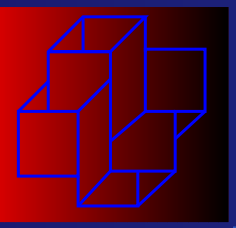
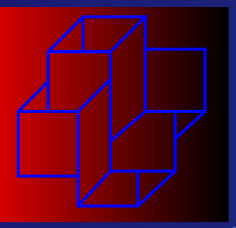


Steganography with Public-Key Cryptography for Videoconference

XXX CNMAC - Set/2007

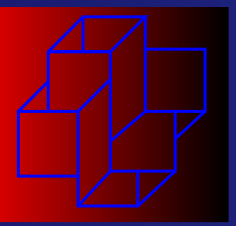
Fábio Borges de Oliveira



Steganography

Source:

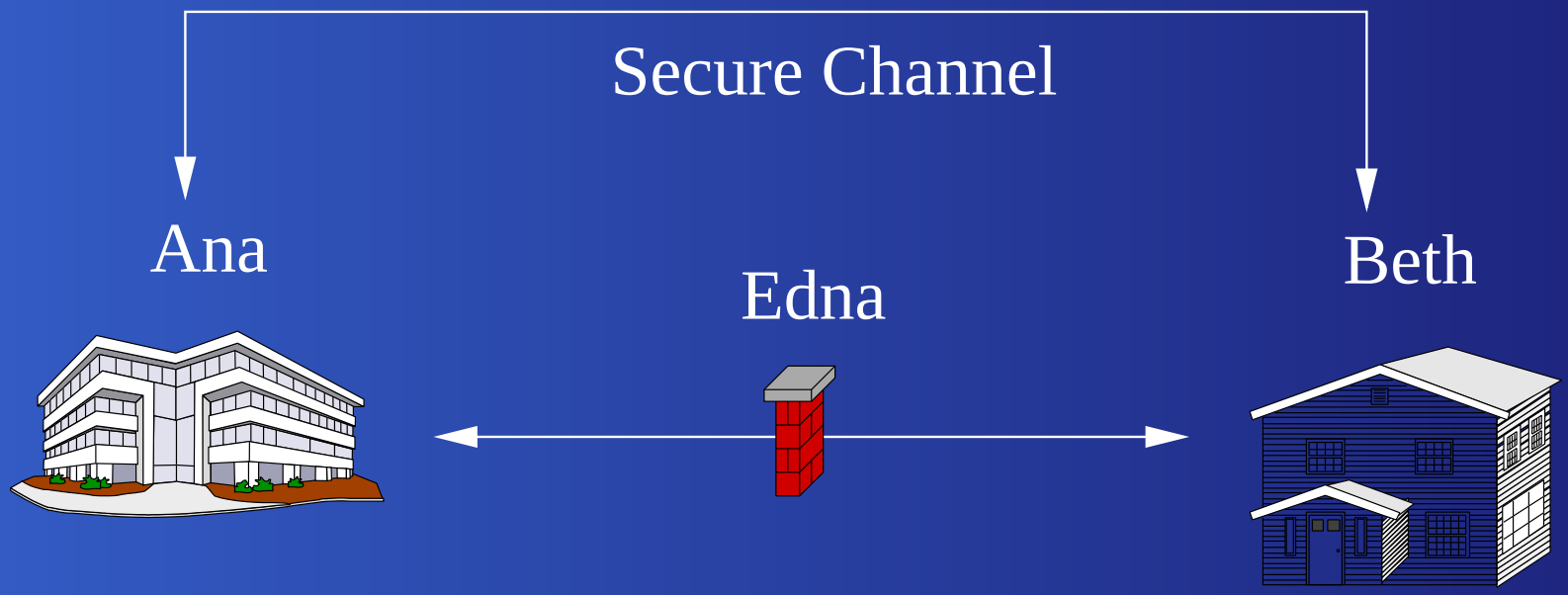
Steganography:



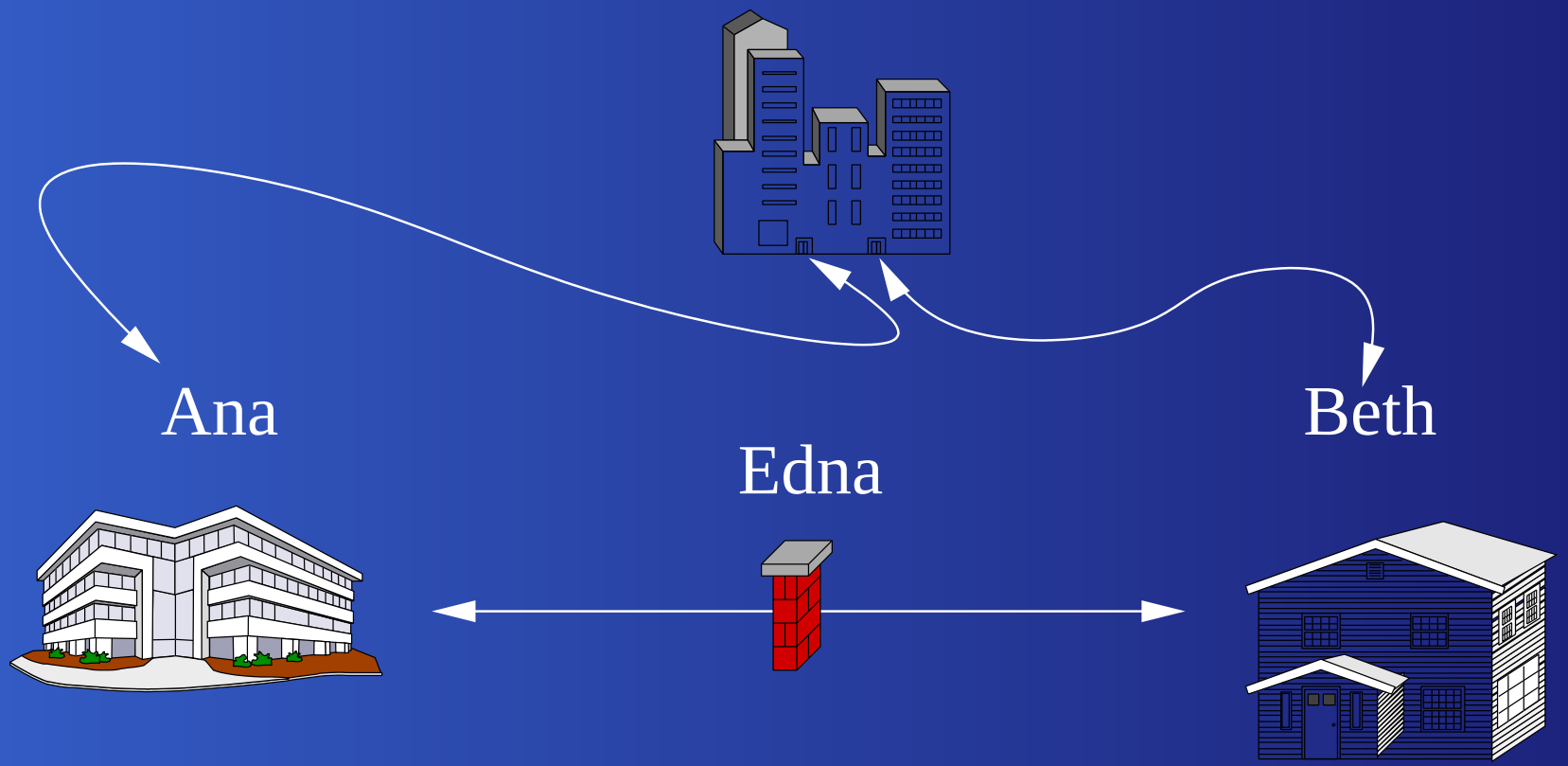
Why do we need to use it?

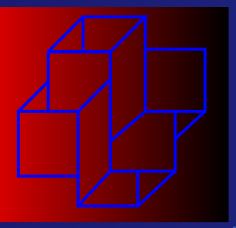
1. The enemy could interrupt the message
2. There is the Shor's quantum algorithm that can factor huge numbers quickly $O(n^3)$
3. Someone might find a way to break the cryptosystem

Symmetric



Asymmetric





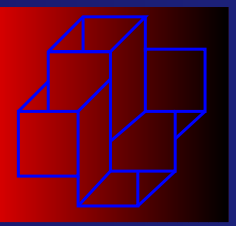
RSA

$$\varphi = \varphi(pq) = (p-1)(q-1)$$

Choose a so that $\gcd(a, \varphi) = 1$

$$ab \equiv 1 \bmod \varphi.$$

$$x^{ab} \equiv x \bmod pq \quad \forall x \in \mathbb{Z}.$$

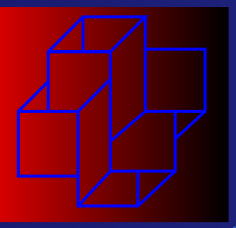


Diffie-Hellman

Alice chooses k with $gcd(k, pq) = 1$ and sends the values of k and pq. Then, Alice chooses a r, computes k^r and sends the result to Bob while keeping r secret. At the same moment Bob chooses s, computes k^s and sends the result to Alice while keeping s secret.
So, both form the candidate exponent

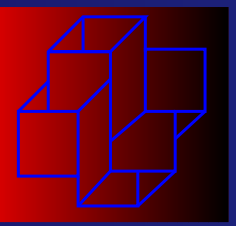
$$a = (k^r)^s = (k^s)^r.$$

To verify if a is a valid RSA exponent, Alice computes $gcd(a, \varphi) = 1$. If a is not valid they repeat the process.



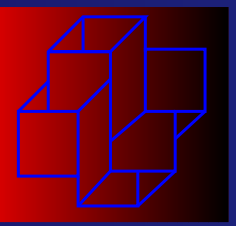
Key agreement

- Diffie-Hellman
- ElGamal
- Menezes-Vanstone
  - Discrete Logarithmic Problem



Steganography and Public-key

Steganography using public-key cryptography cannot use a static media, like an image, but it requires a data stream, like a dialog.



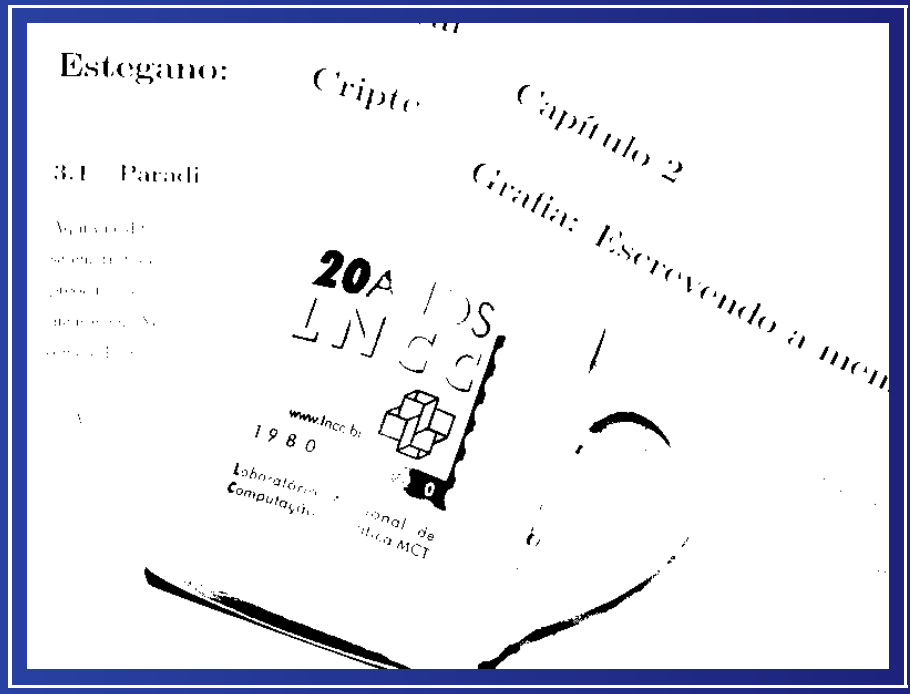
Videoconference

- We have the option to use the sound or the video
- We chose the ITU-T H263 - video codec protocol
- An H263 video stream contains I-frame, P-frame and B-frame
- Hiding in a sequence of JPEG

Spatial domain

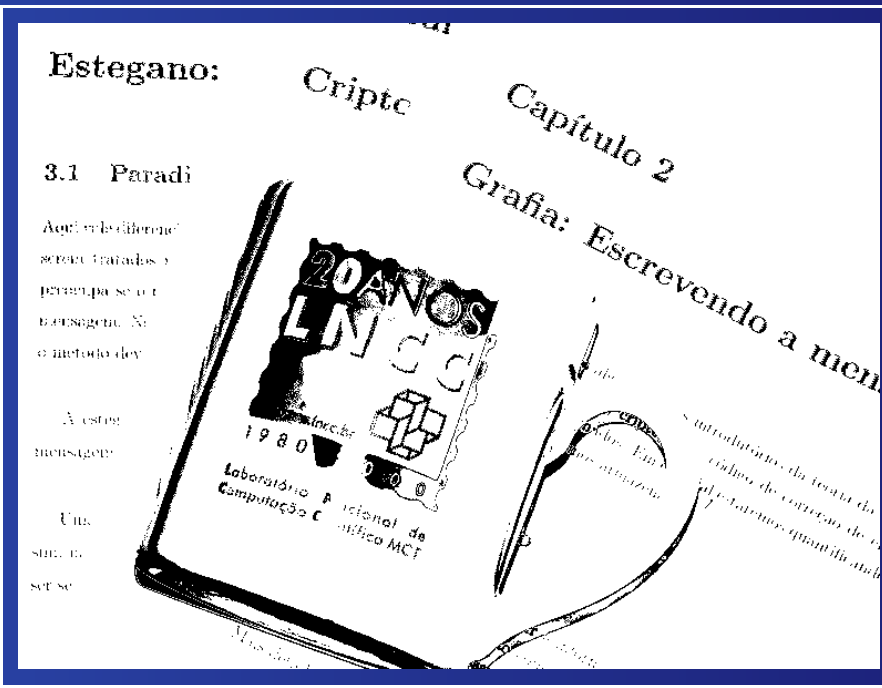
For every 8 bits.

Spatial domain



Bit position: 12345678

Spatial domain

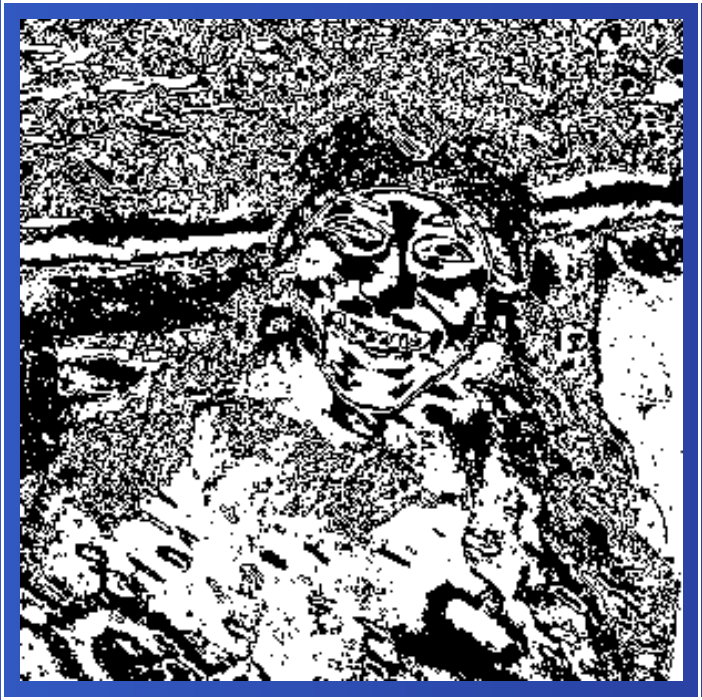


Bit position: 12345678

Spatial domain

Bit position: 12345678

Spatial domain

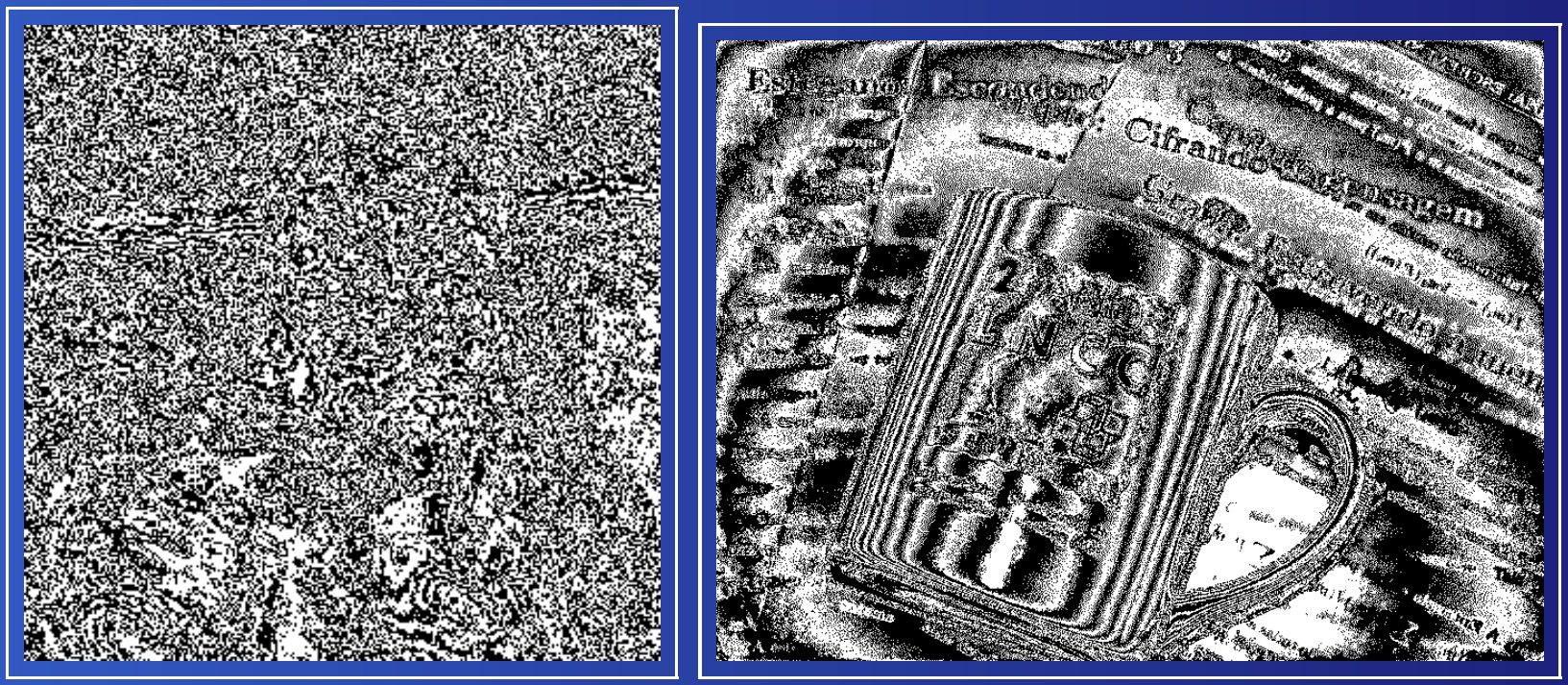


Bit position: 12345678

Spatial domain

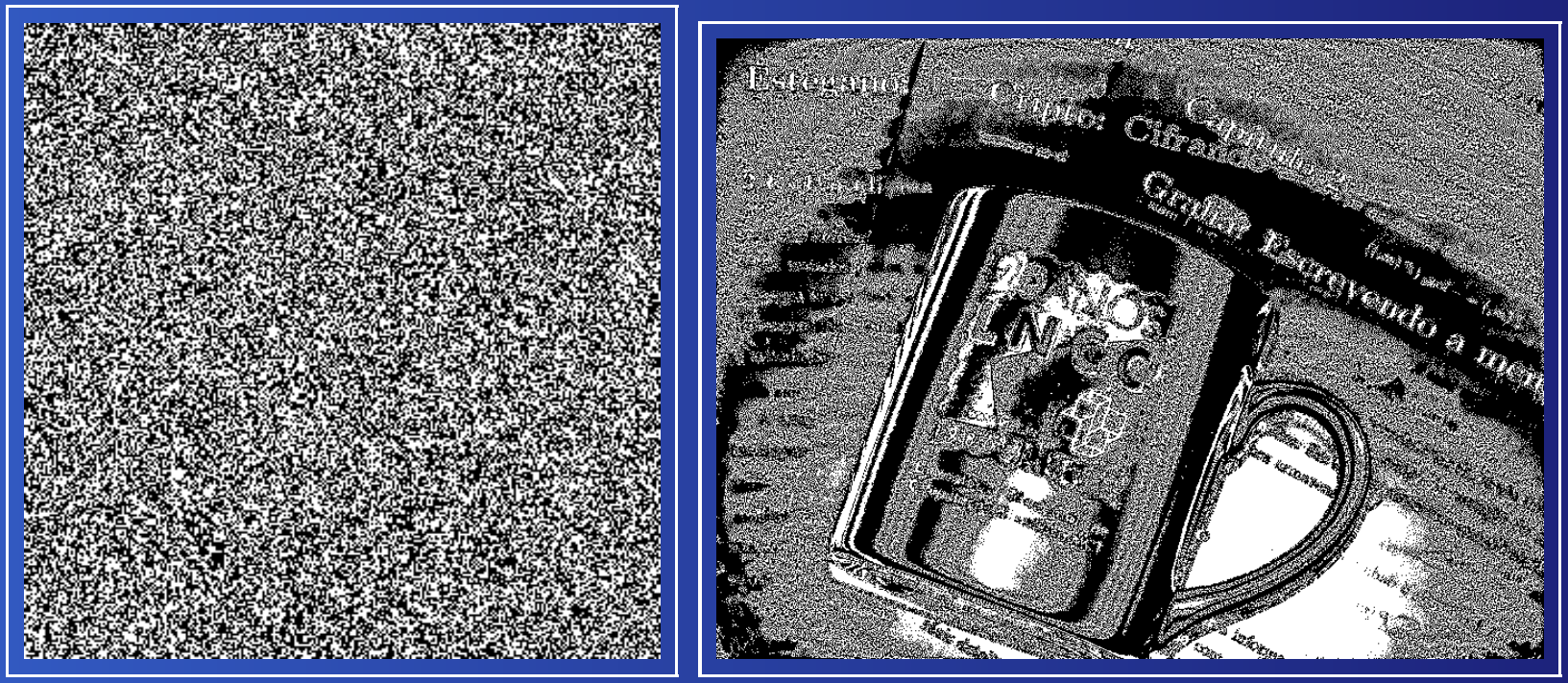
Bit position: 12345678

Spatial domain



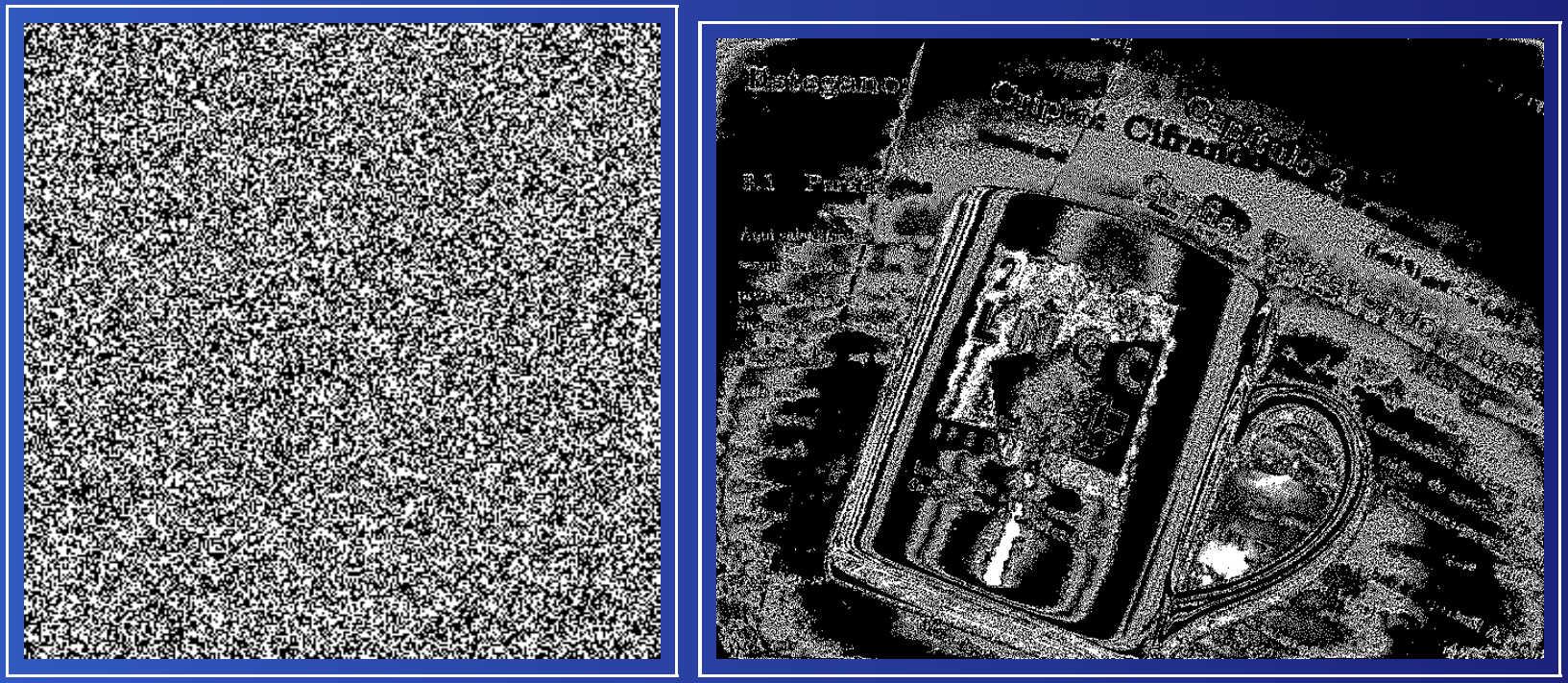
Bit position: 12345678

Spatial domain

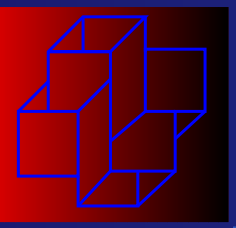


Bit position: 1234567**8**

Spatial domain

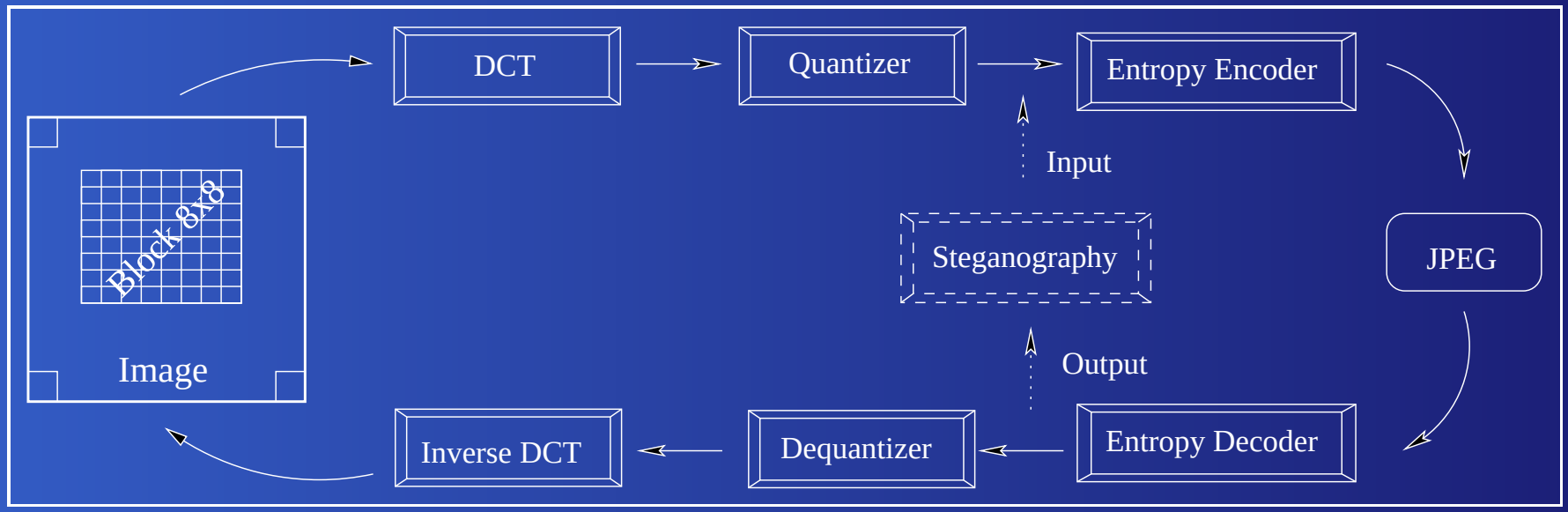


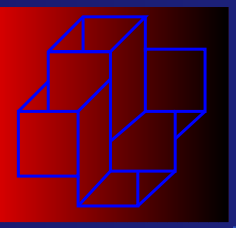
Bit position: 1234567**8**



Visual attack

Steganographic scheme in JPEG





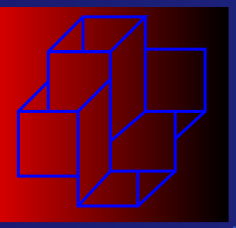
Discrete Cosine Transform (DCT)

$$F[m,n] = \frac{C(m)}{2}\frac{C(n)}{2}\sum_{x=0}^{7}\sum_{y=0}^{7} P[x,y]\cos\alpha\cos\beta,$$

$$\alpha = \frac{(2x+1)m\pi}{16},$$

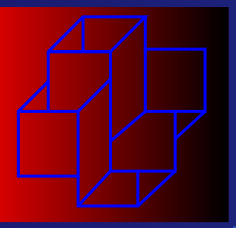
$$\beta = \frac{(2y+1)n\pi}{16}$$

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} \text{ for } k = 0, \\ 1 \text{ for all other values of } k. \end{cases}$$



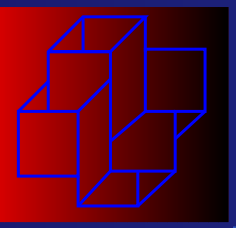
The quantization

$$F'[m,n] = \frac{F[m,n]}{Q[m,n]}$$



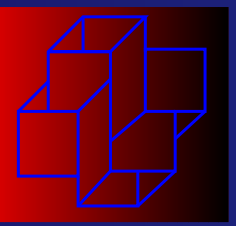
Pixel matrix P

$$P = \begin{bmatrix} 0 & 0 & 0 & 200 & 200 & 0 & 0 & 0 \\ 0 & 0 & 200 & 200 & 200 & 200 & 0 & 0 \\ 0 & 200 & 200 & 200 & 200 & 200 & 200 & 0 \\ 200 & 200 & 200 & 200 & 200 & 200 & 200 & 200 \\ 200 & 200 & 200 & 200 & 200 & 200 & 200 & 200 \\ 0 & 200 & 200 & 200 & 200 & 200 & 200 & 0 \\ 0 & 0 & 200 & 200 & 200 & 200 & 0 & 0 \\ 0 & 0 & 0 & 200 & 200 & 0 & 0 & 0 \end{bmatrix}$$



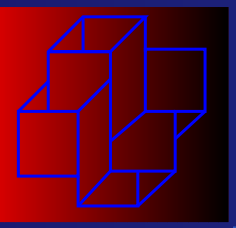
Quantization matrix Q

$$Q = \begin{bmatrix} 6 & 11 & 16 & 21 & 26 & 31 & 36 & 41 \\ 11 & 16 & 21 & 26 & 31 & 36 & 41 & 46 \\ 16 & 21 & 26 & 31 & 36 & 41 & 46 & 51 \\ 21 & 26 & 31 & 36 & 41 & 46 & 51 & 56 \\ 26 & 31 & 36 & 41 & 46 & 51 & 56 & 61 \\ 31 & 36 & 41 & 46 & 51 & 56 & 61 & 66 \\ 36 & 41 & 46 & 51 & 56 & 61 & 66 & 71 \\ 41 & 46 & 51 & 56 & 61 & 66 & 71 & 76 \end{bmatrix}$$



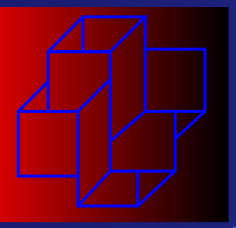
Consider the matrices

- A that has not suffered steganography
- B that has changed in every second LSB of coefficients AC, whose modulus is greater than two
- C that has changed only the second LSB of $F'[0, 2]$
- D that has changed the LSB of AC, whose modulus is greater than one

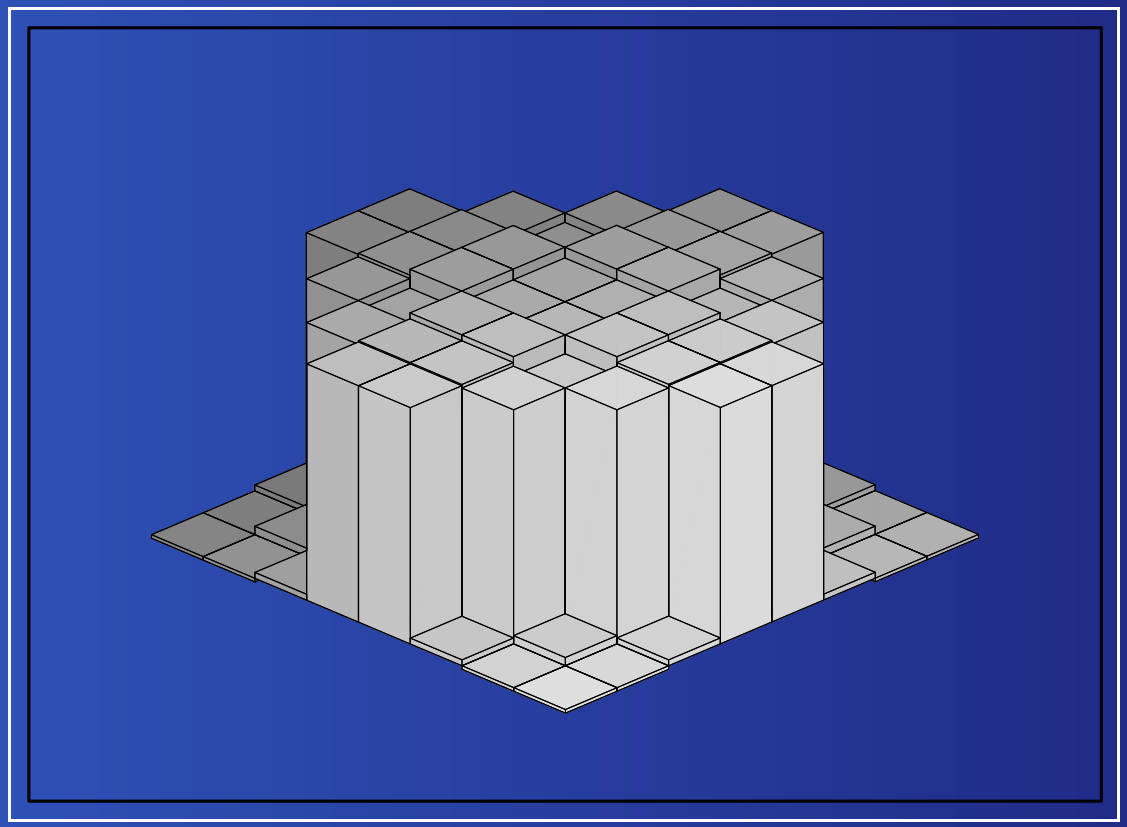


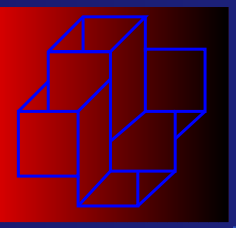
Euclidian distance

- $|P - A| = 35.60898762$
- $|P - B| = 200.2698180$
- $|P - C| = 48.98979486$
- $|P - D| = 106.5833008$

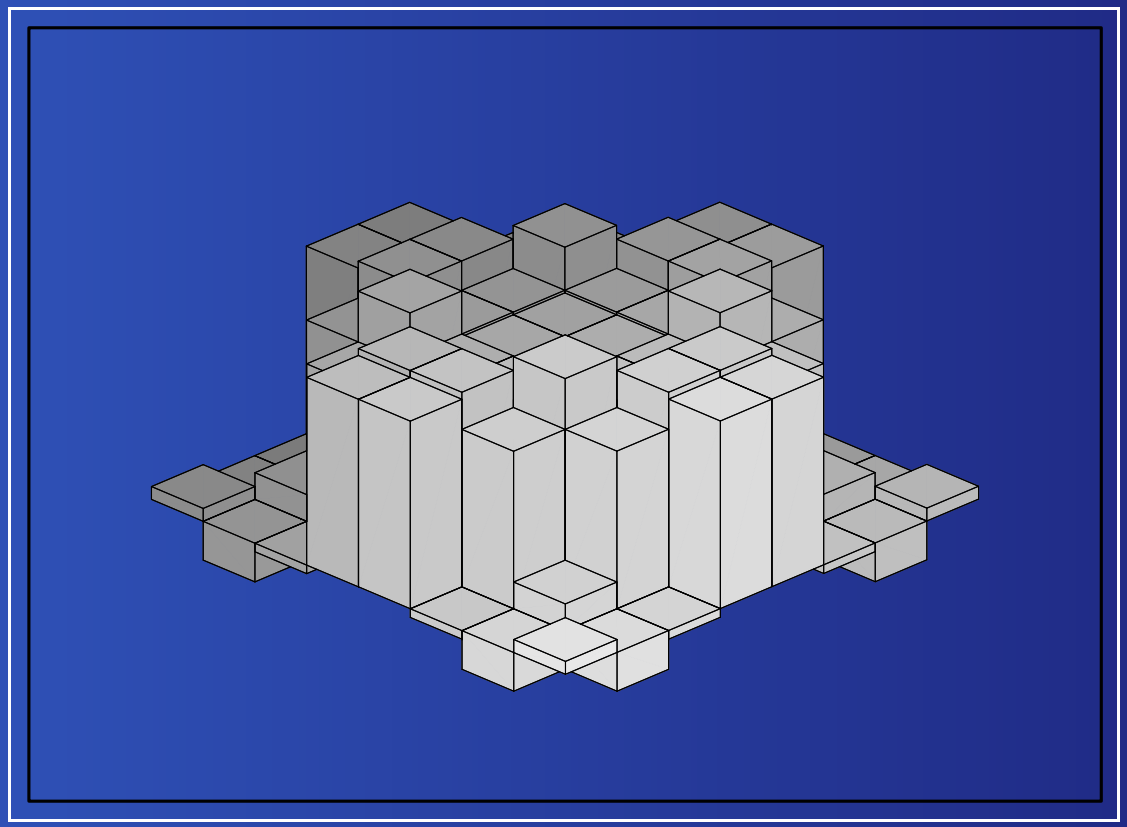


Matrix A without steganography

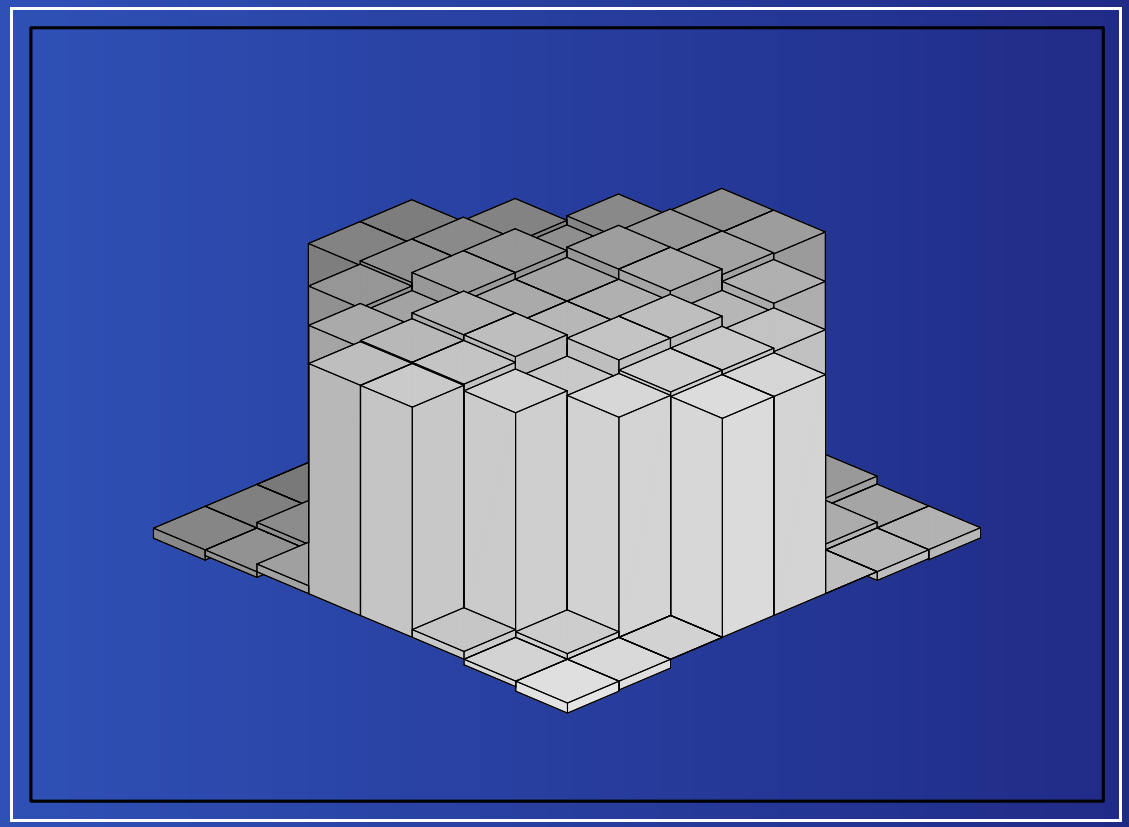


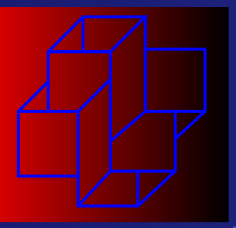


Matrix B with aggressive settings

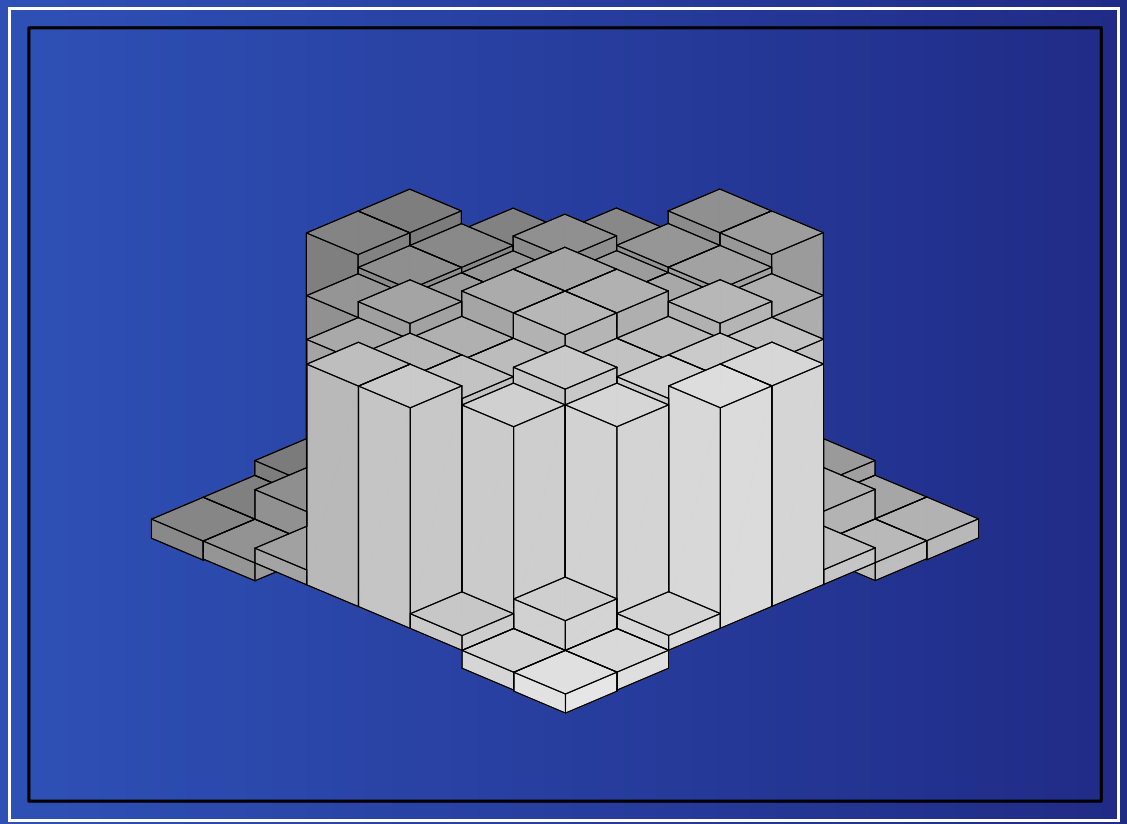


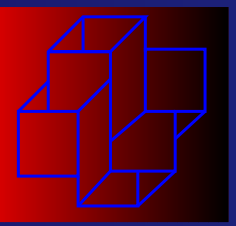
Matrix C no aggressive settings





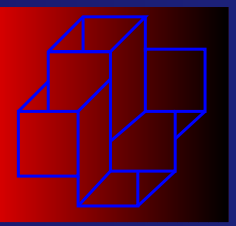
Matrix D with aggressive settings





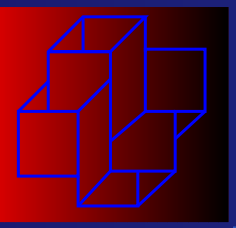
The protocol

1. the position of the sequence of bits previously agreement to establish communication in a videoconference,
2. steganography more secure,
3. Diffie-Hellman key agreement,
4. RSA to exchange an irrational number generator,
5. strong cryptography based on irrational numbers.



Conclusion

- We have introduced a model for steganocryptography
- First of all we revised the RSA, Diffie-Hellman and JPEG's compression
- Our contribution is showing the viability to embed in others LSB
- It brings an extra-layer of security



Last Slide

- Thank you.
- Any suggestions will be welcome.

www.lncc.br/borges

Fábio Borges de Oliveira