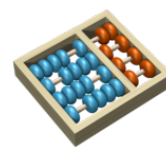




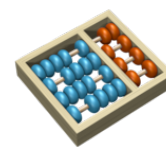
UNIVERSIDADE ESTADUAL DE CAMPINAS  
Instituto de Computação – IC  
MO421 – Introdução a Criptografia  
Prof. Dr. Diego de Freitas Aranha



THALES EDUARDO NAZATTO

## RELATÓRIO

**Projeto 2** – Diferenças entre métodos de cifração através de imagens



## 1. Introdução

A cifra de Vigenère e a cifra *affine* são dois tipos clássicos de cifras de substituição, em que cada unidade (neste caso, cada *byte*) de um texto plano são substituídos por outra de modo a formar um cifrotexto (1). A cifra TEA é uma cifra de bloco criada por David J.Wheeler e Roger M. Needham desenvolvida com o intuito de ser pequena, rápida e poderosa (2). Nela é usada uma chave de 128 *bits* e são cifrados blocos de 64 *bits* por vez.

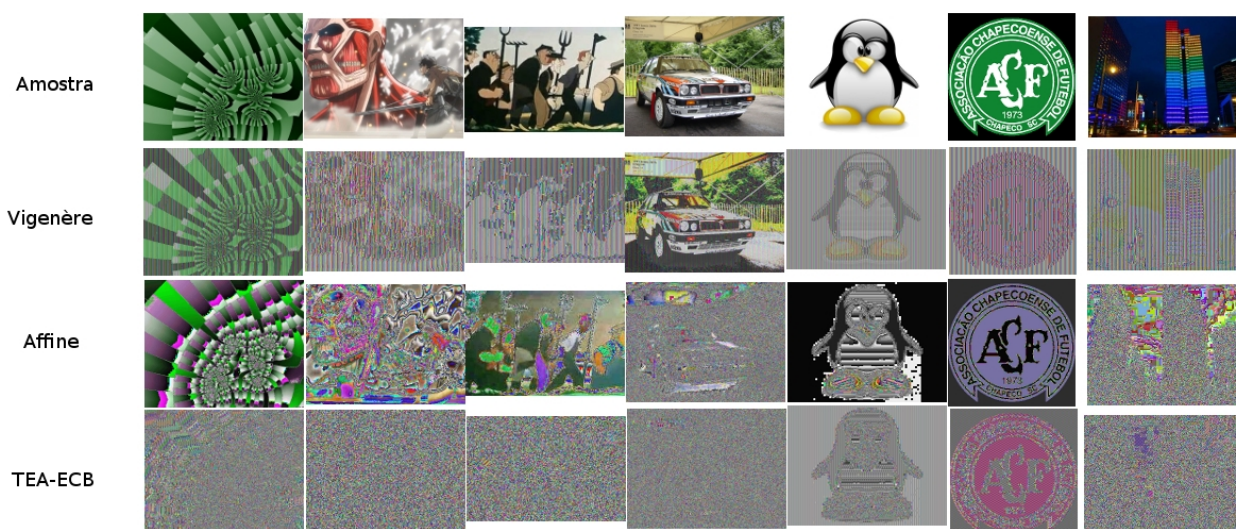
Neste projeto, serão observadas as diferenças entre essas cifras usando imagens para serem cifradas. Serão discutidas limitações e melhoras em suas implementações.

## 2. Desenvolvimento e resultados

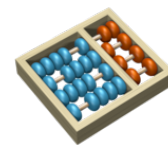
Um programa em C foi disponibilizado com a cifra de Vigenère já implementada. O mesmo foi incrementado com as cifras *affine* e TEA, sendo que a cifra TEA foi implementada com dois modos de operação: ECB (*Electronic Codebook*) e CFB (*Cipher Feedback*). Após os métodos serem implementados, 7 imagens diferentes foram cifradas e colocadas em comparação.

### 2.1 Principais diferenças entre os métodos de cifração

O resultado de cada uma das cifras é visto na imagem abaixo.



**Figura 1.** Resultado de cada imagem após diferentes métodos de cifração



Neste item, o foco está em definir as diferenças entre as cifras, por isso o modo CFB não foi mostrado no momento.

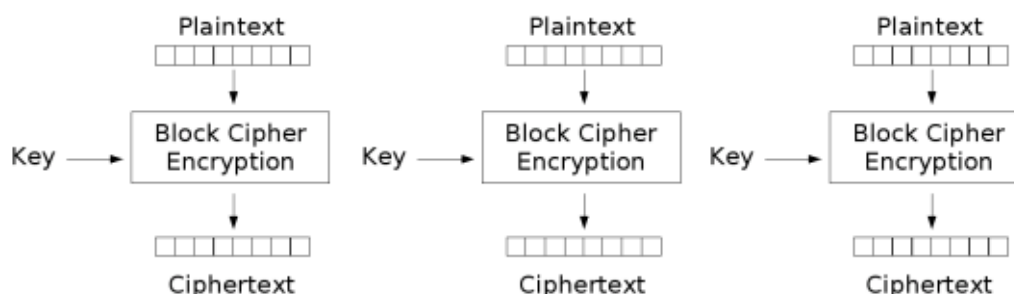
Na cifra de Vigenère as cores ficaram mais “lavadas” e são adicionados alguns “ruídos” a imagem. A imagem fica com algumas listras, entretanto a silhueta da imagem original continua à vista, permitindo que um adversário com experiência faça um ataque a essas imagens sem grandes dificuldades.

Na cifra *affine*, alguns dos padrões são obscurecidos em imagens mais complexas e as cores ficaram com um aspecto mais lisérgico (ou psicodélico). Entretanto, boa parte da silhueta da imagem original continua a vista, embora seja menos óbvia que a cifra de Vigenère.

Na cifra TEA, os princípios de confusão e difusão aplicados nas cifras de bloco ficam evidentes ao comparar com as cifras anteriores. Boa parte da imagem original é obscurecida em imagens mais complexas. As cores não parecem seguir um padrão específico. Ainda há partes da imagem original que são detectadas, mas isso não é problema da cifra utilizada, e sim do modo de operação em que ela foi colocada. O modo ECB possui algumas limitações que serão discutidas a seguir.

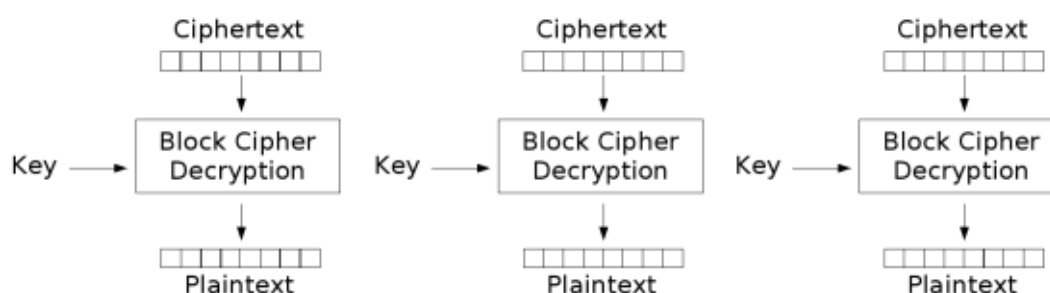
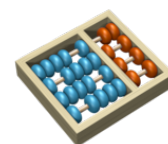
## 2.2 Limitações do uso do modo de operação ECB na cifra TEA

O modo de operação ECB é o mais simples de ser implementado em uma cifra de bloco: Nele, cada bloco é cifrado/decifrado linearmente, sem tratamento adicional. E é justamente por sua natureza que o ECB possui duas limitações ao cifrar uma imagem.



Electronic Codebook (ECB) mode encryption

Figura 2. Cifração pelo modo ECB (3)

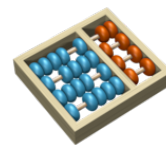
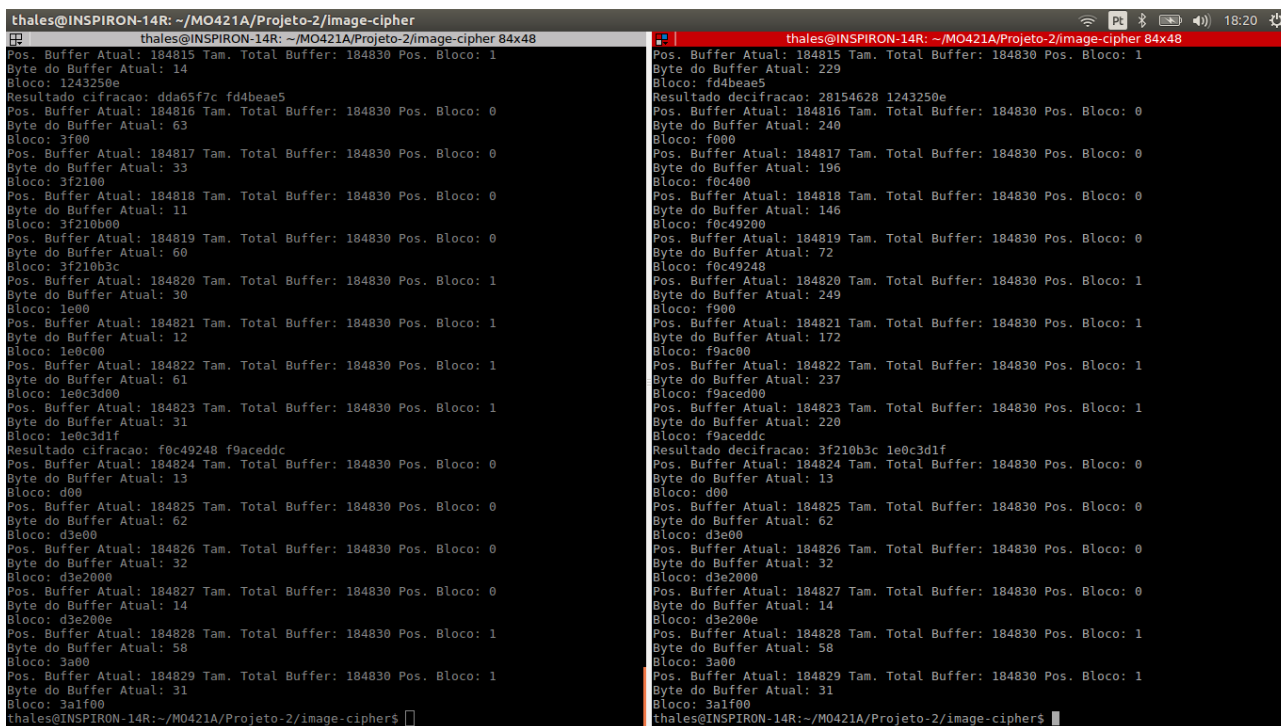


### Electronic Codebook (ECB) mode decryption

**Figura 3.** Decifração no modo ECB (3)

A primeira é que, como um *pixel* pode ser visto também como um *array* de *bytes* (um *byte* para o R, o G, o B e o alpha), a cifração pelo modo ECB irá cifrar *pixels* da mesma cor de modo igual, e em caso de imagens mais simples (como as amostras 5 e 6 da figura 1, contadas da esquerda para a direita) a silhueta da imagem original ainda aparece. Entretanto, mesmo nas imagens mais complexas é possível achar uma “brecha”, um pequeno trecho que possa estabelecer como um padrão da imagem antiga.

A segunda é que, como o TEA cifra blocos de 64 *bits*, qualquer imagem que não tenha um número de *pixels* divisível por 8 não terão todos os seus *bytes* cifrados no modo ECB. Para ilustrar isso foram introduzidos *logs* na aplicação e o resultado de cada bloco é colocado também, conforme figura abaixo. Nisso, há a percepção de que o último bloco nunca será cifrado nesses casos, e um adversário experiente pode explorar essa brecha. As amostras 3, 6 e 7 da figura 1, contadas da esquerda para a direita, são as que possuem esse problema ao serem cifradas no modo ECB.

```

thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher 84x48
Pos. Buffer Atual: 184815 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 14
Bloco: 1243250e
Resultado cifraacao: dda65f7c fd4beae5
Pos. Buffer Atual: 184816 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 63
Bloco: 3f00
Pos. Buffer Atual: 184817 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 33
Bloco: 3f2100
Pos. Buffer Atual: 184818 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 11
Bloco: 3f210b00
Pos. Buffer Atual: 184819 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 60
Bloco: 3f210b3c
Pos. Buffer Atual: 184820 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 30
Bloco: 1e00
Pos. Buffer Atual: 184821 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 12
Bloco: 1e0c00
Pos. Buffer Atual: 184822 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 61
Bloco: 1e0c3d00
Pos. Buffer Atual: 184823 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 31
Bloco: 1e0c3d1f
Resultado cifraacao: f0c49248 f9aceddc
Pos. Buffer Atual: 184824 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 13
Bloco: d00
Pos. Buffer Atual: 184825 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 62
Bloco: d3e00
Pos. Buffer Atual: 184826 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 32
Bloco: d3e2000
Pos. Buffer Atual: 184827 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 14
Bloco: d3e200e
Pos. Buffer Atual: 184828 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 58
Bloco: 3a00
Pos. Buffer Atual: 184829 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 31
Bloco: 3a1f00
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher$

thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher 84x48
Pos. Buffer Atual: 184815 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 229
Bloco: fd4beae5
Resultado decifraacao: 28154628 1243250e
Pos. Buffer Atual: 184816 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 240
Bloco: f000
Pos. Buffer Atual: 184817 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 196
Bloco: f0c400
Pos. Buffer Atual: 184818 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 146
Bloco: f0c49200
Pos. Buffer Atual: 184819 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 72
Bloco: f0c49248
Pos. Buffer Atual: 184820 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 249
Bloco: f900
Pos. Buffer Atual: 184821 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 172
Bloco: f9ac00
Pos. Buffer Atual: 184822 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 237
Bloco: f9aced00
Pos. Buffer Atual: 184823 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 220
Bloco: f9aceddc
Resultado decifraacao: 3f210b3c 1e0c3d1f
Pos. Buffer Atual: 184824 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 13
Bloco: d00
Pos. Buffer Atual: 184825 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 62
Bloco: d3e00
Pos. Buffer Atual: 184826 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 32
Bloco: d3e2000
Pos. Buffer Atual: 184827 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 14
Bloco: d3e200e
Pos. Buffer Atual: 184828 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 58
Bloco: 3a00
Pos. Buffer Atual: 184829 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 31
Bloco: 3a1f00
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher$

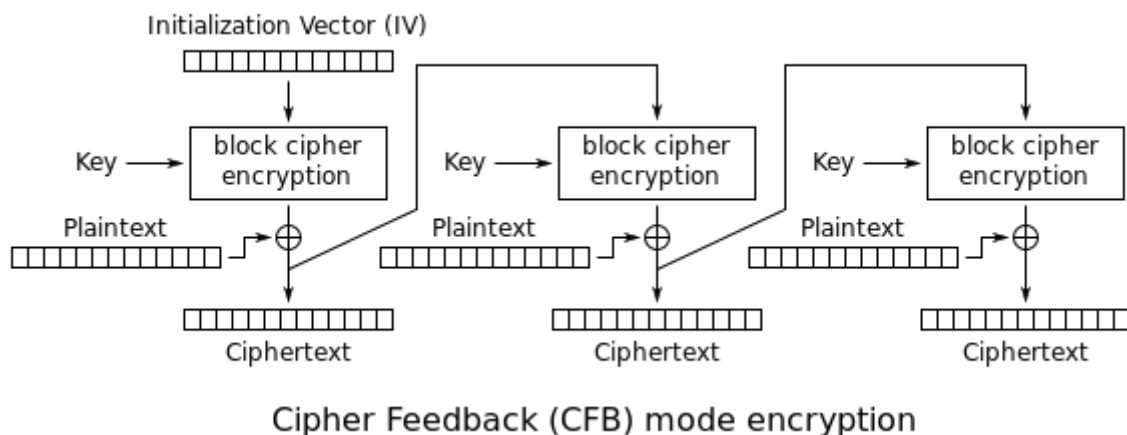
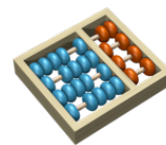
```

**Figura 4.** Logs da aplicação em modo ECB de uma imagem cujo número de pixels não é divisível por 8. Cifração a esquerda e decifração a direita. O último bloco é o mesmo em ambos os casos e não é alterado.

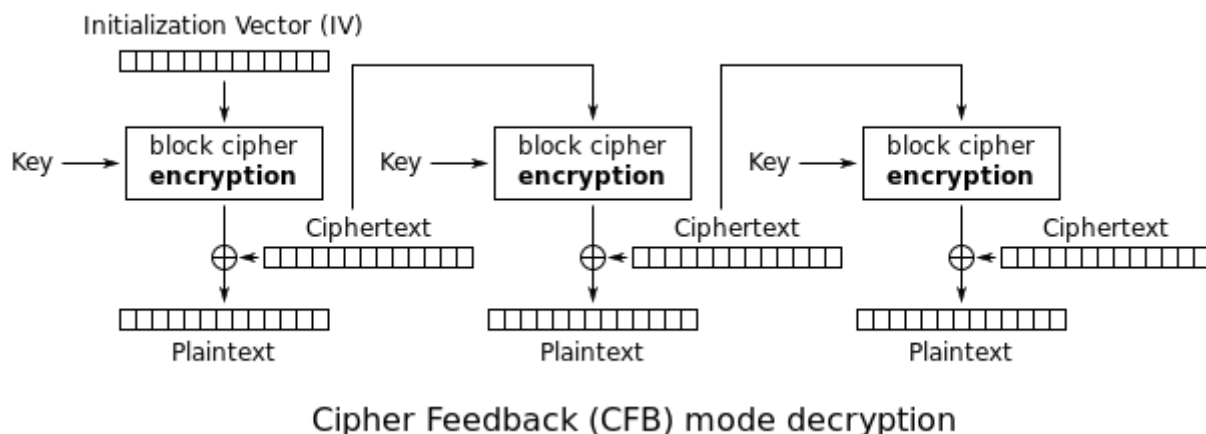
### 2.3 Resolvendo as limitações: O modo de operação CFB

Para resolver as limitações do modo ECB, a solução é simples: implementar outro modo de operação que não possui essas limitações. No caso, o CFB foi o escolhido.

O CFB é um modo de operação que faz a cifra de bloco se comportar como uma cifra de fluxo. Nele, para cifrar e decifrar uma mensagem é usado apenas o método de cifração. Para a cifração, um vetor de inicialização (IV) é cifrado e é feita uma operação XOR com o texto plano, gerando um cifrotexto. Esse cifrotexto é armazenado e colocado como entrada de outra cifração, repetindo a operação XOR com o texto plano. Tal processo é repetido até que todos os bytes tenham sido cifrados. Para a decifração o processo é o mesmo, com a diferença de que o cifrotexto não precisa ser gerado, só colocado como entrada do método de cifração.



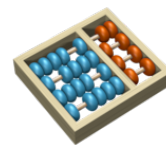
**Figura 5.** Cifração no modo CFB (3)



**Figura 6.** Decifração no modo CFB (3)

Com ele, pela natureza da cifra de fluxo todos os bytes vão ser cifrados, e pela uniformidade da operação XOR os padrões da imagem são totalmente ocultados, ganhando segurança no processo. As duas fraquezas do modo ECB acabam sanadas de uma única maneira, sendo ilustrado nas duas imagens abaixo:

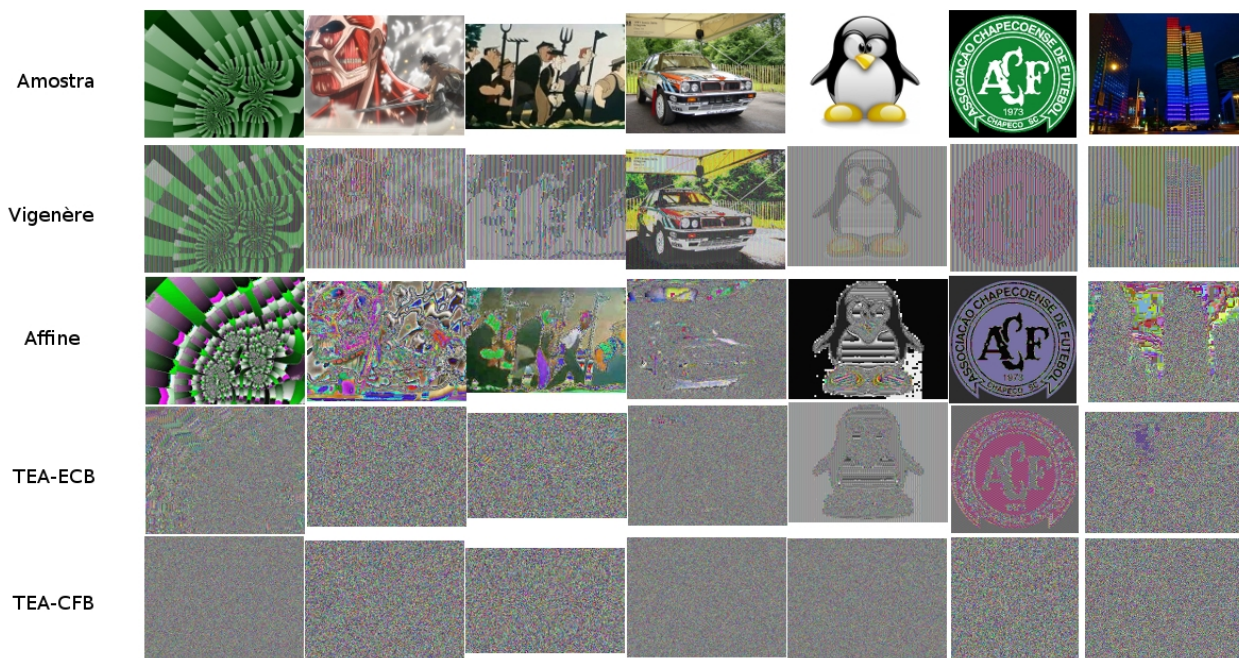




```
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher 84x48
Bloco: 1243250e
Resultado cifração: b27919b0 9da8a6c5
Pos. Buffer Atual: 184816 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 63
Bloco: 3f00
Pos. Buffer Atual: 184817 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 33
Bloco: 3f2100
Pos. Buffer Atual: 184818 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 11
Bloco: 3f210b00
Pos. Buffer Atual: 184819 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 60
Bloco: 3f210b3c
Pos. Buffer Atual: 184820 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 30
Bloco: 1e00
Pos. Buffer Atual: 184821 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 12
Bloco: 1e0c00
Pos. Buffer Atual: 184822 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 61
Bloco: 1e0c3d00
Pos. Buffer Atual: 184823 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 31
Bloco: 1e0c3d1f
Resultado cifração: f6b67bef fff6c2b7
Pos. Buffer Atual: 184824 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 13
Bloco: d00
Pos. Buffer Atual: 184825 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 62
Bloco: d3e00
Pos. Buffer Atual: 184826 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 32
Bloco: d3e2000
Pos. Buffer Atual: 184827 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 14
Bloco: d3e200e
Pos. Buffer Atual: 184828 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 58
Bloco: 3a00
Pos. Buffer Atual: 184829 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 31
Bloco: 3a1f00
Bloco final: d3e200e 3a1f0000
Resultado cifração: fb885be1 c5e9c2b7
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher$

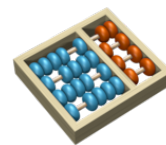
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher 84x48
Bloco: 9da8a6c5
Resultado decifração: 28154628 1243250e
Pos. Buffer Atual: 184816 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 246
Bloco: f600
Pos. Buffer Atual: 184817 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 182
Bloco: f6b600
Pos. Buffer Atual: 184818 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 123
Bloco: f6b67b00
Pos. Buffer Atual: 184819 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 239
Bloco: f6b67bef
Pos. Buffer Atual: 184820 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 255
Bloco: ff00
Pos. Buffer Atual: 184821 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 246
Bloco: fff600
Pos. Buffer Atual: 184822 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 194
Bloco: fff6c200
Pos. Buffer Atual: 184823 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 183
Bloco: fff6c2b7
Resultado decifração: 3f210b3c 1e0c3d1f
Pos. Buffer Atual: 184824 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 251
Bloco: fb00
Pos. Buffer Atual: 184825 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 136
Bloco: fb8800
Pos. Buffer Atual: 184826 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 91
Bloco: fb885b00
Pos. Buffer Atual: 184827 Tam. Total Buffer: 184830 Pos. Bloco: 0
Byte do Buffer Atual: 225
Bloco: fb885be1
Pos. Buffer Atual: 184828 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 197
Bloco: c500
Pos. Buffer Atual: 184829 Tam. Total Buffer: 184830 Pos. Bloco: 1
Byte do Buffer Atual: 233
Bloco: c5e900
Bloco final: fb885be1 c5e90000
Resultado decifração: d3e200e 3a1fc2b7
thales@INSPIRON-14R: ~/MO421A/Projeto-2/image-cipher$
```

**Figura 7.** Logs da aplicação em modo CFB de uma imagem cujo número de pixels não é divisível por 8. Cifração a esquerda e decifração a direita. Desta vez, o último bloco é cifrado e decifrado.



**Figura 8.** Diferenças entre o modo CFB da cifra TEA e as outras formas de cifrar. O modo CFB é o único que não deixa rastros da imagem original e tem sua distribuição de cores aleatória e uniforme, sendo a mais segura dentre as 4.

### 3. Conclusão



Podemos concluir que, ao cifrar uma imagem, o melhor método a ser escolhido é o que não deixa rastros na cifração. Em outras palavras, que deixa a distribuição de *pixels* da imagem cifrada de um modo aleatório e uniforme, de modo a não deixar padrões da imagem original. Dessa forma, o modo de operação CFB na cifra TEA se mostrou bastante eficaz, enquanto o modo de operação ECB, a cifra de Vigenère e a cifra *affine* tiveram desempenho inferior.

O modo de operação CFB também resolve o problema do modo ECB de cifragem de todos os *bytes*, uma vez que o ECB cifra apenas o bloco por inteiro e o CFB usa a cifra de bloco como se fosse uma cifra de fluxo.

Por esses dois motivos, a cifra TEA no modo CFB é o método de cifração a ser escolhido dentre os 4 analisados.

## 4. Bibliografia

- (1) Cifra de Substituição – Wikipedia, presente em:  
<[https://pt.wikipedia.org/wiki/Cifra\\_de\\_substitui%C3%A7%C3%A3o](https://pt.wikipedia.org/wiki/Cifra_de_substitui%C3%A7%C3%A3o)> Acesso em: 28 Mai. 2017
- (2) WHEELER, David J., NEEDHAM, Roger M. , “TEA, a Tiny Encryption Algorithm”
- (3) Block Cipher Mode of Operation – Wikipedia, presente em:  
<[https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)> Acesso em: 28 Mai. 2017