I JORNADA STIC

CAPÍTULO COLOMBIA

Criptografía post-cuántica basada en teoría de códigos

En colaboración con:

ccn-cert centro criptológico nacional

incibe_

ean universidad

fundación in-nova

Valérie Gauthier Umaña

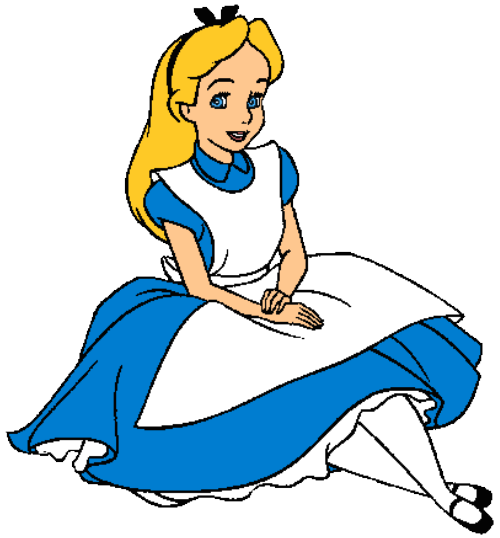
Escuela de Ingeniería, Ciencia y Tecnología

Universidad del Rosario

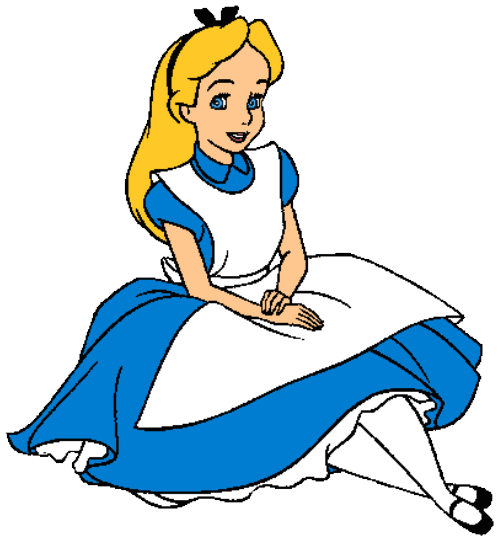
Valeriee.Gauthier@urosario.edu.co

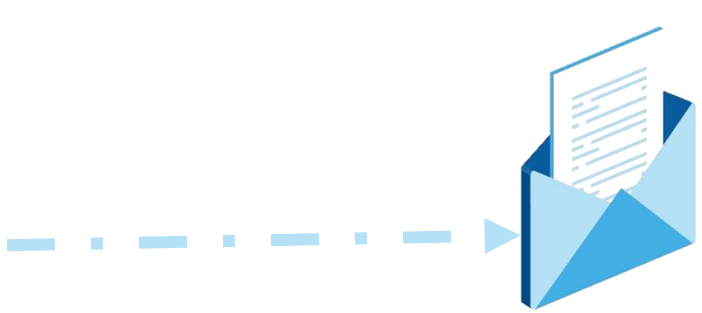
@VGauthierU

Criptografía

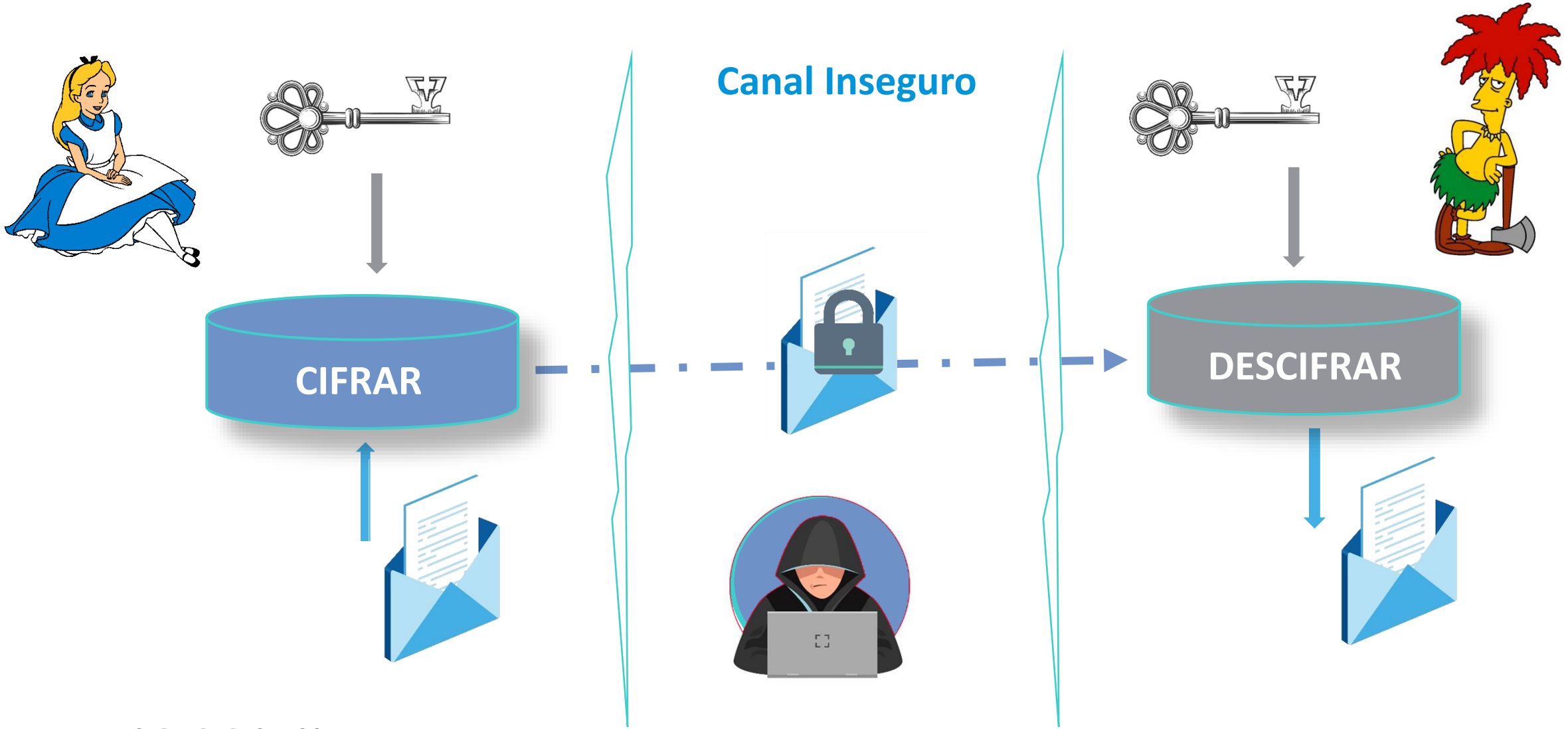


Criptografía

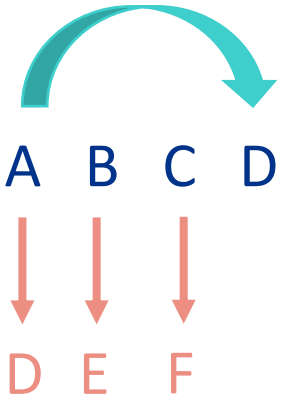




Criptografía a clave secreta



Cifrado de César

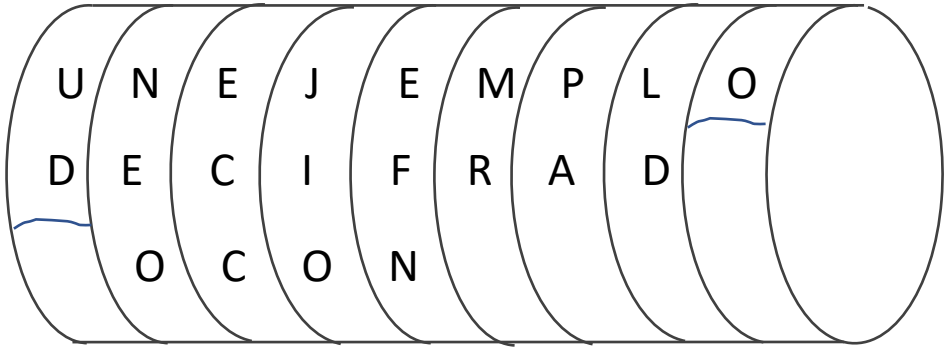


LAS MATEMATICAS SON LA MUSICA DE LA RAZON

ODVPDWHPDWLFDVVRQODPXVLFDGHODUDCRQ

Escitala

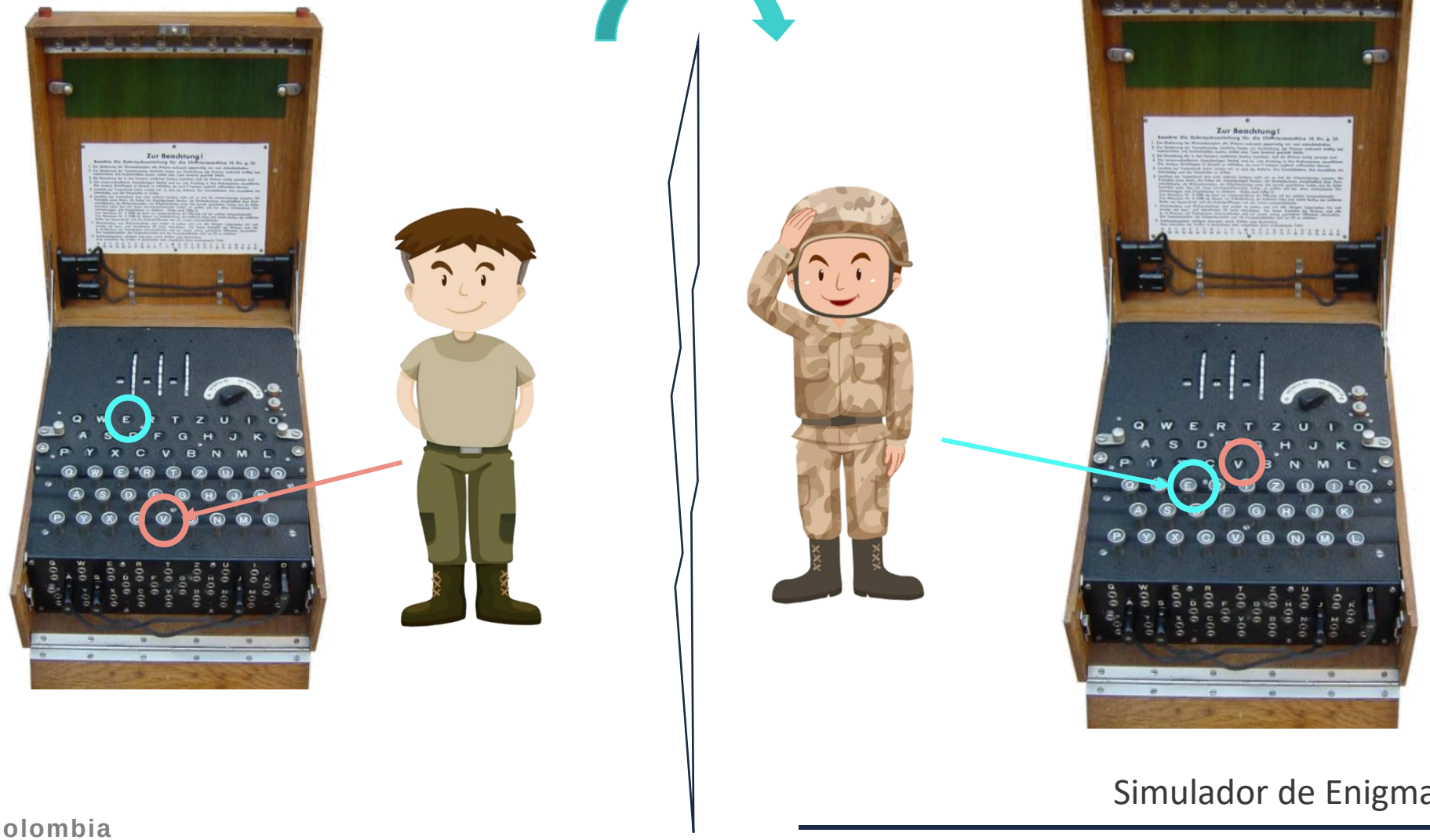
Alterar el orden de los elementos de un mensaje:



M= UN EJEMPLO DE CIFRADO CON

C= UD NEO JIO EFN MR PA LD O

Enigma



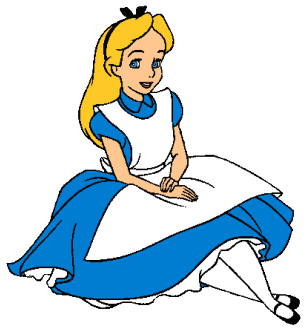
Simulador de Enigma

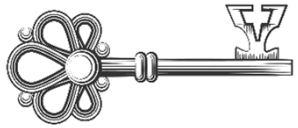
Código ASCII

Código ASCII (American Standard Code for Information Interchange) 1963 … 1986

01000001	01010011	01000011	01001001	01001001
↓	↓	↓	↓	↓
A	S	C	I	I

Criptografía a clave secreta



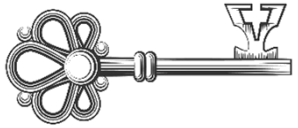


CIFRAR

Canal Inseguro

11000100…11000

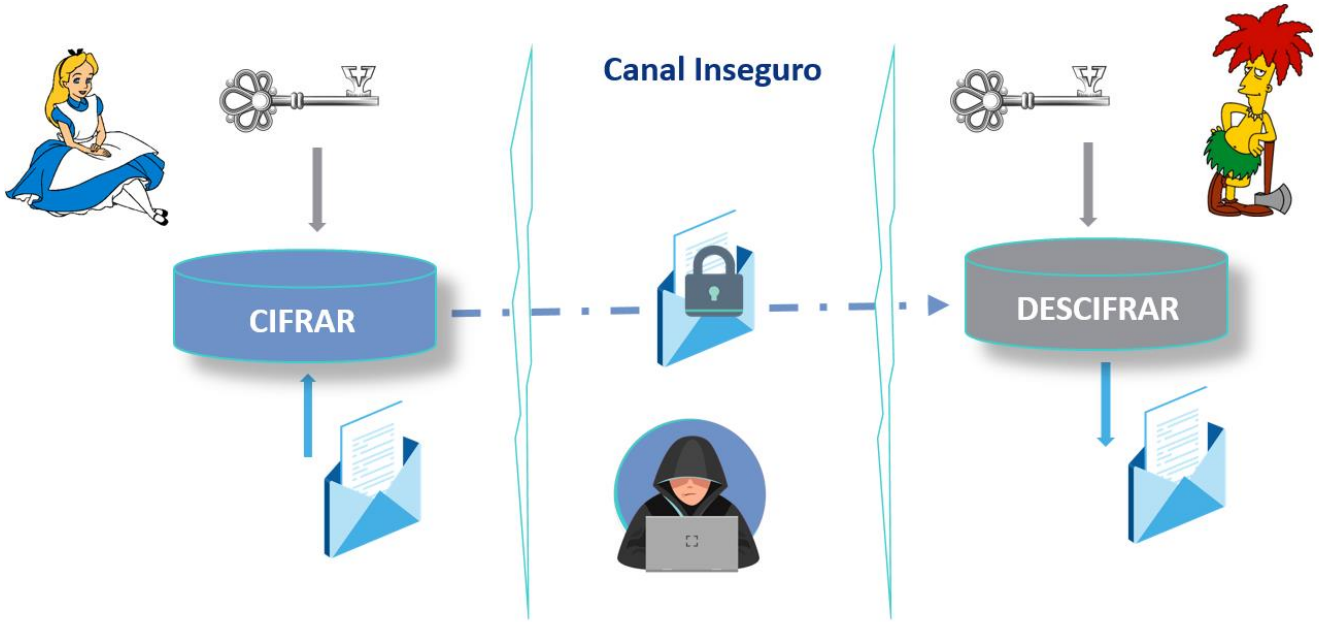
10010110…01101



DESCIFRAR

10010110…01101

Stream Cipher



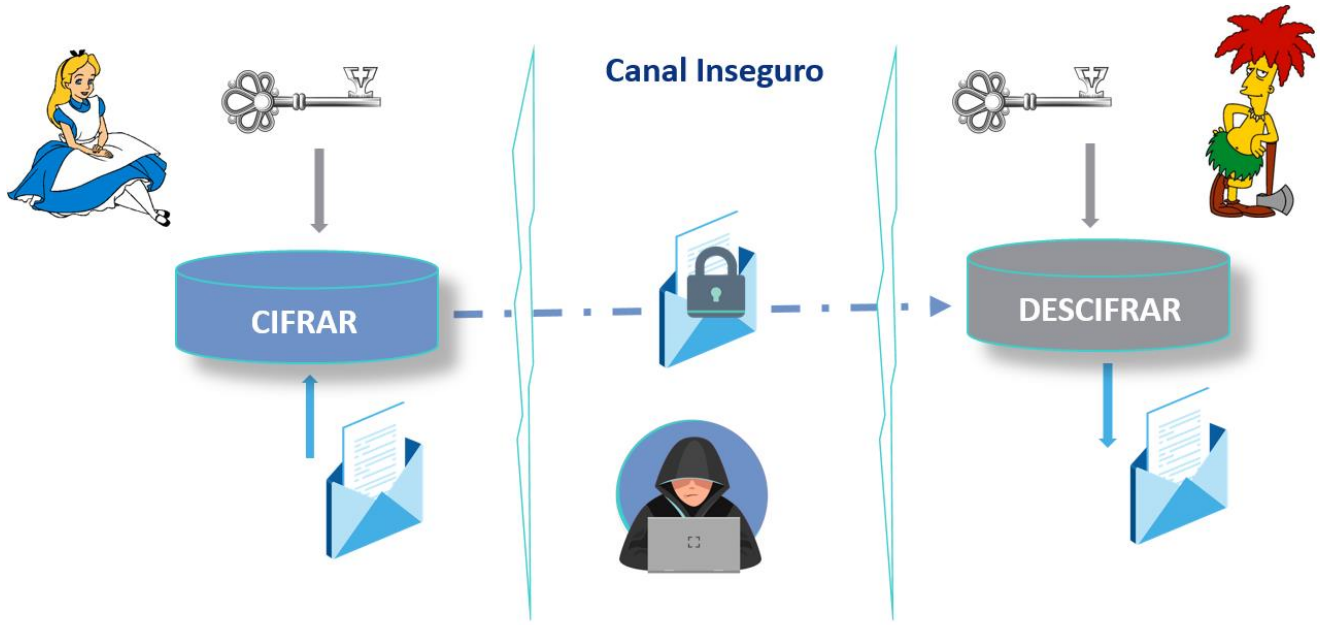
A partir de la clave K, se genera una cadena de bits que se suma bit a bit al mensaje para crear el texto cifrado.

= 10010110…01101

= 10010110…01101 ⊕ 11101110…10110

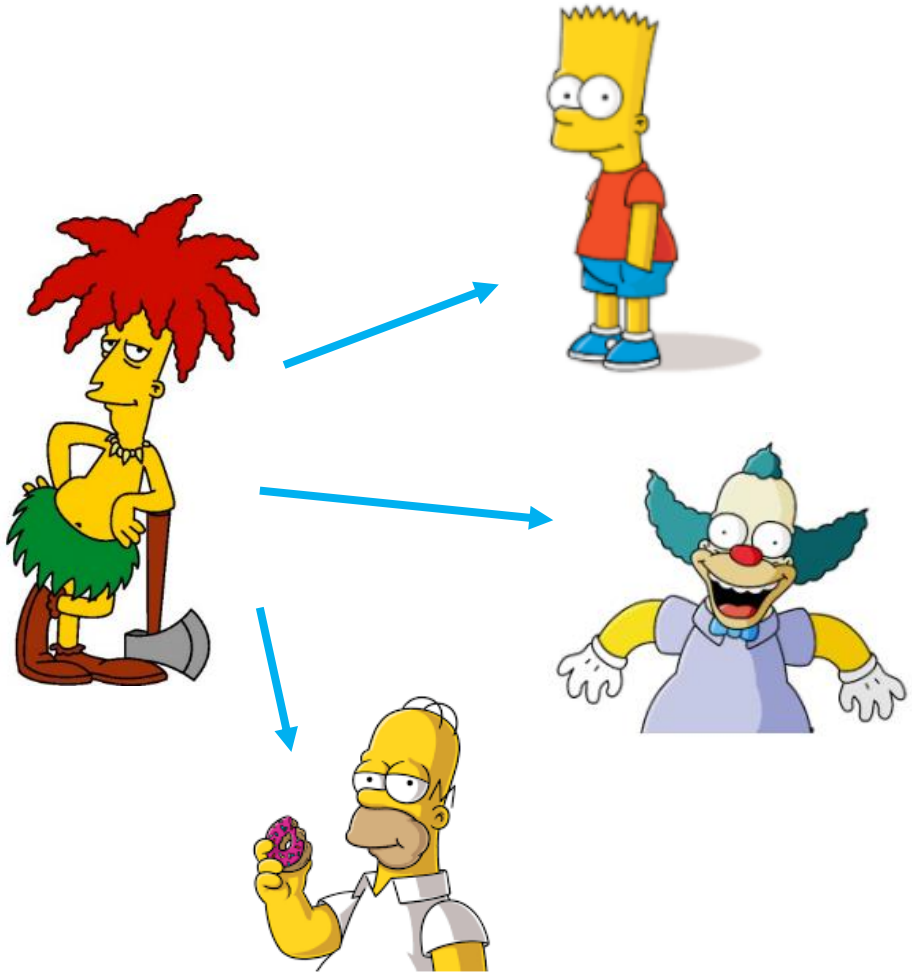
Cifrado de bloques

Partir el mensaje en bloque. Típicamente de 16 bytes, depende del criptosistema.



Repetir el mismo cifrado para cada bloque del mensaje usando la misma clave k.

Criptografía simétrica



Función de un solo sentido

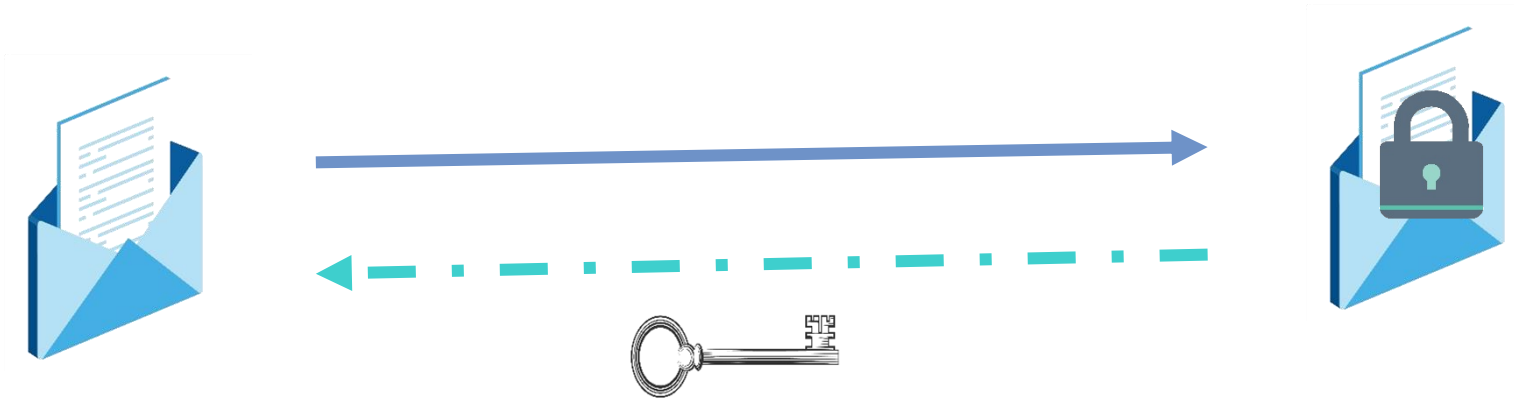
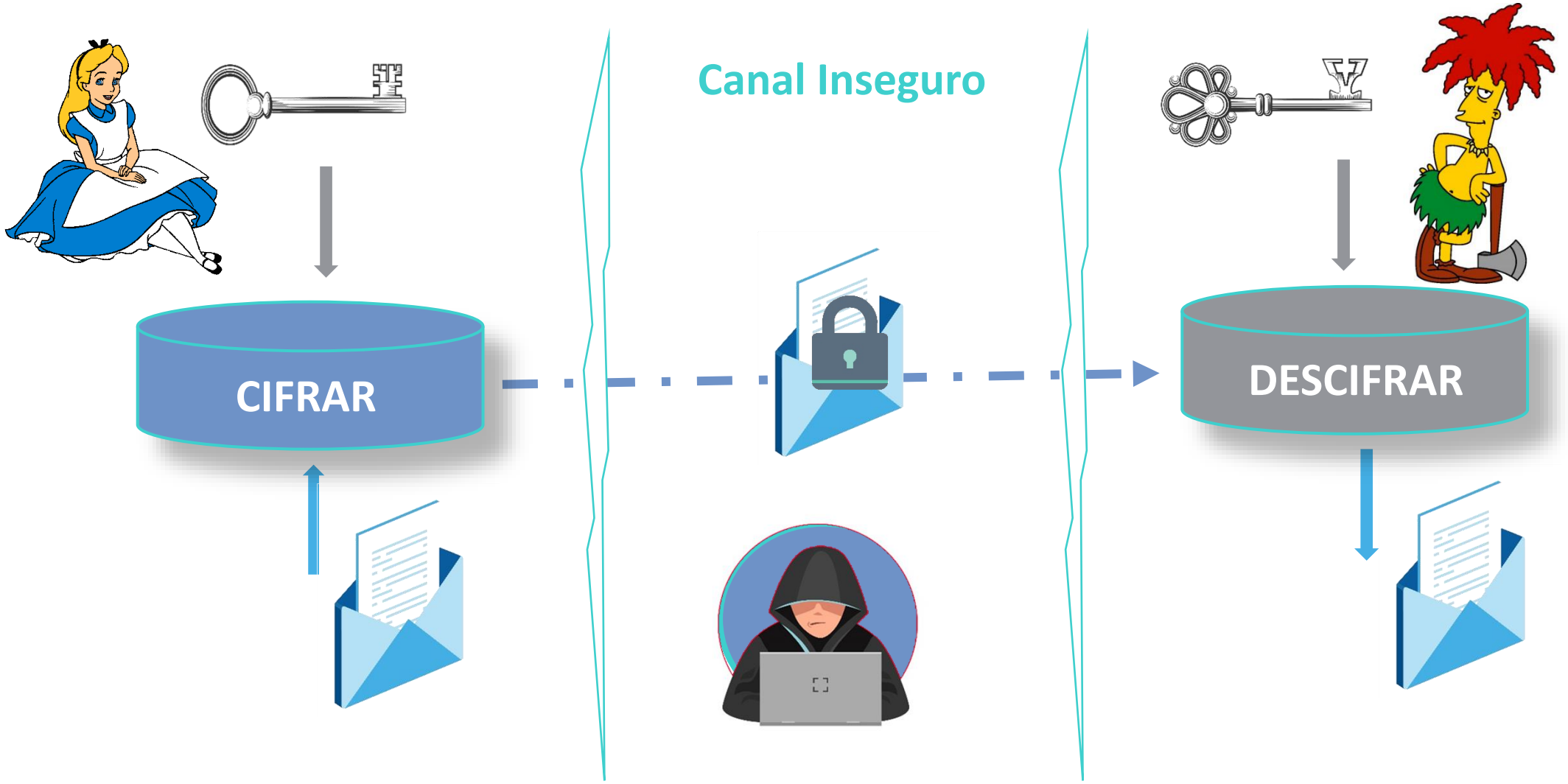


Foto tomada de: https://alum.mit.edu/slice/turing-award-goes-cryptography-pioneer-65

Criptografía a clave pública



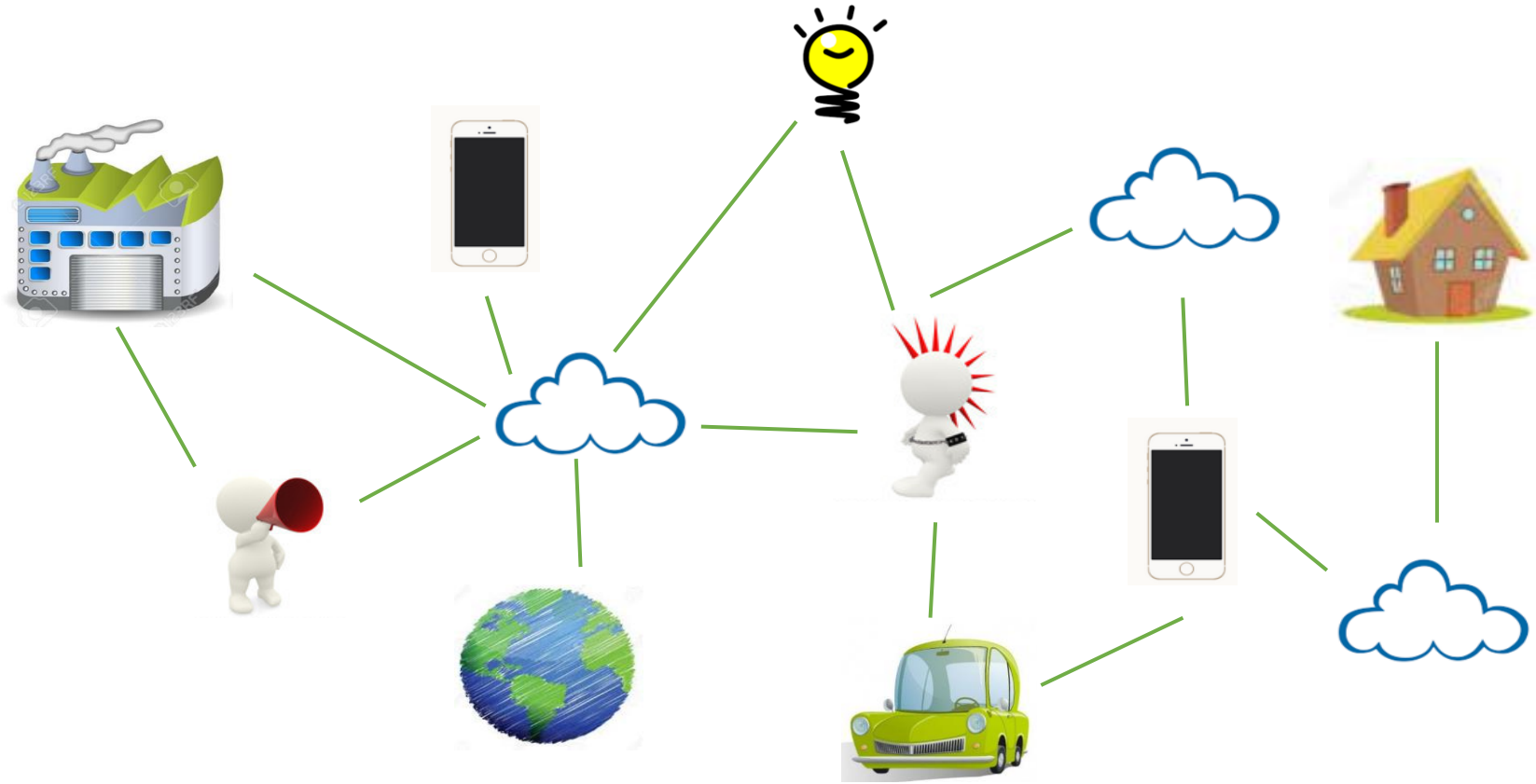
Criptografía a clave pública

40 años después, los criptosistemas que usamos a Clave pública están basados en los dos problemas siguientes:

- ✓ El problema de la factorización de enteros.
- ✓ Problema del Logaritmo Discreto.

Foto tomada de: https://indiatechlaw.com/security/understanding-asymmetric-cryptography-public-key-private-key-rsa-algorithm/attachment/rivest-shamir-adleman/

Primitivas Criptográficas



Autenticaciones

Voto Electrónico

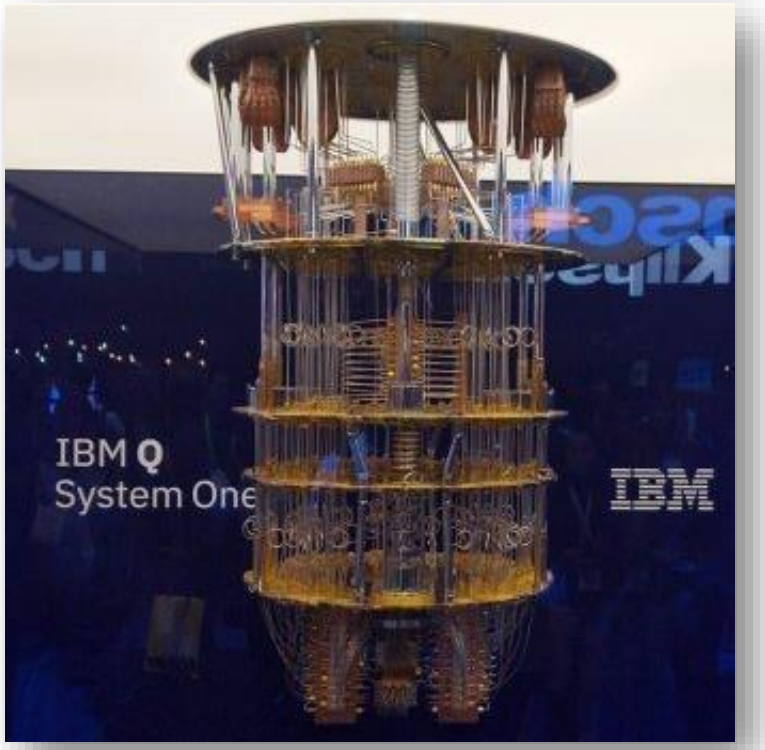
Firmas Electrónicas

Llaves compartida / Mapa del tesoro

Algoritmo de Shor

1994, El algoritmo de Peter Shor los resuelve usando un Computador Cuántico

- ✓ 2001: IBM Factoriza 15 (7-qbits)
- ✓ 2012: 21 y 143
- ✓ 2014 : Se descubre que en el 2012 se factorizó: 56 153



¿Qué hacemos?

NSA announced preliminary plans for transitioning to quantum resistant algorithms.

NIST published a draft of the report on post-quantum cryptography NISTIR 8105.

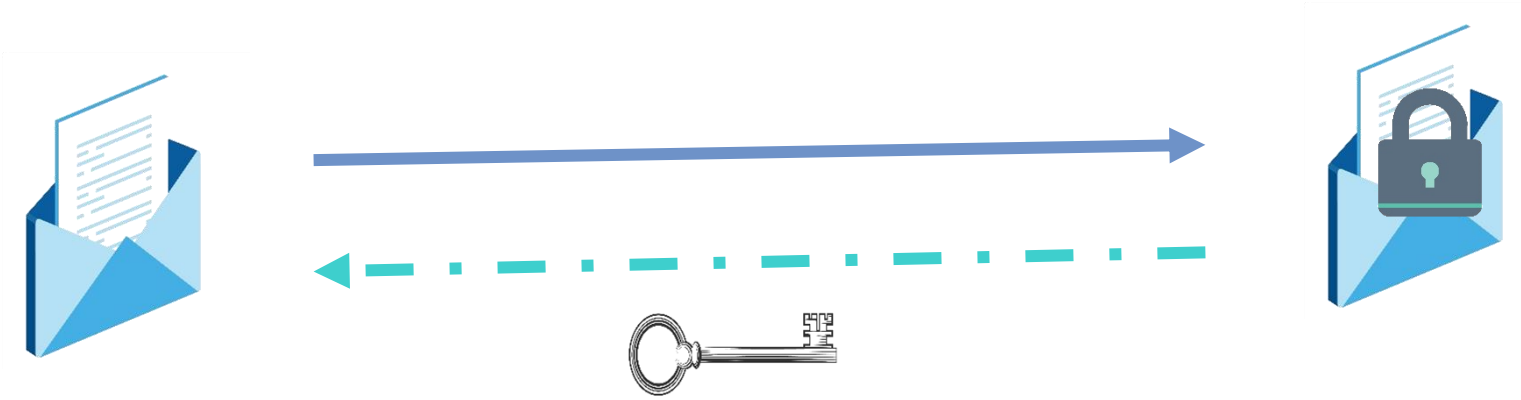
The slides of NIST announcement "Post-Quantum Cryptography: NIST's Plan for the Future" by Dustin Moody at PQCrypto 2016.

The sky is falling?

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES — Need larger keys
    - Triple DES — Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 — Use longer output

Dustin Moody
Post Quantum Cryptography Team
National Institute of Standards and Technology (NIST)

Criptografía Post- Cuántica



Teoría de Códigos

Álgebra Multivariada

Retículos

Isogeny

https://csrc.nist.gov/projects/post-quantum-cryptography

Finalistas - tercera ronda

Finalistas:

Public-Key Encryption/KEMs

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

Digital Signatures

CRYSTALS-DILITHIUM
FALCON
Rainbow

Candidatos Alternos:

Public-Key Encryption/KEMs

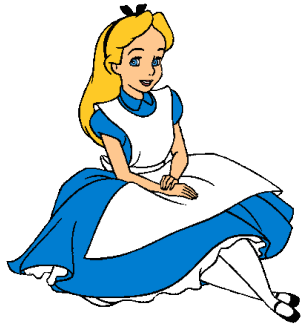
BIKE;
FrodoKEM
HQC
NTRU Prime
SIKE

Digital Signatures

GeMSS
Picnic
SPHINCS+

https://csrc.nist.gov/news/2020/pqc-third-round-candidate-announcement

Teoría de códigos



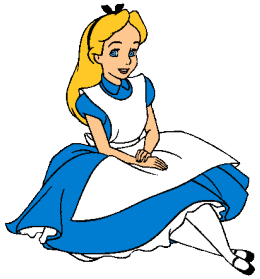
Canal con ruido

m= 10010110…01101

y= 11010010…00100

e= 01000100…01001

Teoría de códigos



$m = (m_1, m_2, \ldots, m_k)$

CODIFICAR

$c = (c_1, c_2, \ldots, c_n)$

$n > k$

Canal con ruido

$e = (e_1, e_2, \ldots, e_n)$

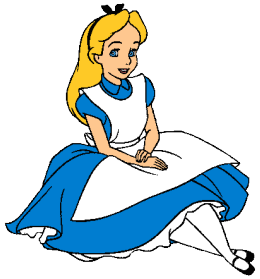
$\oplus$

$m = (m_1, m_2, \ldots, m_k)$

DECODIFICAR

$y = (y_1, y_2, \ldots, y_n) = c \oplus e$

Códigos lineales



$m = (m_1, m_2, \ldots, m_k)$

CODIFICAR

$c = m\,G = (c_1, c_2, \ldots, c_n)$

$n > k$

Canal con ruido

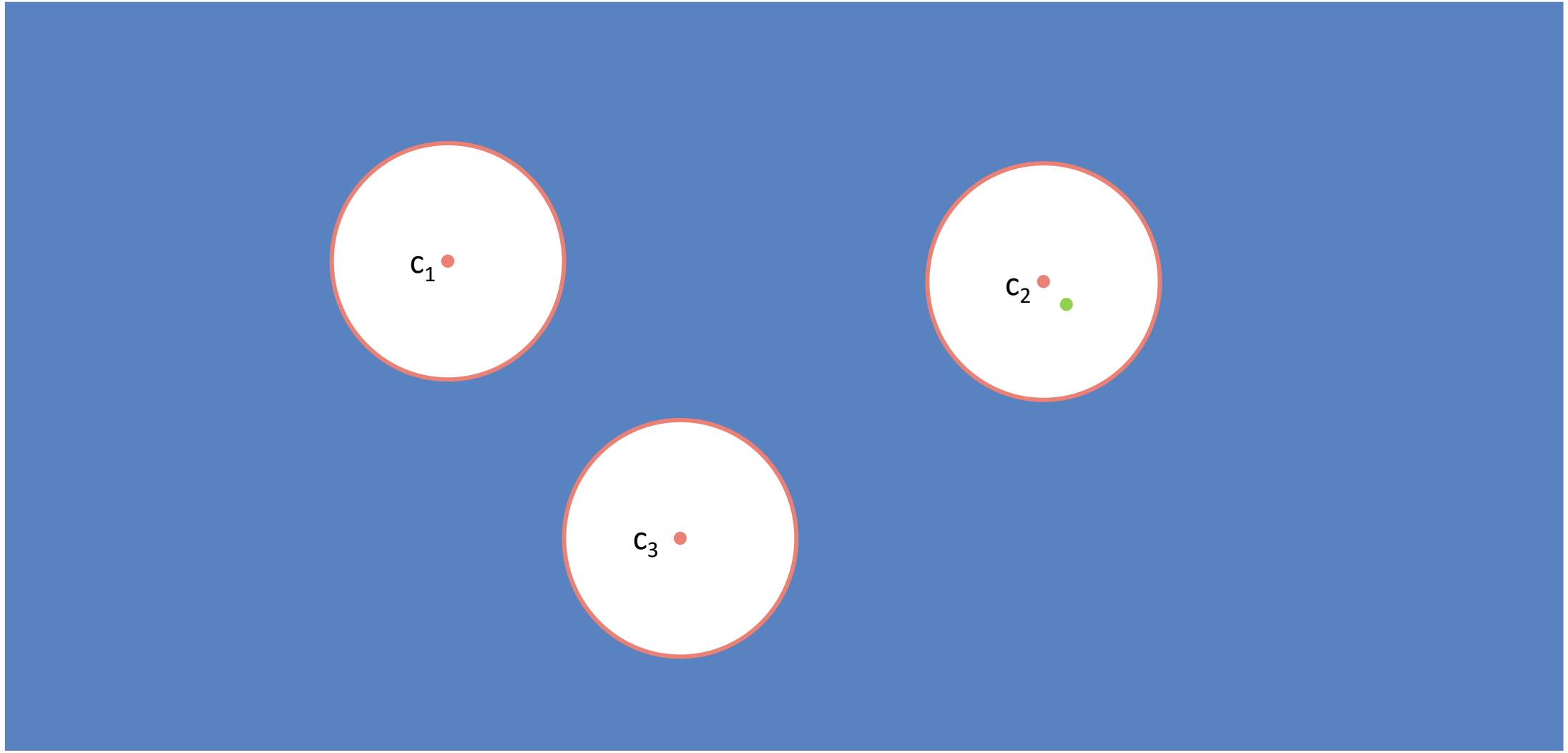
$e = (e_1, e_2, \ldots, e_n)$

$m = (m_1, m_2, \ldots, m_k)$

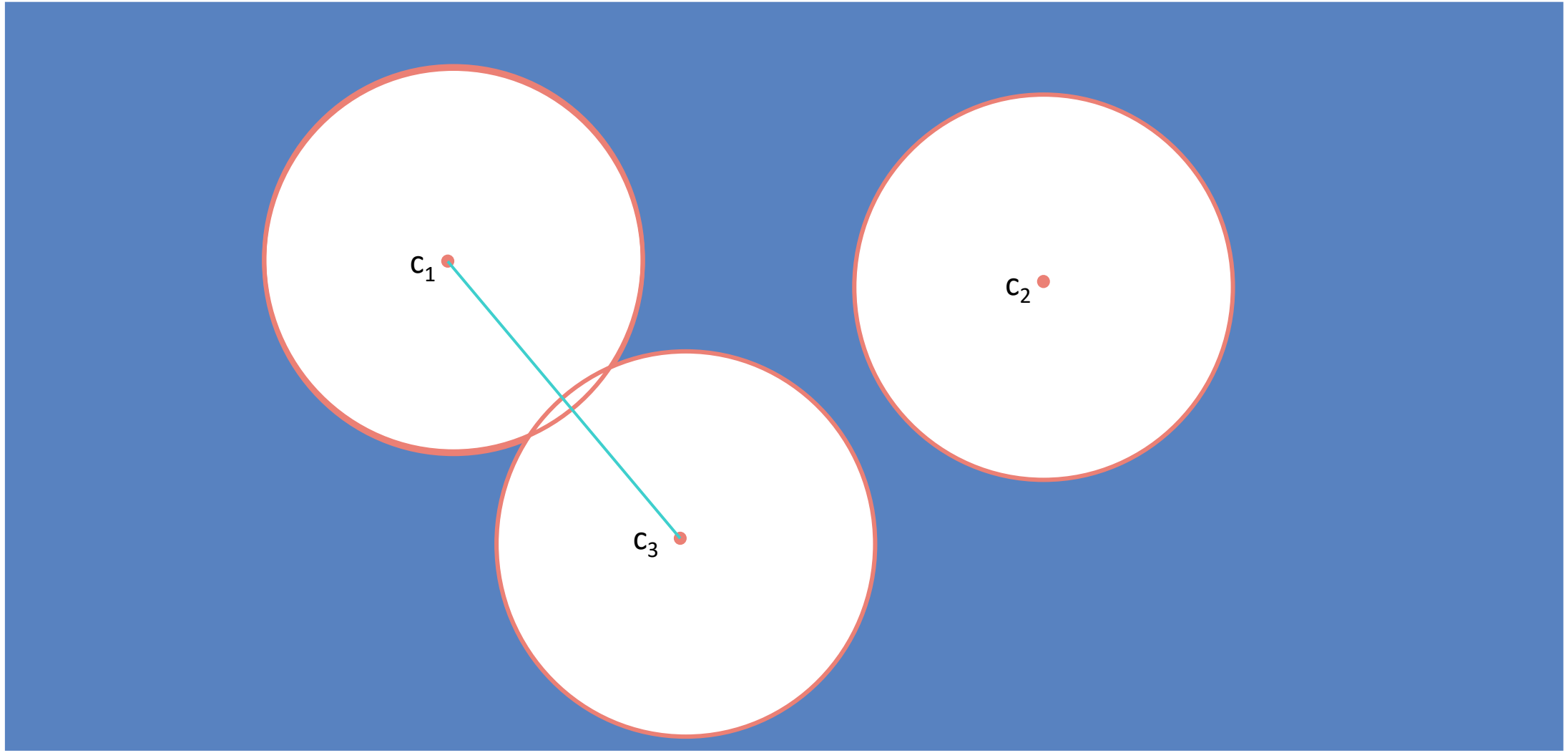
DECODIFICAR

$y = (y_1, y_2, \ldots, y_n) = c \oplus e$

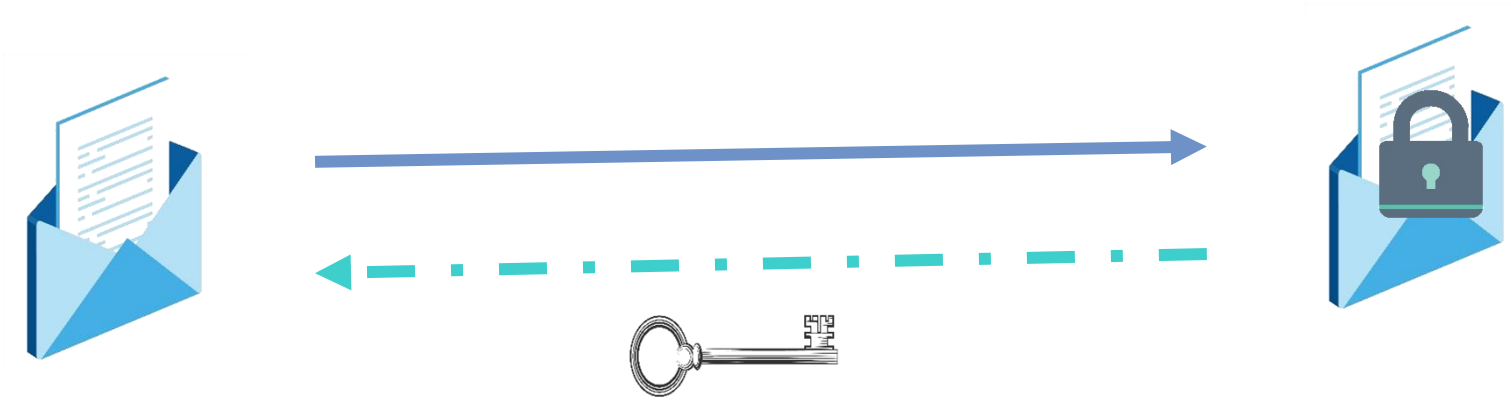
Códigos lineales



Códigos lineales



Crypto basada en códigos



Crypto basada en códigos

Idea:

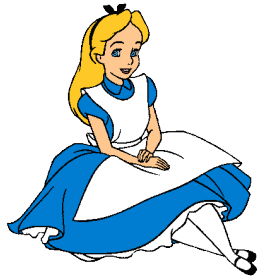
- Elegir un código de Goppa con matriz generadora G_0 y un algoritmo de decodificación $\mathcal{A}$ que corrija hasta t errores.

- Sea P una matriz de permutación y S una matriz invertible.

- Sea $G = S\, G_0\, P$

Criptosistema de McEliece

$G = S\, G_0\, P$



Clave pública de Bob (G,t)

$m = (m_1, m_2, \ldots, m_k)$

CIFRAR

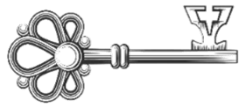
$Z = mG \oplus e$

$e = (e_1, e_2, \ldots, e_n)$

e de peso $\leq t$

Canal con ruido

$\mathcal{A}(z\,P^{-1}) = \mathcal{A}(m\,S\,G_0\,P\;\;P^{-1} \oplus e P^{-1})$
$= \mathcal{A}(m\,S\,G_0 \oplus e')$
$= m\,S$



Clave secreta de Bob $(S, G_0, P, \mathcal{A})$

DESCIFRAR

$\mathcal{A}(z\,P^{-1}) \times S^{-1}$

JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS

@VGauthierU *Valeriee.Gauthier@urosario.edu.co*

En colaboración con:

ccn-cert centro criptológico nacional

incibe_

ean universidad

fundación in-nova