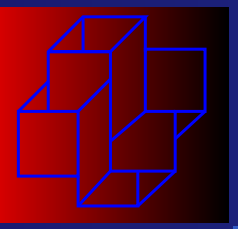
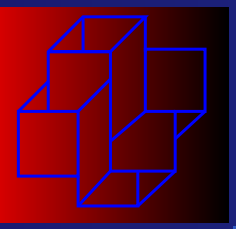


Análise da segurança de esteganocriptografia em seqüências de imagens

LNCC - Fev/2007

Fábio Borges de Oliveira

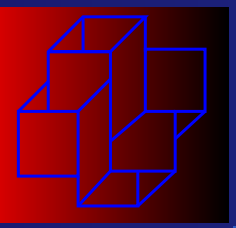


Divisão do trabalho

Compressão e codificação

Criptografia

Esteganografia

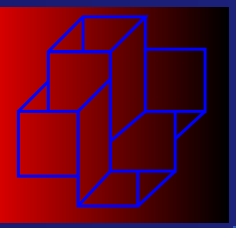


Divisão do trabalho

Compressão e codificação

Criptografia

Esteganografia

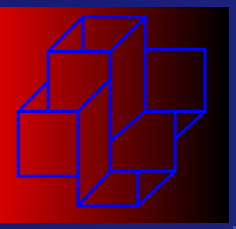


Divisão do trabalho

Compressão e codificação

Criptografia

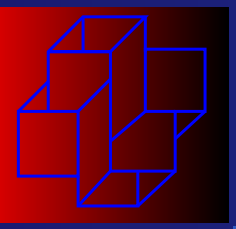
Esteganografia



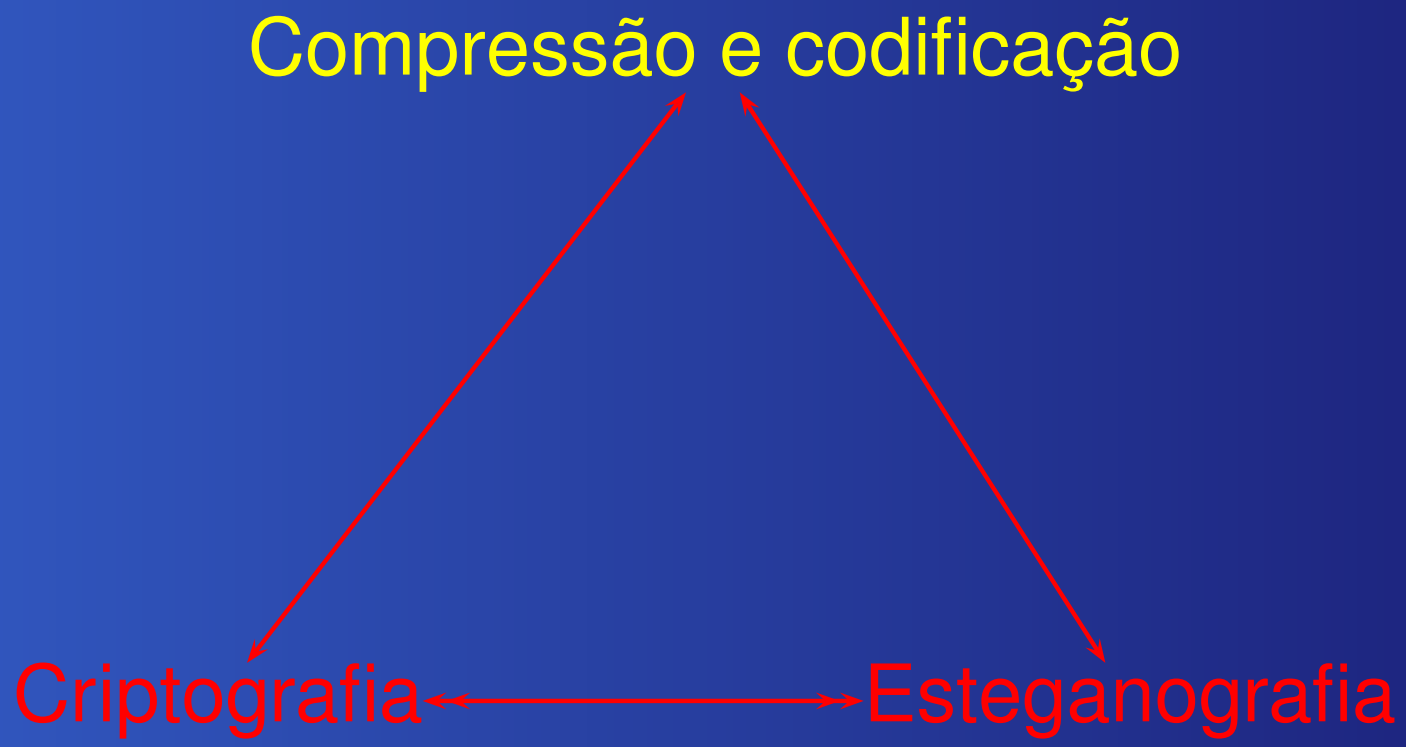
Divisão do trabalho

Compressão e codificação

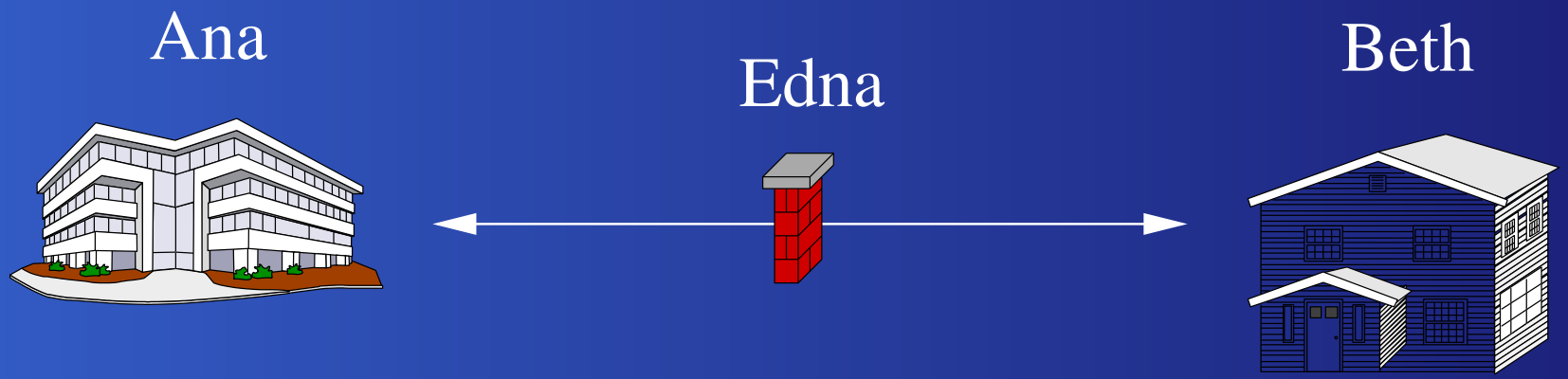
Criptografia ⟷ Esteganografia



Divisão do trabalho

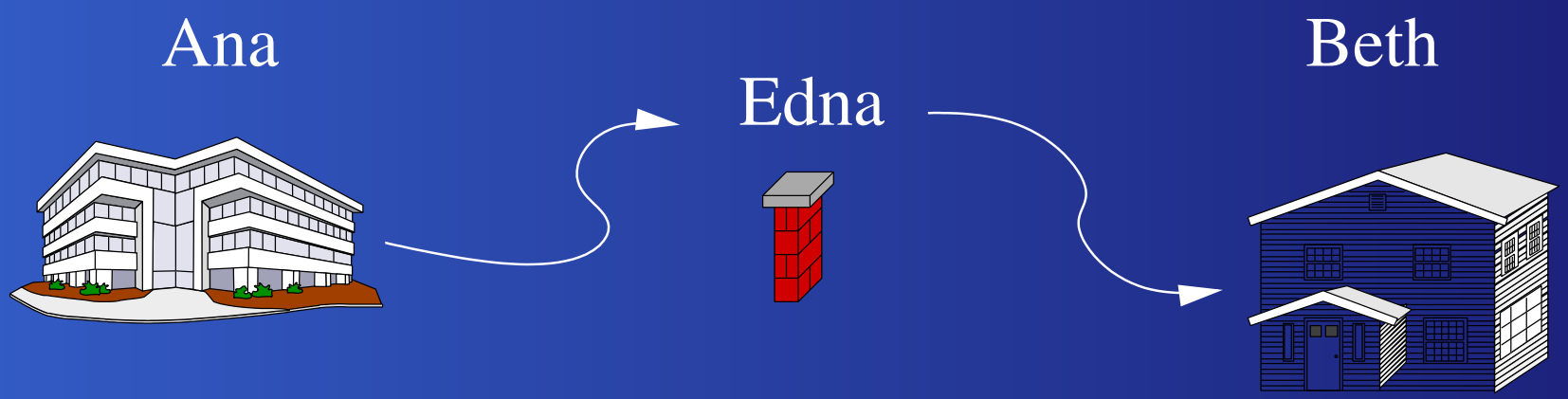


Fluxo Normal

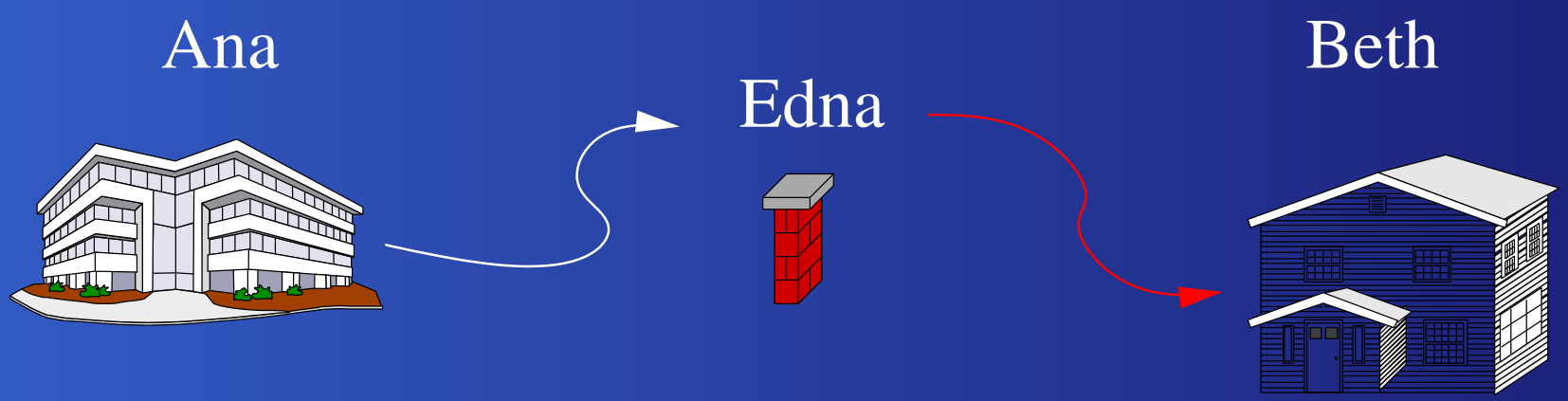


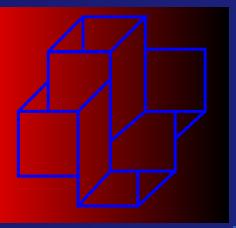
Ameaças iminentes.

Interceptação



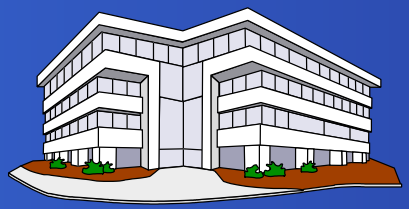
Alteração



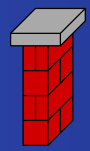


Fabricação

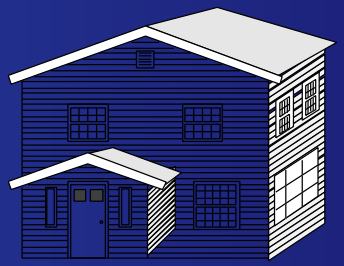
Ana

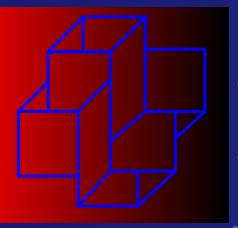


Edna



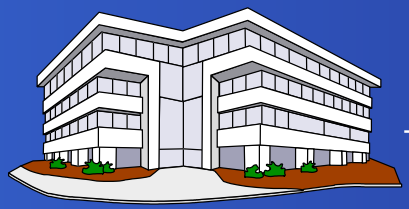
Beth



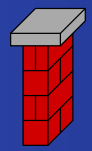


Interrupção

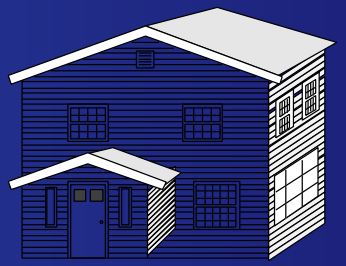
Ana

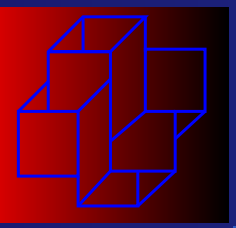


Edna



Beth





Esteganografia

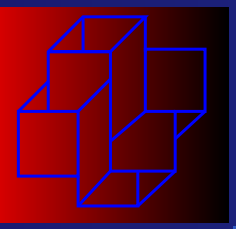
Original:

Esteganografia:

Simétrica

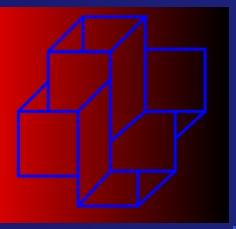
Simétrica

César, Hill (Involutória), RC4



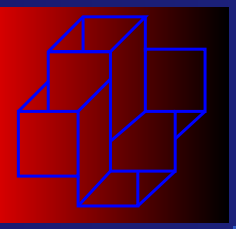
Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$
- $Z \leftrightarrow E$
- "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- "QVDIJTPOCYHNGXAZWUSMFKRLBE"
- $26! - 1 = 403291461126605635583999999$
- $26! \approx 4.03\ 10^{26}$



Altas Freqüências

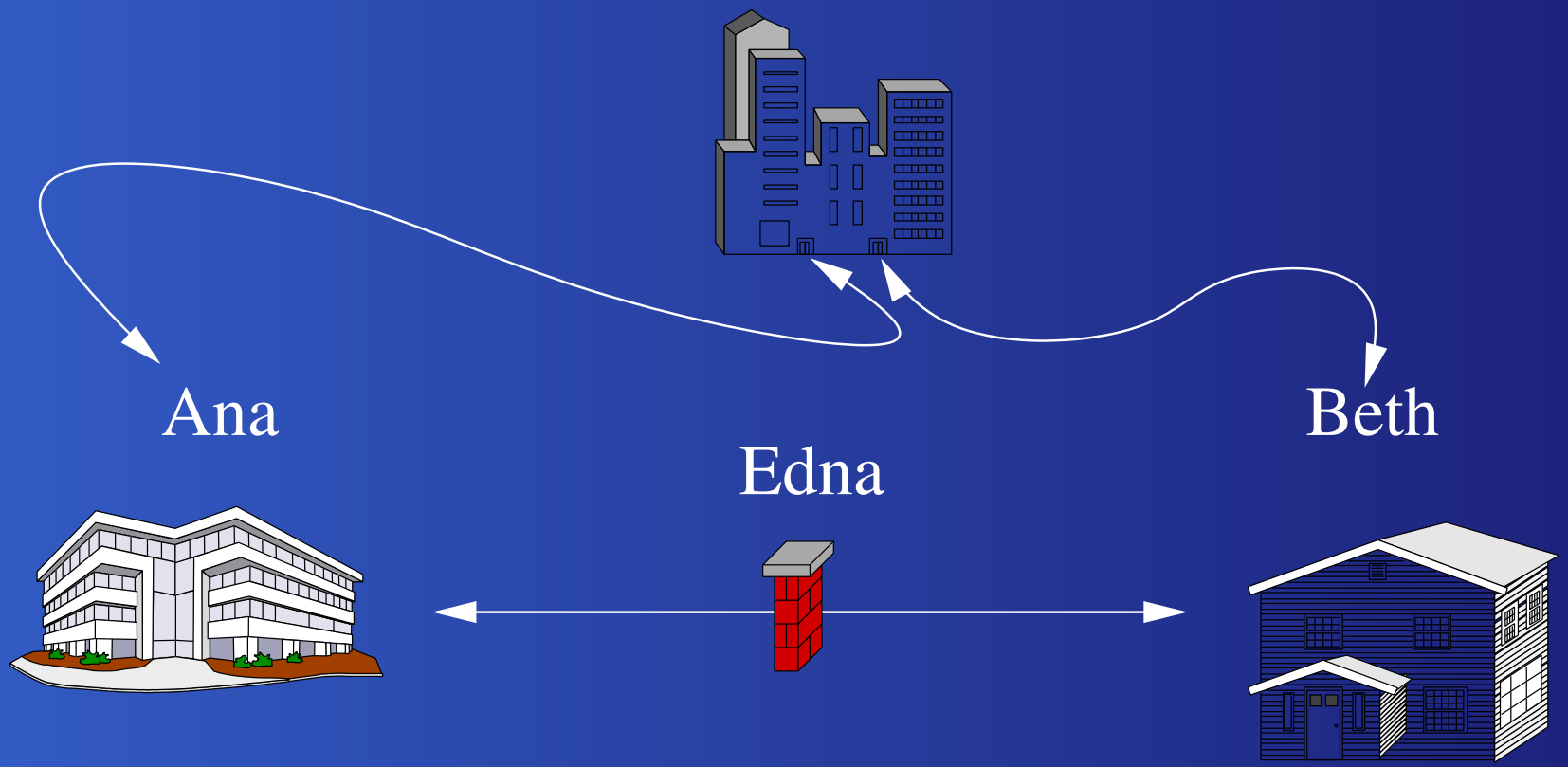
En	%	Fr	%	It	%	Es	%	Pt	%	Br	%
E	11.52	E	16.61	E	11.44	E	12.61	E	12.76	E	12.81
T	8.58	S	8.15	I	10.38	A	11.36	A	12.32	A	12.36
O	8.11	N	7.06	A	9.86	O	9.13	O	10.27	O	10.28
A	6.89	A	6.78	O	9.07	S	8.03	S	8.85	S	8.91
I	6.80	I	6.69	N	6.78	N	6.89	R	6.20	R	6.16
S	6.46	U	6.35	R	6.19	R	6.36	I	5.47	I	5.42
N	6.13	T	6.34	T	5.64	I	6.04	N	5.02	N	5.01
H	5.71	R	6.33	L	5.23	D	4.92	M	4.86	M	4.90
R	5.61	O	5.59	S	5.03	L	4.40	D	4.81	D	4.77
L	3.96	L	4.54	C	4.55	U	4.02	U	4.15	U	4.20



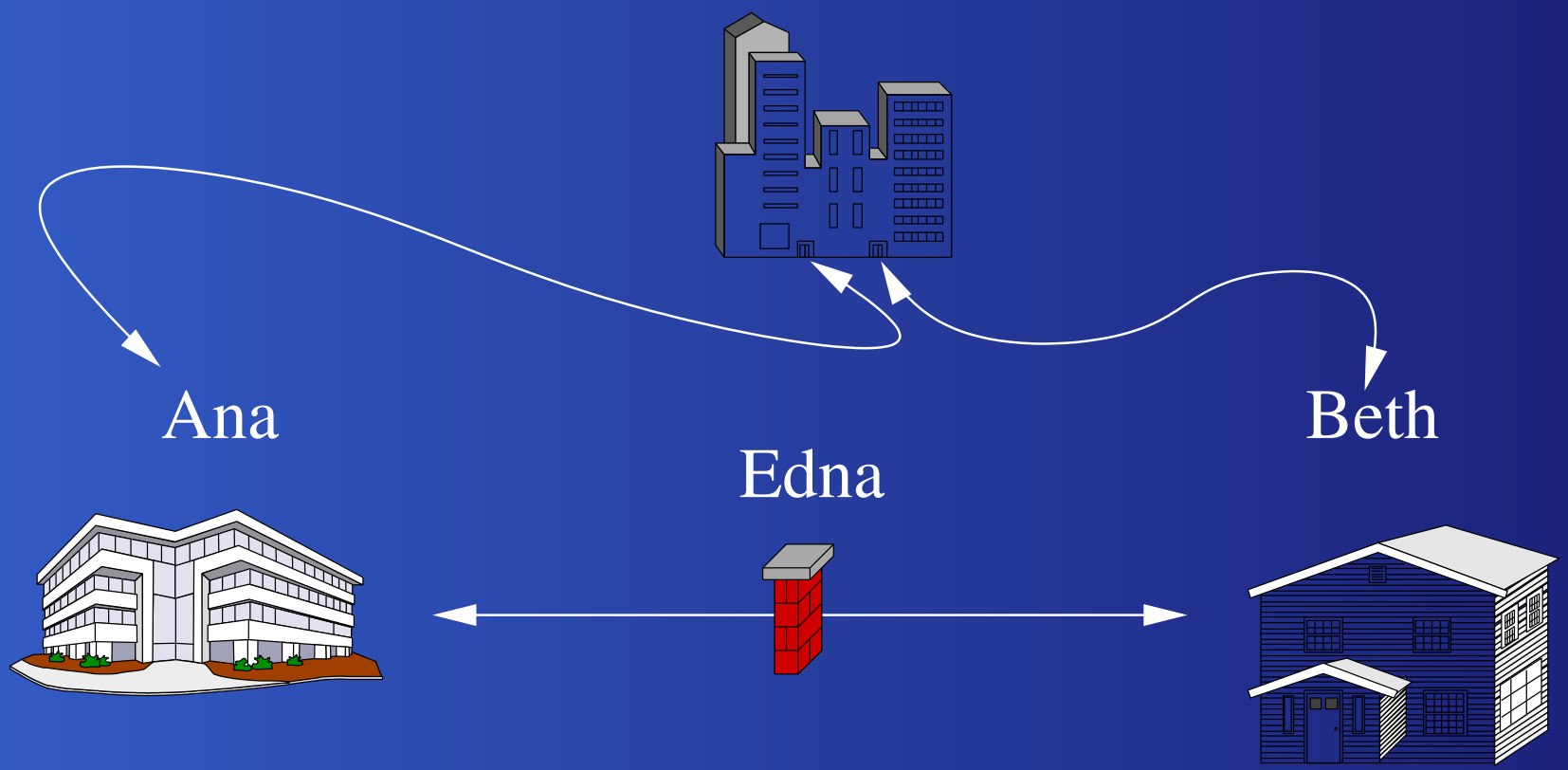
Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR
- $\vdots$
- ZZZZ $\leftrightarrow$ EYTO
- $26^4 = 456976$

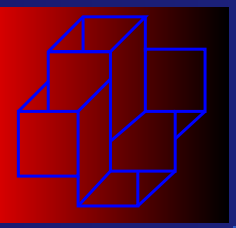
Assimétrica



Assimétrica

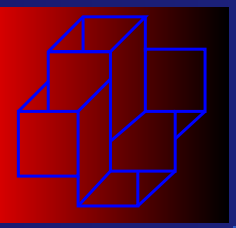


RSA e ECC



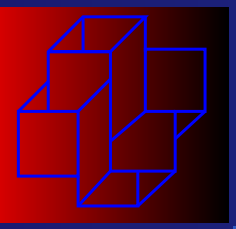
A Troca de Chaves

- Diffie-Hellman
- ElGamal
- Menezes-Vanstone
  - Problema do Logaritmo Discreto



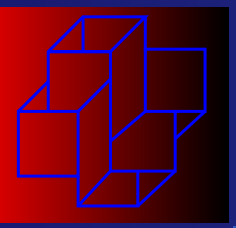
Compressão $\times$ Cifrar

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR
- RATO $\leftrightarrow$ YGUJ
- $\vdots$
- AAAA $\leftrightarrow$ GFHOGHD
- ZZZZ $\leftrightarrow$ EYTOYUI



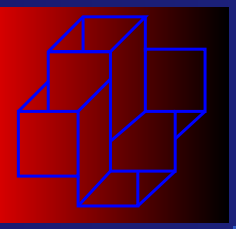
Número de bits recomendado

Simétrico	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521



Vulnerabilidade

- Existem algoritmos cuja segurança é baixa enquanto a entropia e difusão são máximas
- *Segredo Perfeito*:
  - One-time-pad
    - Vigenère-Vernam
    - Quadrados Latinos
  - Método de Criptografia com Números Irracionais



Vigenère-Vernam (One-time-pad)

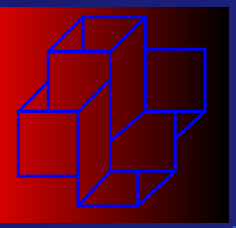
- ∅TOYNIMCEYVS∅E∅
- 00 ,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA

=

- 01 ,00,13,05,14,09,14,01,00,02,18,09,14,03,01

-

- 01 ,07,25,07,00,00,01,25,22,04,23,17,14,25,01



Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00 ,20,15,25,14,09,13,03,05, 25 ,22,19,00,05,00
- A∅MENINA∅BRINCA

=

- 01 ,00,13,05,14,09,14,01,00,02,18,09,14,03,01

-

- 01 ,07,25,07,00,00,01,25,22,04,23,17,14,25,01

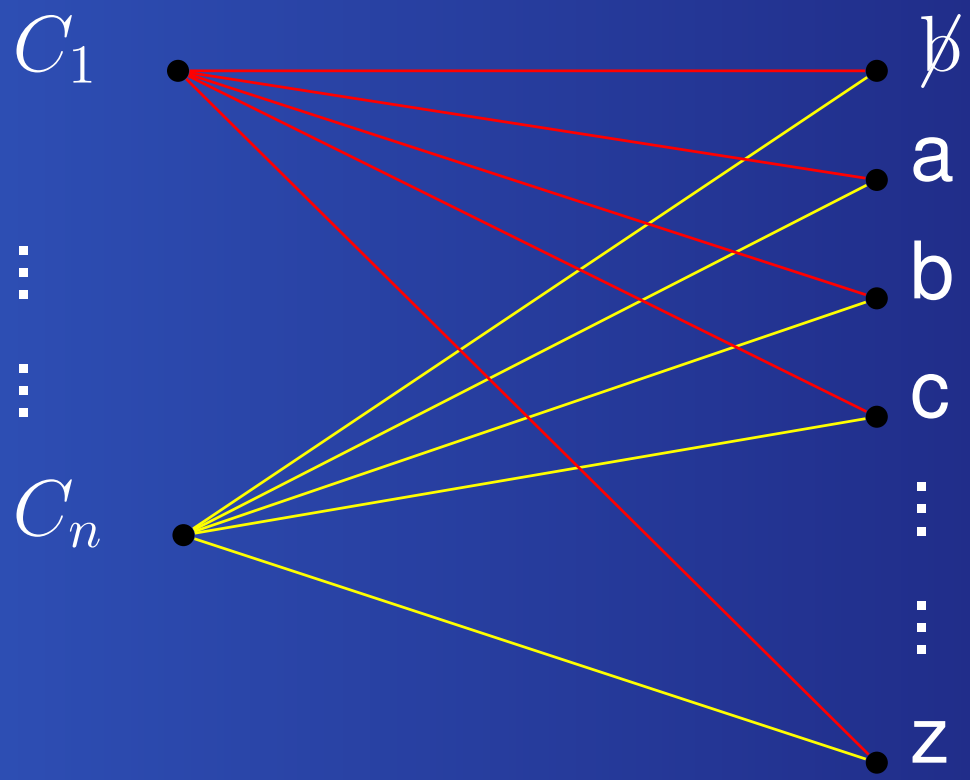
=

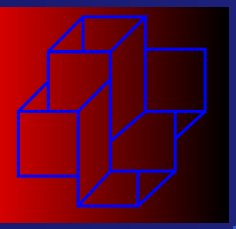
- ATACAR∅DE∅MANHA
- 01,20,01,03,01,18,00,04,05, 00 ,13,01,14,08,01

-

- 01,00,13,05,14,09,14,01,00, 02 ,18,09,14,03,01

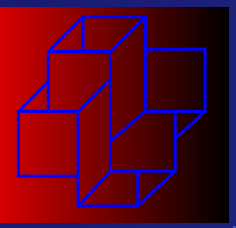
Diagrama





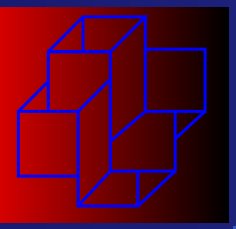
Método com Números Irracionais

- Motivações:



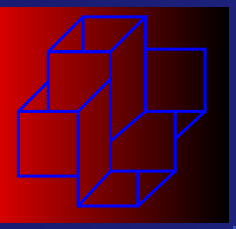
Método com Números Irracionais

- Motivações:
  - Possibilidade do combinar outra chave no final da mensagem



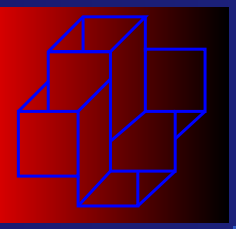
Método com Números Irracionais

- Motivações:
  - Possibilidade do combinar outra chave no final da mensagem
  - Transferir o custo do tamanho da chave para um custo computacional



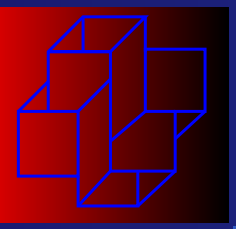
Método com Números Irracionais

- Motivações:
  - Possibilidade do combinar outra chave no final da mensagem
  - Transferir o custo do tamanho da chave para um custo computacional
  - Natureza diferente do One-time-pad



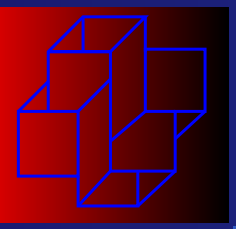
Método com Números Irracionais

- Princípio de funcionamento:



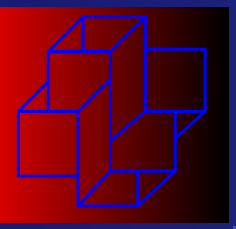
Método com Números Irracionais

- Princípio de funcionamento:
  - Escolher aleatoriamente uma expressão



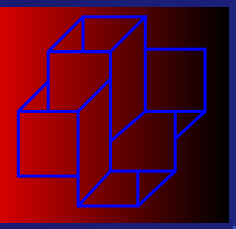
Método com Números Irracionais

- Princípio de funcionamento:
  - Escolher aleatoriamente uma expressão
  - Extrair a raiz



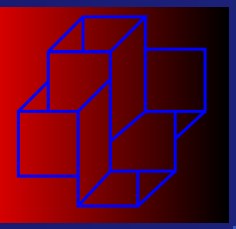
Método com Números Irracionais

- Princípio de funcionamento:
  - Escolher aleatoriamente uma expressão
  - Extrair a raiz
  - Verificar se é um número irracional



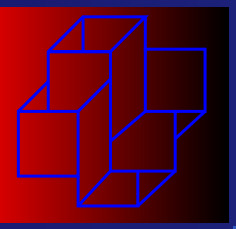
Método com Números Irracionais

- Princípio de funcionamento:
  - Escolher aleatoriamente uma expressão
  - Extrair a raiz
  - Verificar se é um número irracional
  - Usar a mantissa como One-time-pad



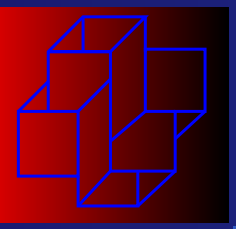
Método com Números Irracionais

- Características:



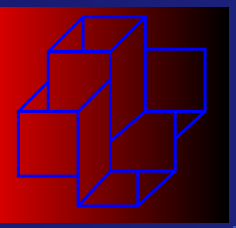
Método com Números Irracionais

- Características:
  - Semântica da chave



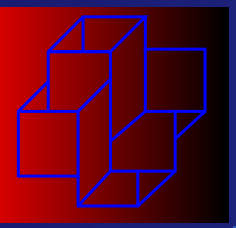
Método com Números Irracionais

- Características:
  - Semântica da chave
  - Números irracionais são densos



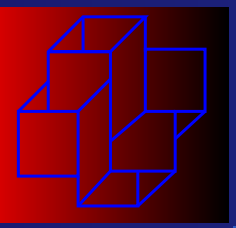
Método com Números Irracionais

- Características:
  - Semântica da chave
  - Números irracionais são densos
  - Raízes quadradas são normais na base 2



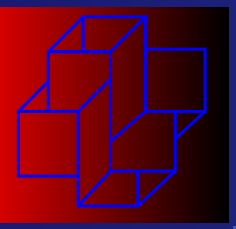
Método com Números Irracionais

- Características:
  - Semântica da chave
  - Números irracionais são densos
  - Raízes quadradas são normais na base 2
  - A escolha da chave é aleatória



Método com Números Irracionais

- Características:
  - Semântica da chave
  - Números irracionais são densos
  - Raízes quadradas são normais na base 2
  - A escolha da chave é aleatória
  - Chaves de tamanhos variados em um *Segredo Perfeito*



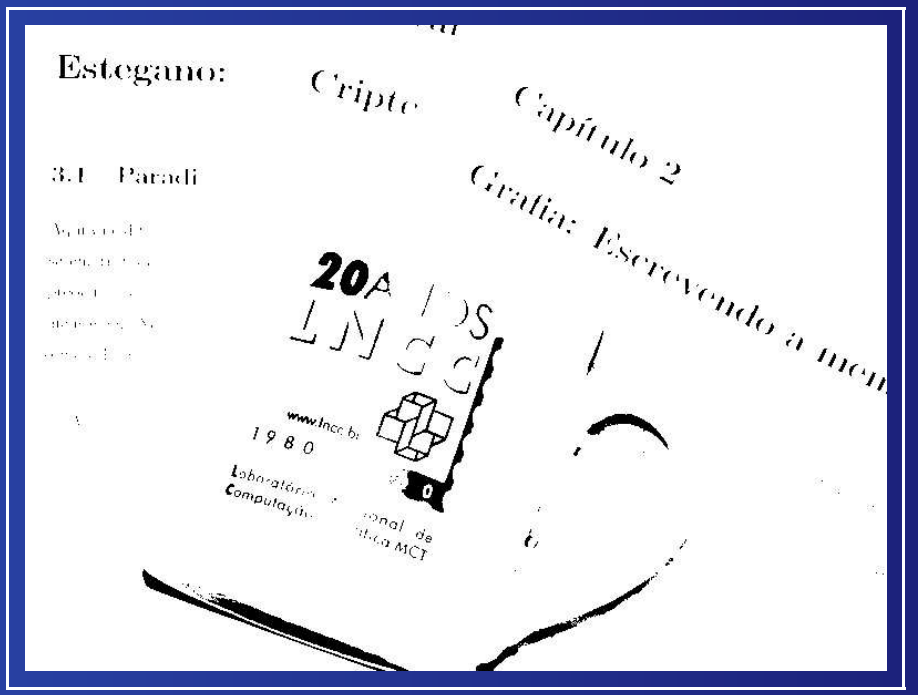
Grau de Segurança

Algoritmos	Segurança
Assimétricos	computacional
Simétricos	probabilística
Segredo Perfeito	matemática

Domínio Espacial

Todos os 8 bits.

Domínio Espacial

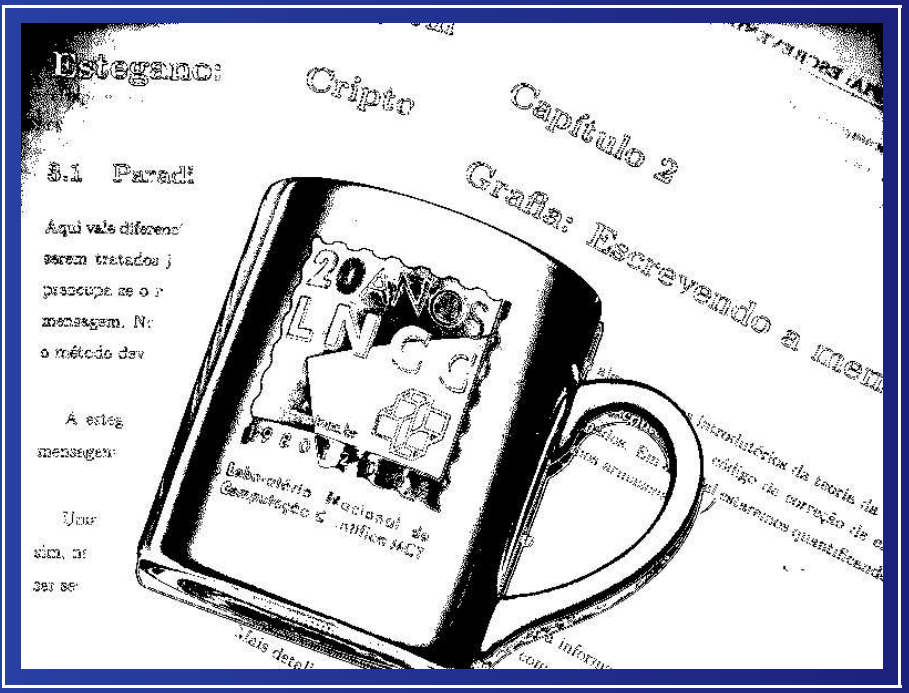


Posição do Bit: 12345678

Domínio Espacial

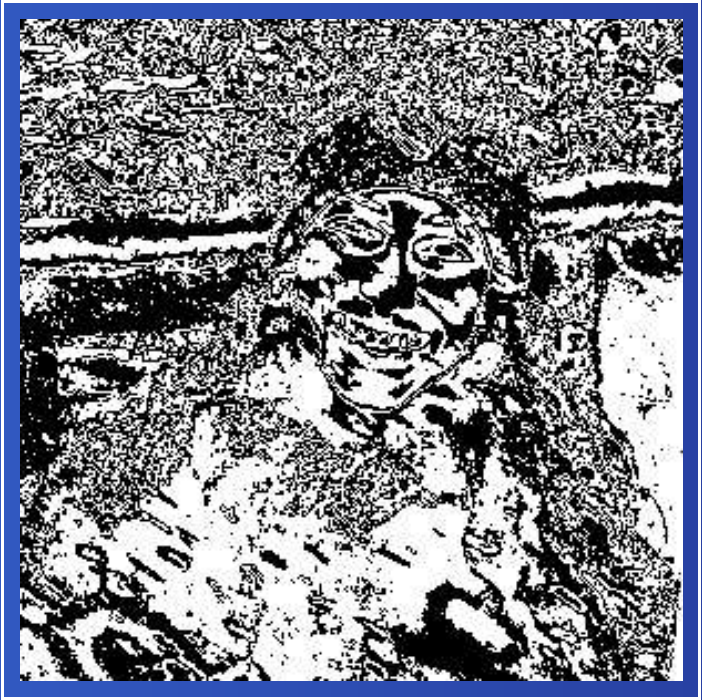
Posição do Bit: 12345678

Domínio Espacial



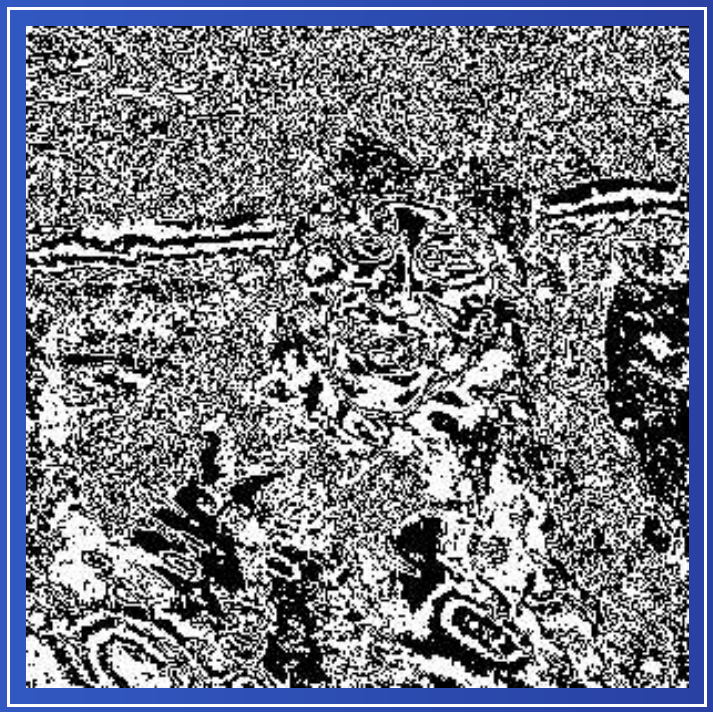
Posição do Bit: 12345678

Domínio Espacial



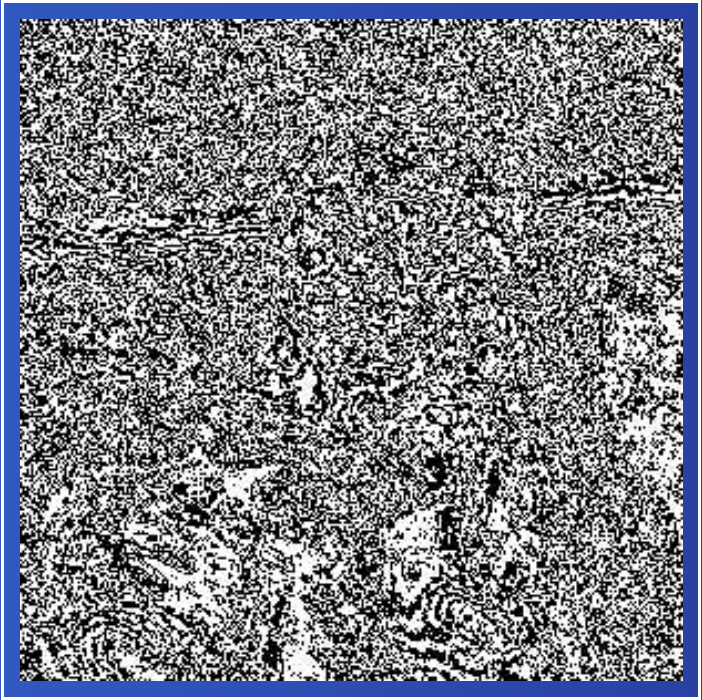
Posição do Bit: 12345678

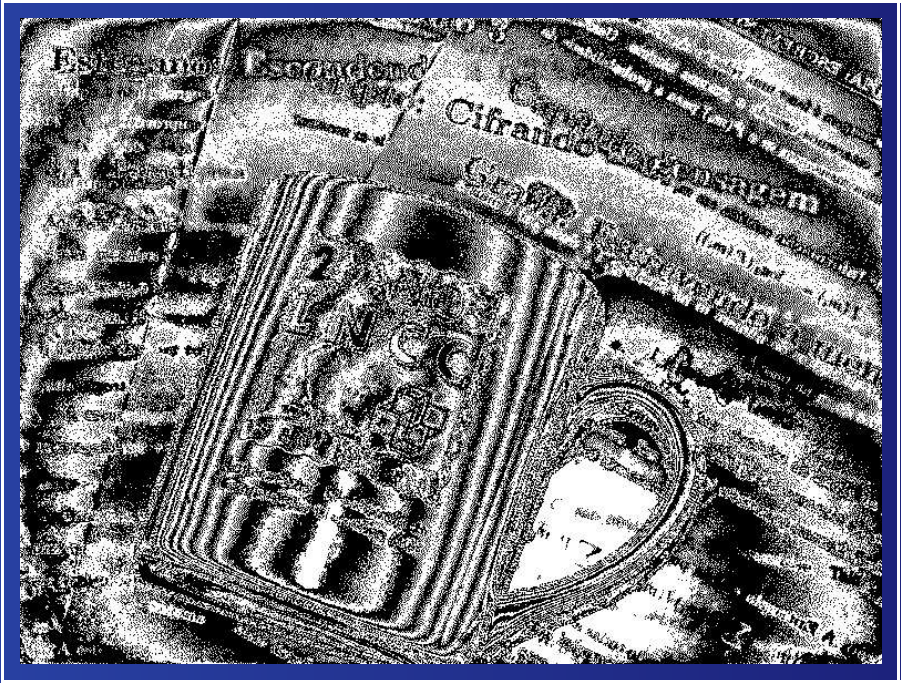
Domínio Espacial



Posição do Bit: 12345678

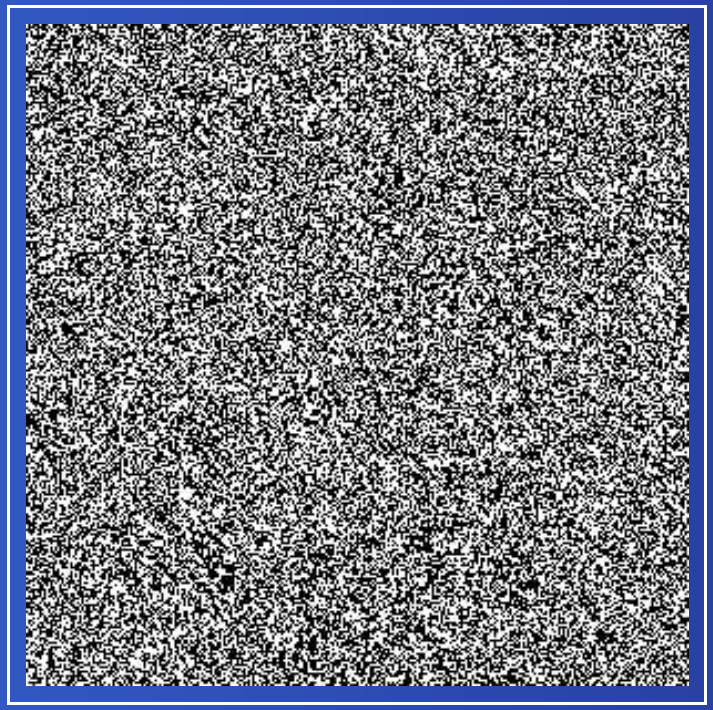
Domínio Espacial



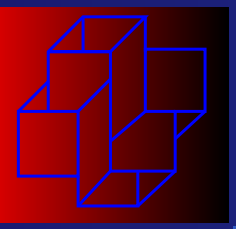


Posição do Bit: 12345678

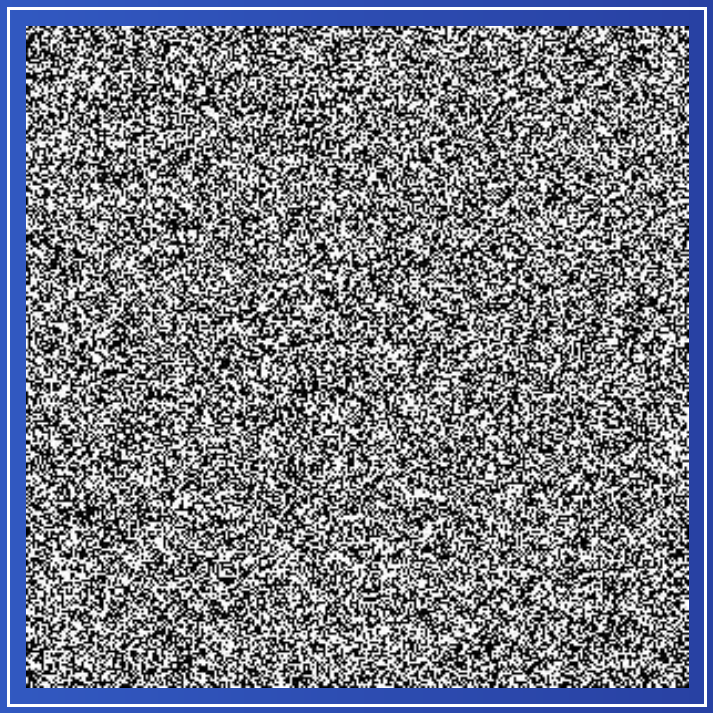
Domínio Espacial

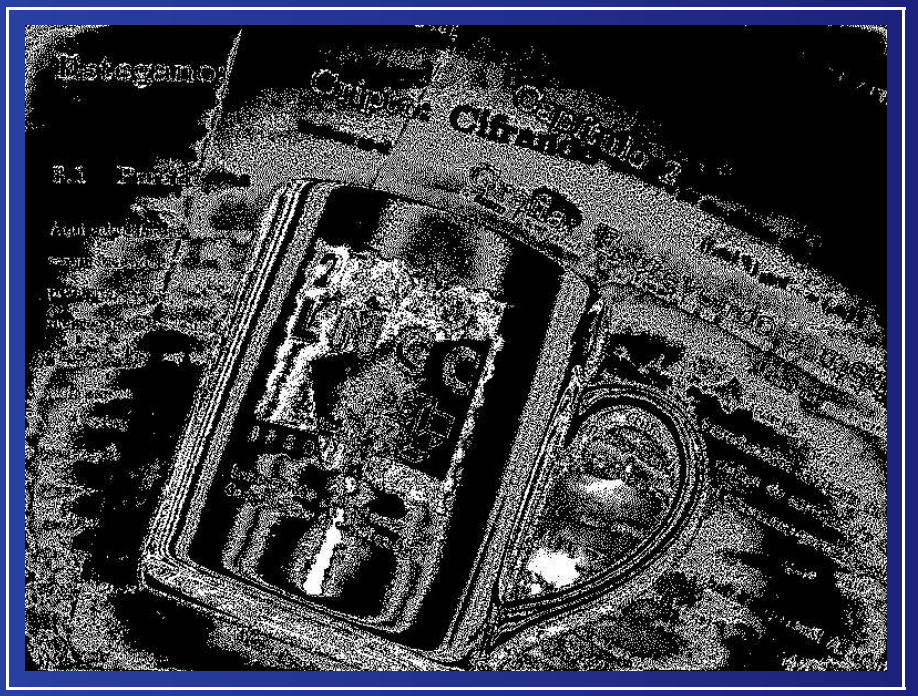


Posição do Bit: 1234567**8**

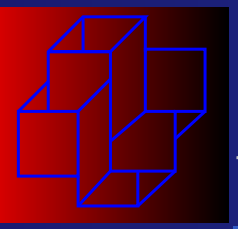


Domínio Espacial



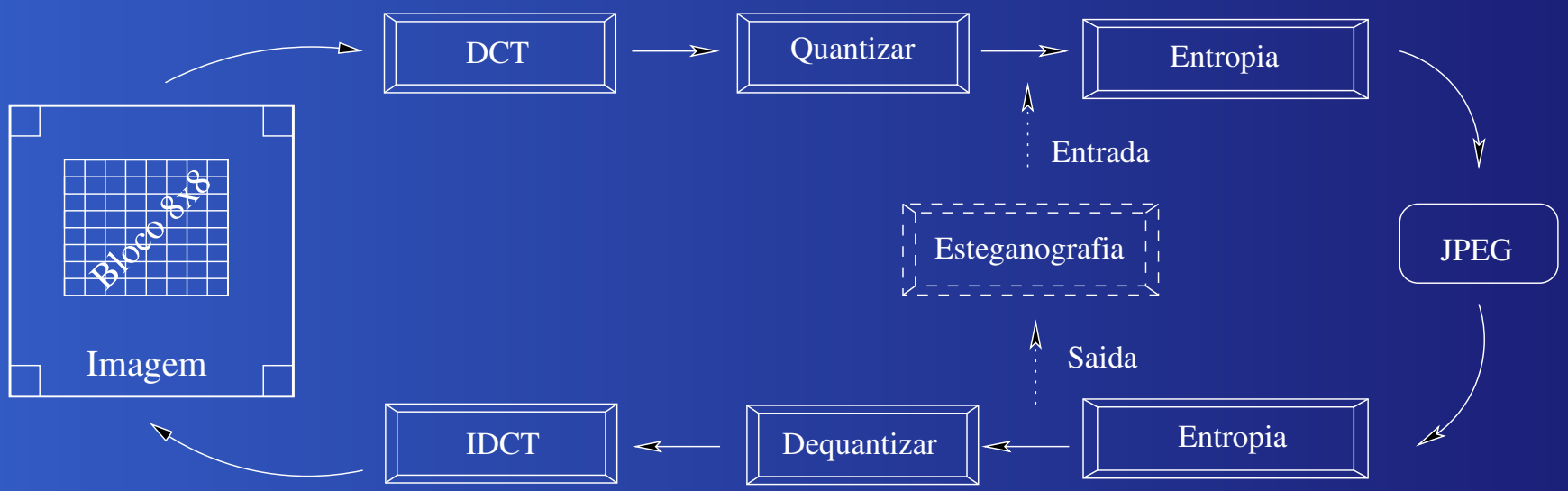


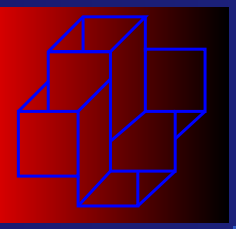
Posição do Bit: 1234567**8**



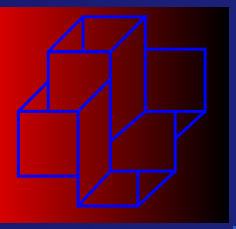
Ataque Visual

Esquema de esteganografia em JPEG

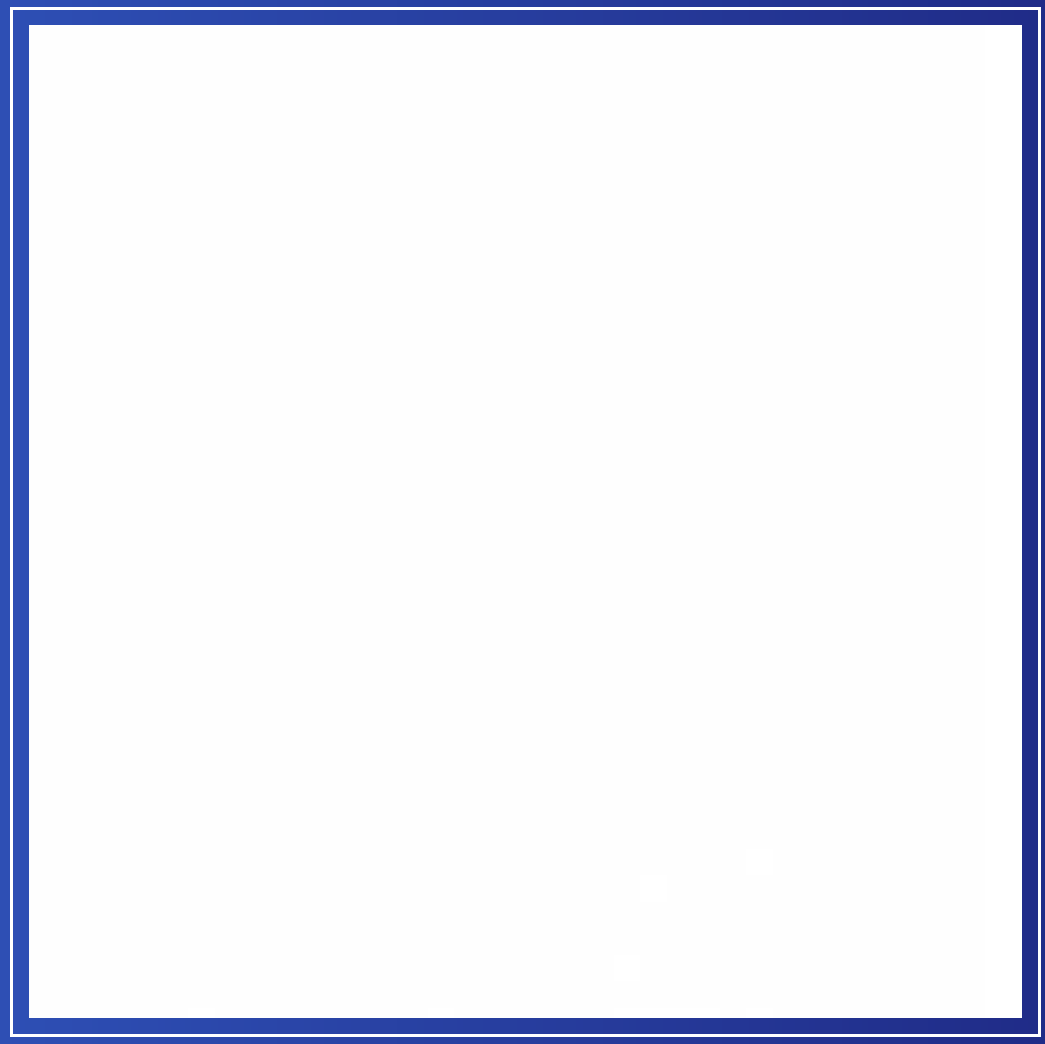




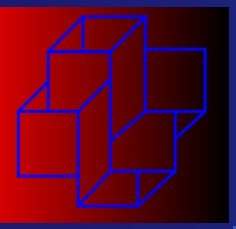
Domínio de Freqüência



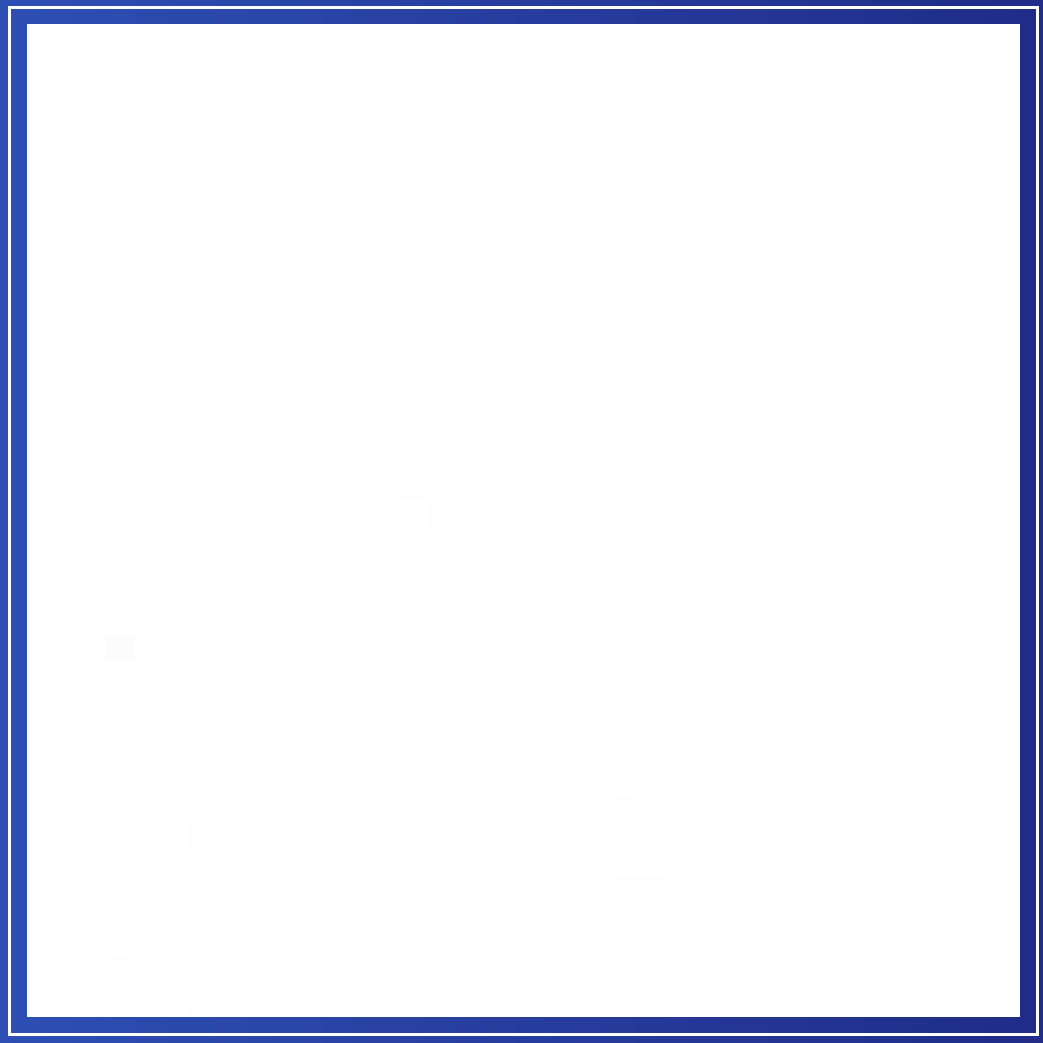
Domínio de Freqüência



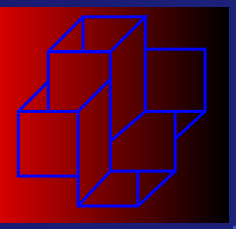
Ordem 1 Coeficientes alterados: 50632



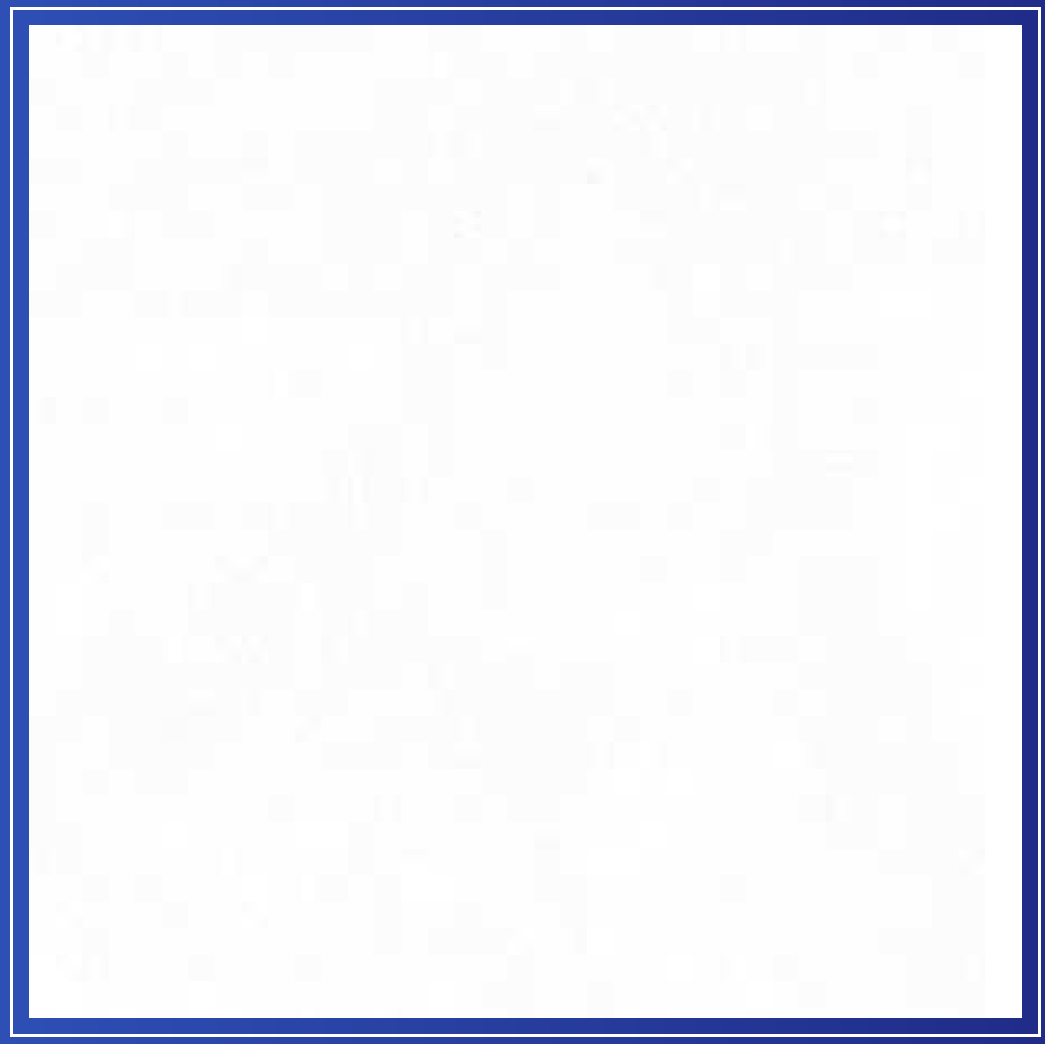
Domínio de Freqüência



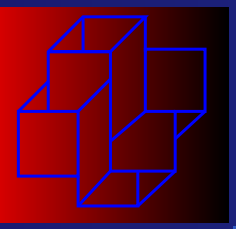
Ordem 2 Coeficientes alterados: 34795



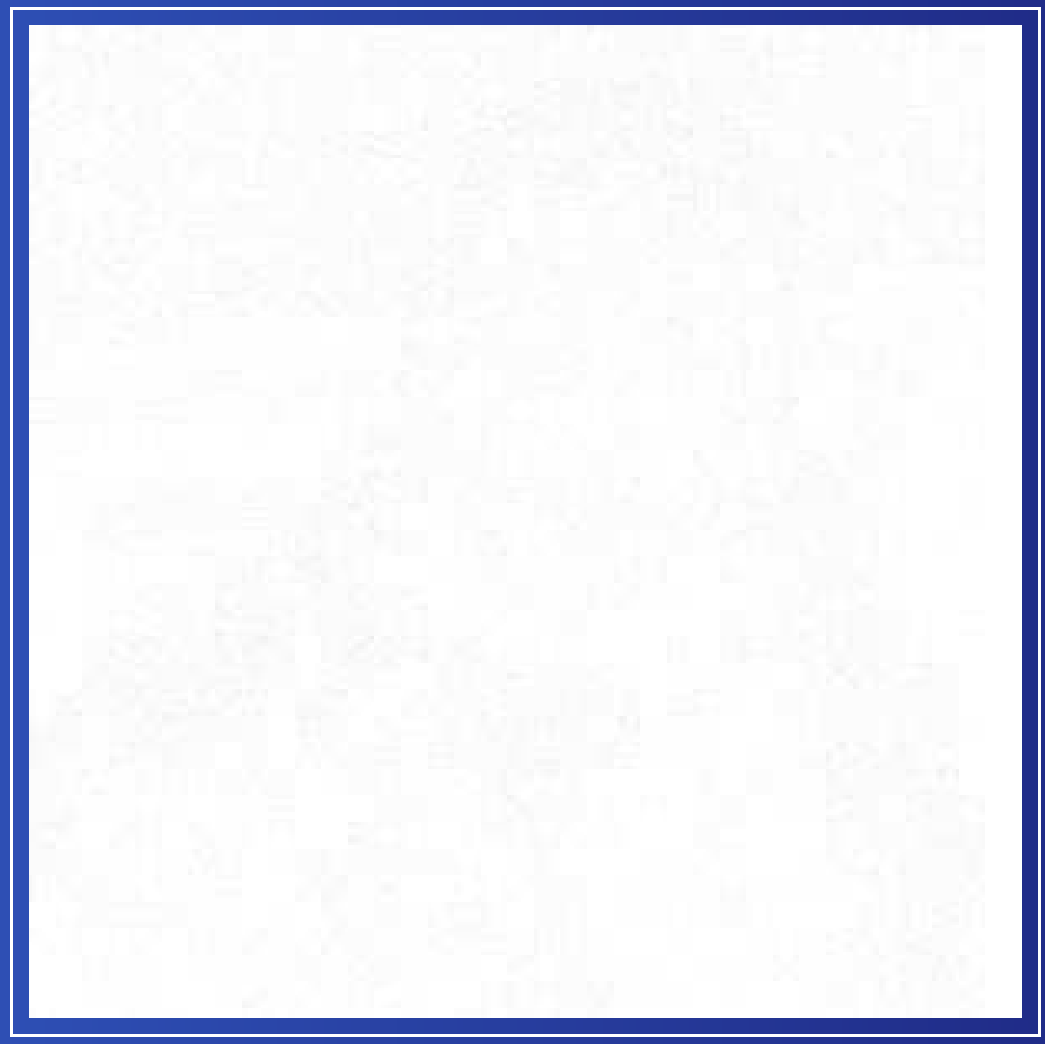
Domínio de Freqüência



Ordem 3 Coeficientes alterados: 20952

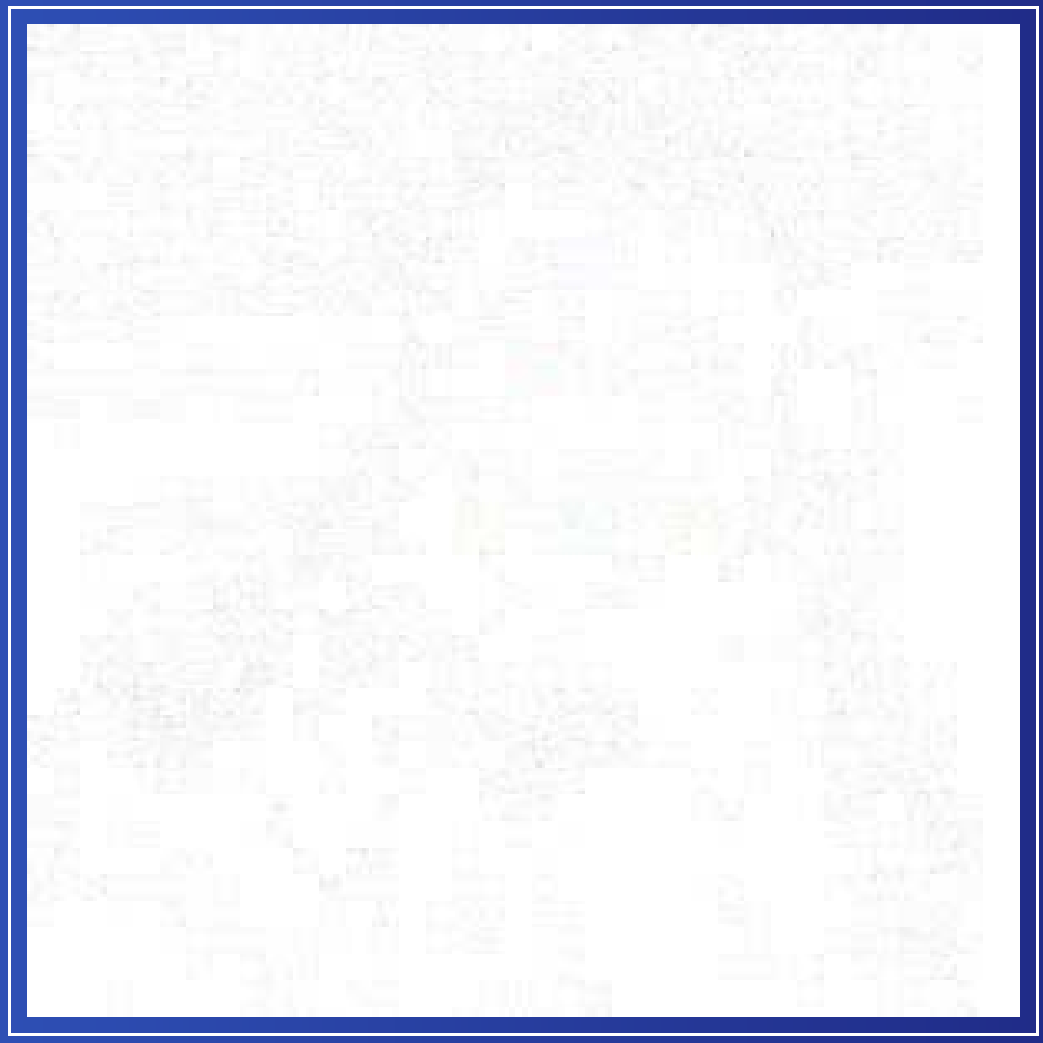


Domínio de Freqüência

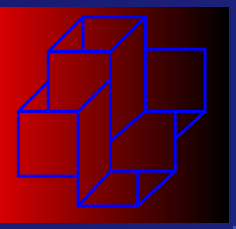


Ordem 4 Coeficientes alterados: 10522

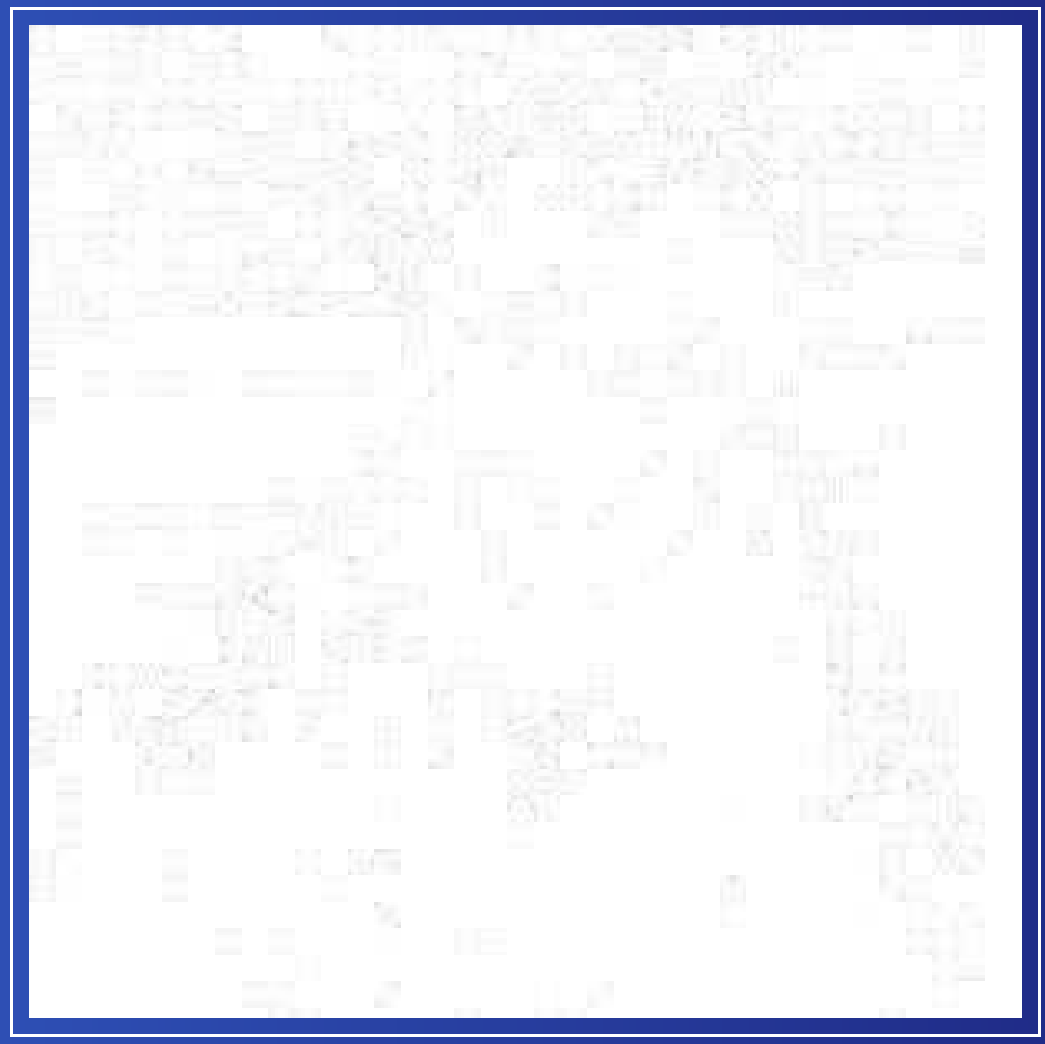
Domínio de Freqüência



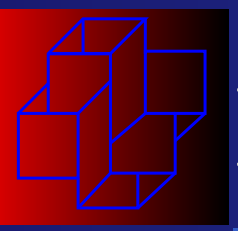
Ordem 5 Coeficientes alterados: 4260



Domínio de Freqüência

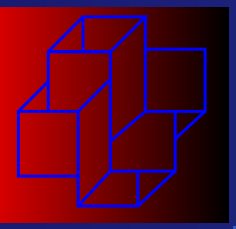


Ordem 6 Coeficientes alterados: 1343



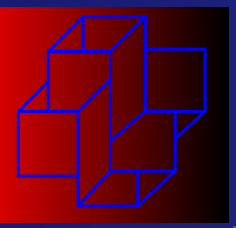
Domínio de Freqüência

Ordem 7 Coeficientes alterados: 288



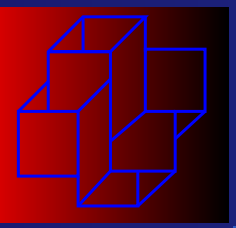
Domínio de Freqüência

Ordem 8 Coeficientes alterados: 28



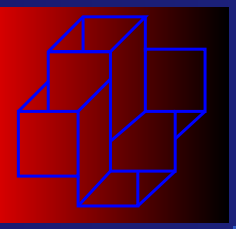
Grau de Segurança

- Os testes, em seqüências de imagens, mostraram que podemos usar outros bits diferentes do LSB aumentando a segurança.
- Uma esteganografia com *Segredo Perfeito* pode ser feita quando se cria ou escolhe um meio com as posições pré-determinada para transmitir a mensagem.



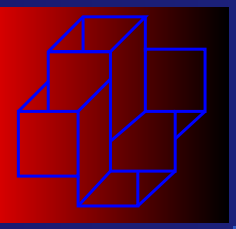
Resultados

- Conceito de semântica



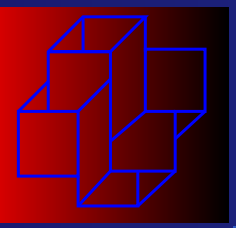
Resultados

- Conceito de semântica
- *Segredo Perfeito* sem ser do tipo One-time-pad



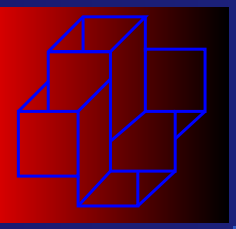
Resultados

- Conceito de semântica
- *Segredo Perfeito* sem ser do tipo One-time-pad
- *Segredo Perfeito* na esteganografia



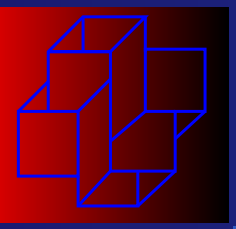
Resultados

- Conceito de semântica
- *Segredo Perfeito* sem ser do tipo One-time-pad
- *Segredo Perfeito* na esteganografia
- Esteganografia em bits diferentes do LSB



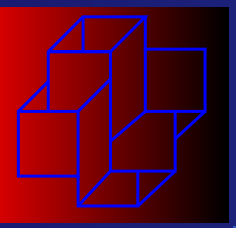
Resultados

- Conceito de semântica
- *Segredo Perfeito* sem ser do tipo One-time-pad
- *Segredo Perfeito* na esteganografia
- Esteganografia em bits diferentes do LSB
- Análise da segurança dos algoritmos



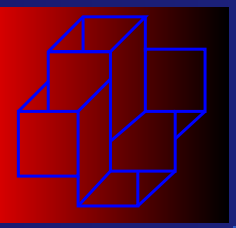
Trabalhos Futuros

- É possível ter sempre uma chave menor na criptografia com números irracionais?



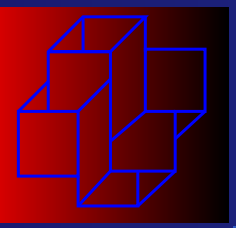
Trabalhos Futuros

- É possível ter sempre uma chave menor na criptografia com números irracionais?
- Tal método poderia ser usado para altíssima compressão?



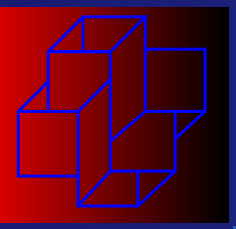
Trabalhos Futuros

- É possível ter sempre uma chave menor na criptografia com números irracionais?
- Tal método poderia ser usado para altíssima compressão?
- É possível construir um *Segredo Perfeito* assimétrico?



Trabalhos Futuros

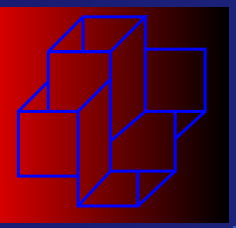
- É possível ter sempre uma chave menor na criptografia com números irracionais?
- Tal método poderia ser usado para altíssima compressão?
- É possível construir um *Segredo Perfeito* assimétrico?
- Existe outro tipo de *Segredo Perfeito* na esteganografia?



Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges



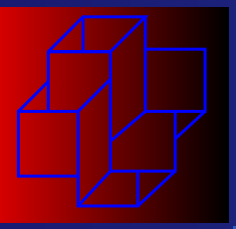
Segredo Perfeito

- Criptografia:

$$P_C(M) = P(M)$$

- Esteganografia:

$$P_M(W) = P(W)$$

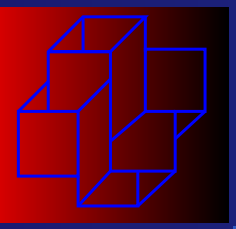


Divisão do trabalho

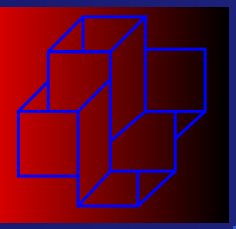
Grafia

Cripto

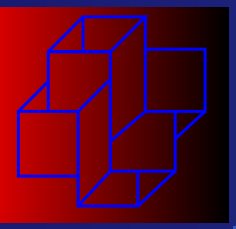
Estegano



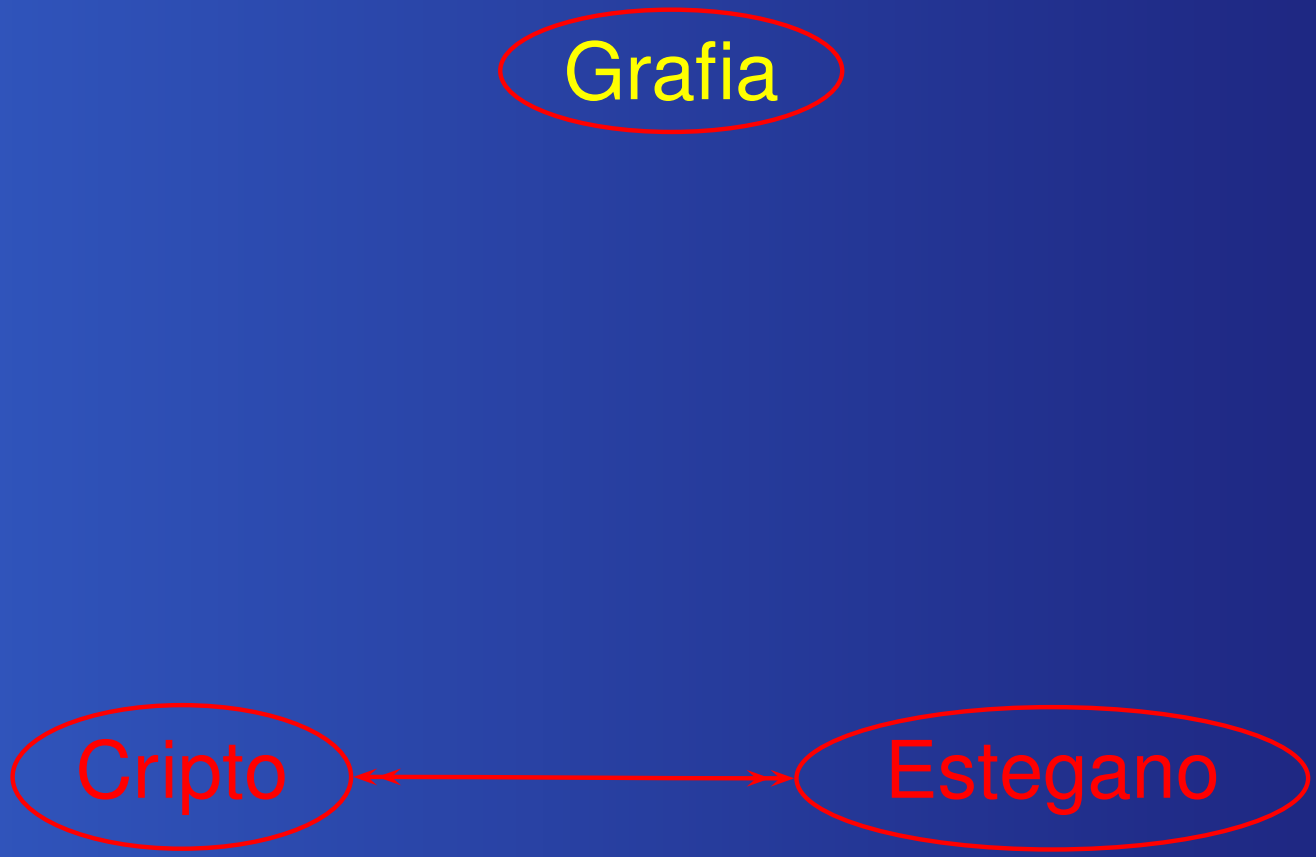
Divisão do trabalho

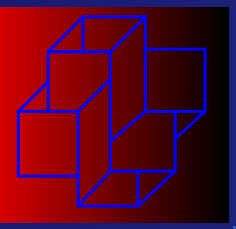


Divisão do trabalho



Divisão do trabalho





Divisão do trabalho