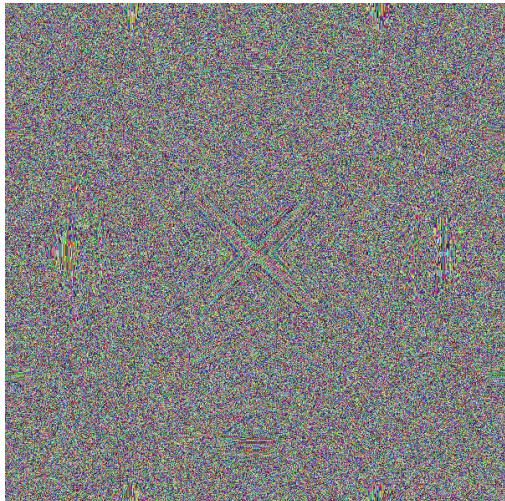
(e) Cifrada com TEA em modo CBC



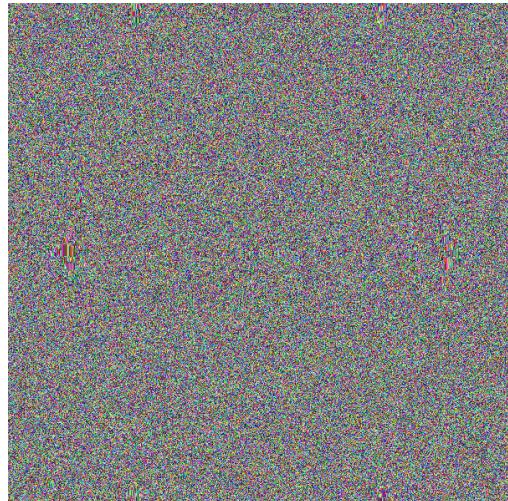
(a) Imagem Original



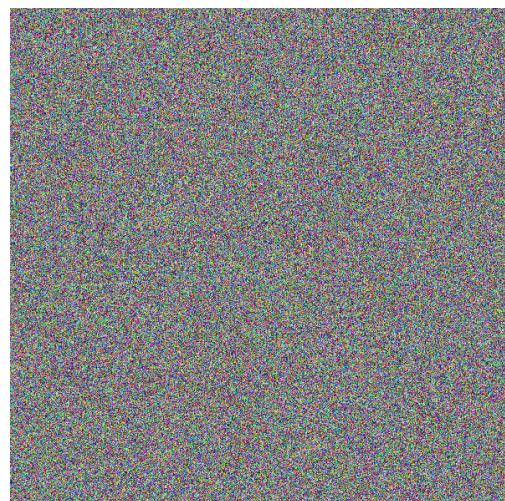
(b) Cifrada com Vigenére



(c) Cifrada com Cifra de Hill



(d) Cifrada com TEA em modo ECB



(e) Cifrada com TEA em modo CBC

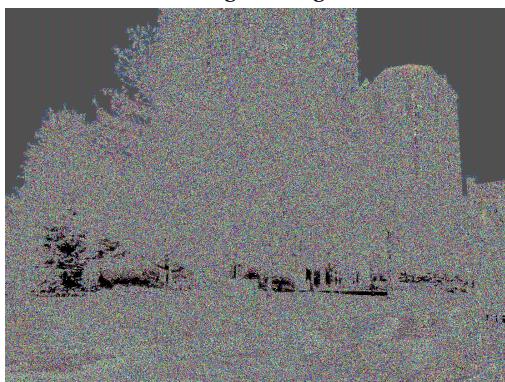
Figure 3.5: Imagem 5



(a) Imagem Original



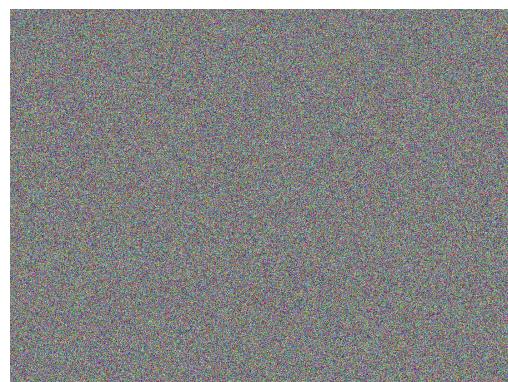
(b) Cifrada com Vigenére



(c) Cifrada com Cifra de Hill



(d) Cifrada com TEA em modo ECB



(e) Cifrada com TEA em modo CBC

Figure 3.6: Imagem 6