Las Matemáticas, el Motor de la Ciberseguridad

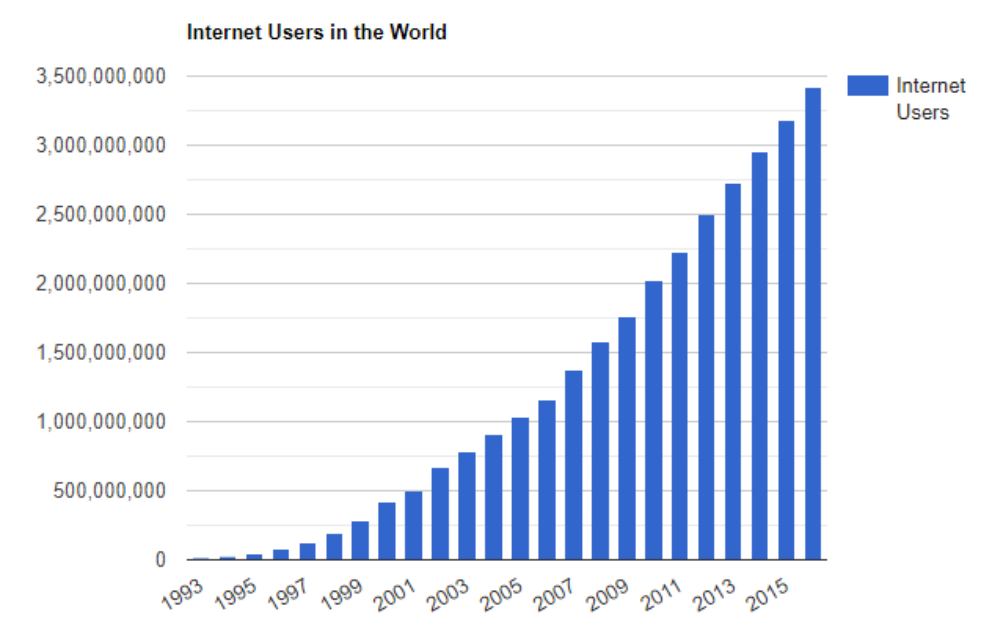
Dr. Iván Jirón Araya
Departamento de Matemáticas
Núcleo de Investigación en Inteligencia Artificial y Data Science
ijiron@ucn.cl

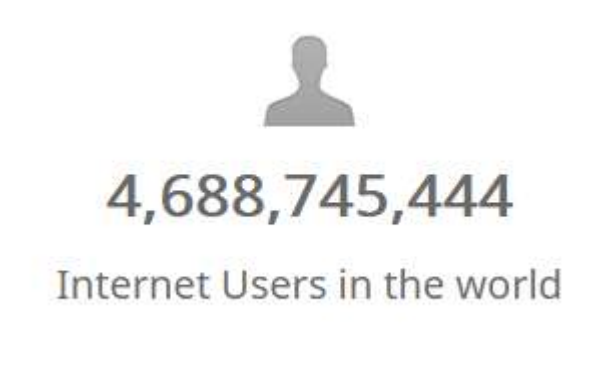
AGENDA

1. **IDEAS PRELIMINARES**
2. **¿QUÉ ES LA CIBERSEGURIDAD?**
3. **CRIPTOGRAFÍA**
4. **CRIPTOGRAFÍA ASIMÉTRICA**
5. **RECIENTE CIBERATAQUE A UN BANCO**

1. IDEAS PRELIMINARES

Internet Live Stats





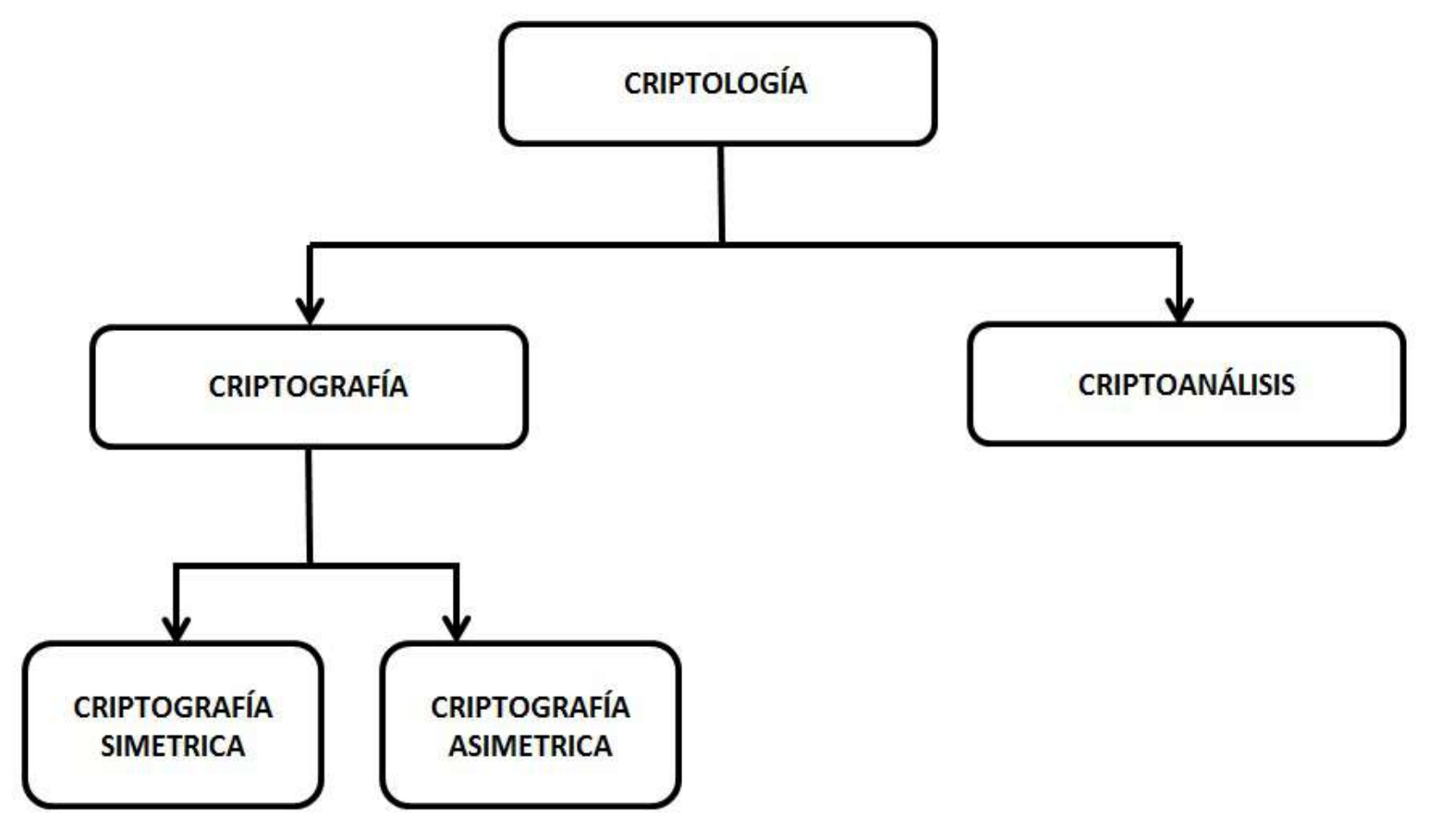
FUENTE: https://www.internetlivestats.com/cybersecurity/

2. ¿QUÉ ES LA CIBERSEGURIDAD?

La **CIBERSEGURIDAD** es la **PROTECCIÓN** del **CIBERESPACIO** (computadoras, redes, software y datos) contra peligros y amenazas con el objetivo de hacerlo estable, seguro y resistente.

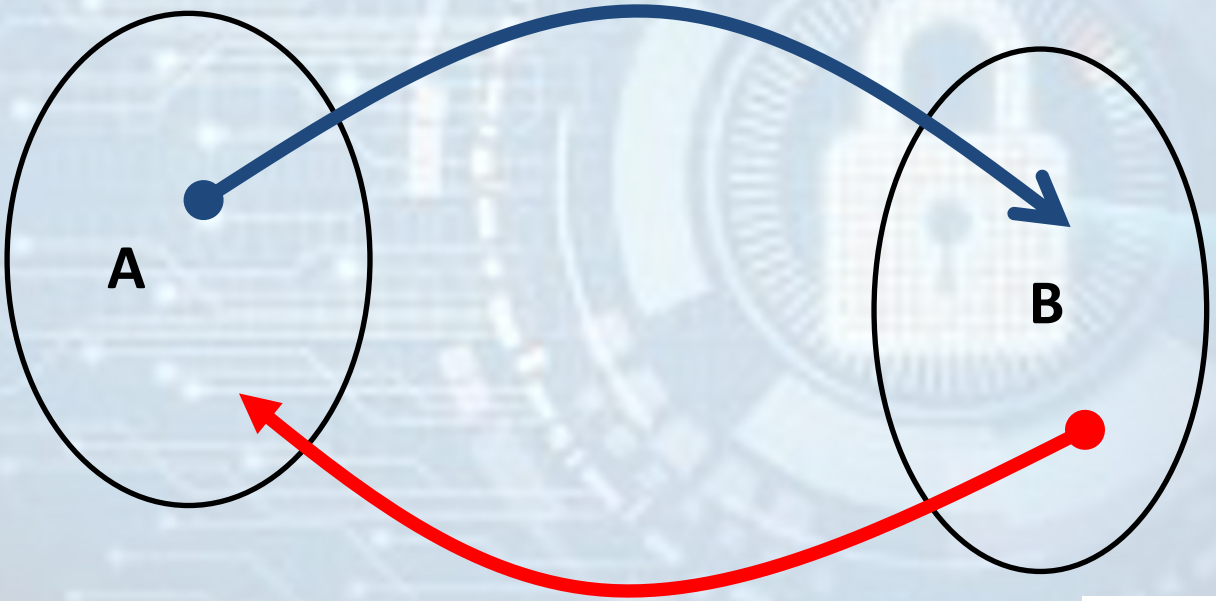
FUENTE: https://www.internetlivestats.com/cybersecurity/

3. CRIPTOGRAFÍA



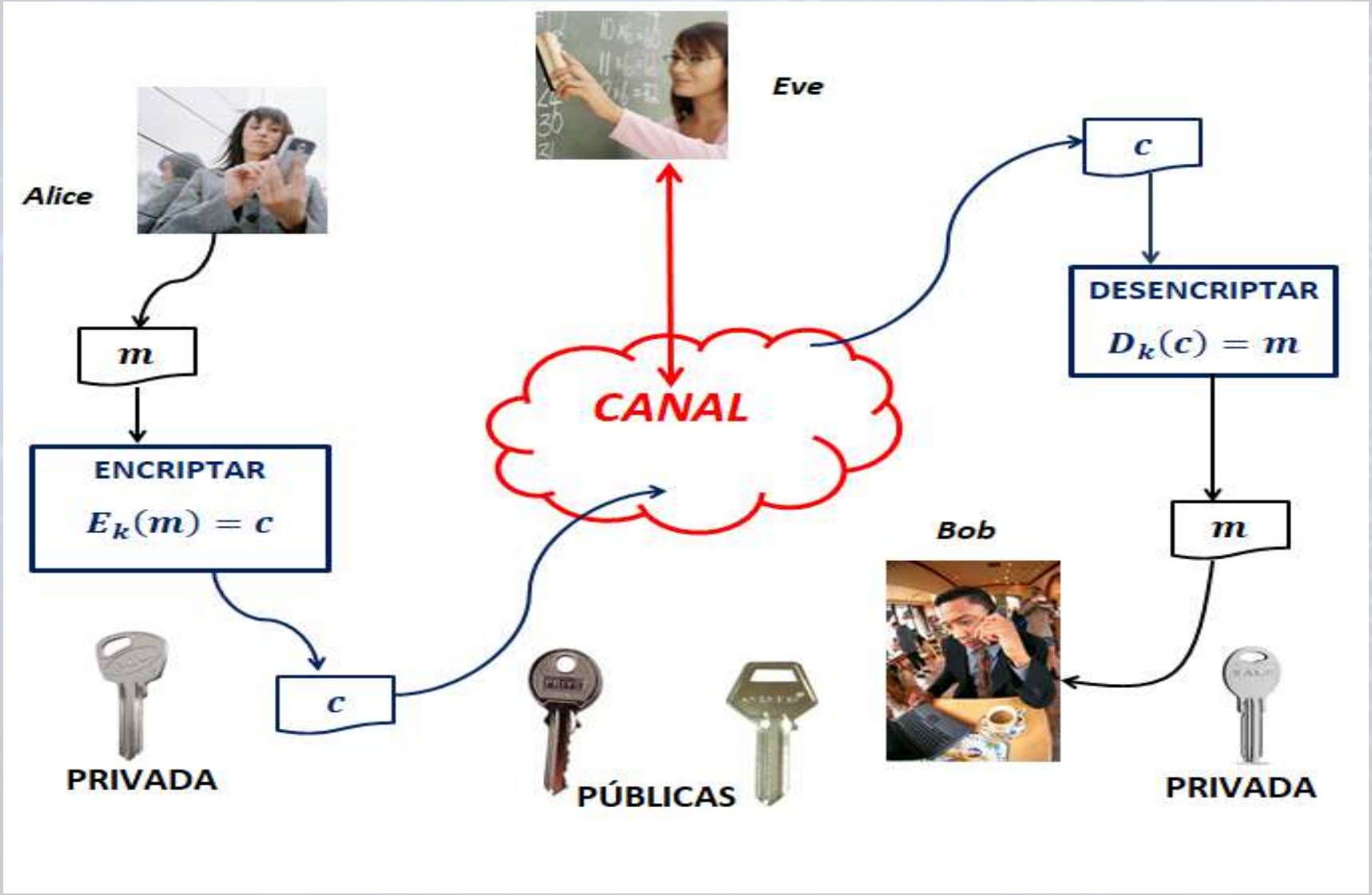
ESENCIA DE LA CRIPTOGRAFÍA

$$y = f(x)$$



$$x = f^{-1}(y)$$

4. CRIPTOGRAFÍA DE LLAVE PÚBLICA



ALGORITMO DE INTERCAMBIO DE LLAVES DE DIFFIE-HELLMAN (1976)

https://blackberry.certicom.com/

PROBLEMA: LOGARITMO DISCRETO

$$2^x = 8 \Longrightarrow x = 3$$

$2^x = 499490918065850$

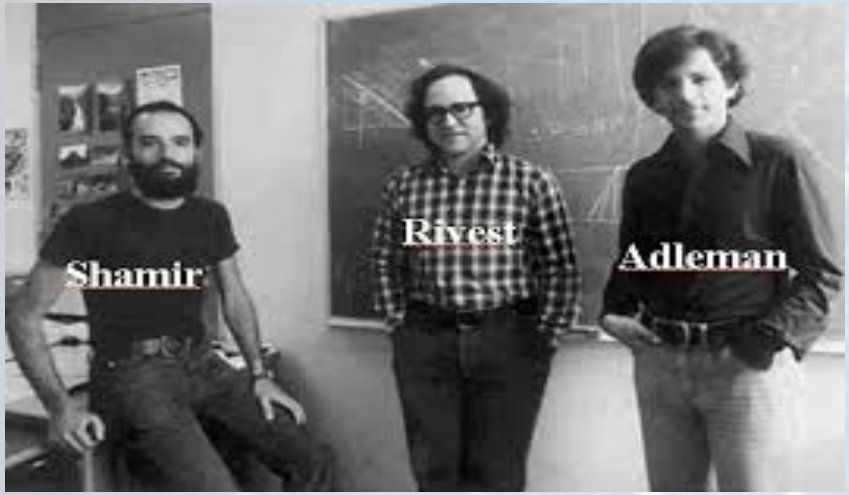
$301921197603564081112 78$

$062369027342098434296869059406 46$

$12108591217229304461006005170865294466525626366754$

$$x = ?\,?\,?\,?\,?$$

ALGORITMO RSA (RIVEST, SHAMIR, ADLEMAN) 1978



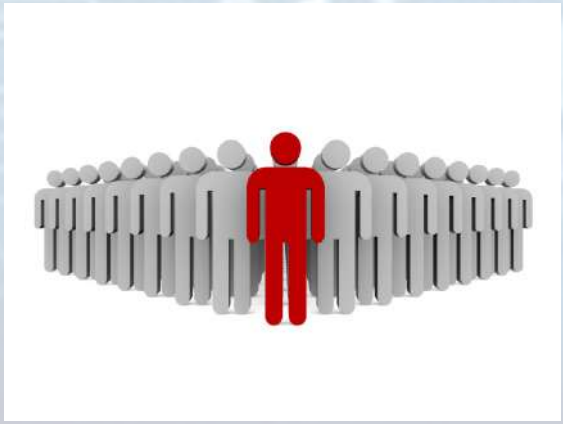
https://www.rsa.com/

PROBLEMA: FACTORIZACIÓN DE NÚMEROS ENTEROS GIGANTES

$$77 = 7 * 11 \qquad 341 = 31 * 11$$

$$64277521770359611021678483693671857112892684339341647476162 57$$

$$= 7 * 607 * 151276822241373525586440300526410583932437477852063185 3993$$



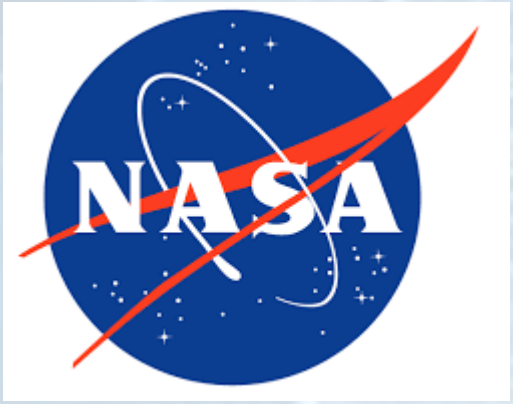
Neal Koblitz, “Algebraic Aspects of Cryptography”, ISBN 3-540-63446-o Springer-Verlag, 1999.

RSA-2048 =

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203571

617 dígitos decimales

SITIOS WEB SEGUROS



https://www.nasa.gov/

https://www.google.com/

5. RECIENTE CIBERATAQUE A UN BANCO

El **RANSOMWARE** es un tipo de **software malicioso** que le impide acceder a archivos importantes o al dispositivo y lo **chantajea** para que **pague un rescate** a fin de impedir que los datos se eliminen o se utilicen de manera inadecuada.

FUENTE: https://support.norton.com/

¡¡¡ Error humano!!!

Teletrabajo fuera de la red segura del banco

Phishing

Apagar los servidores para evitar la propagación del virus

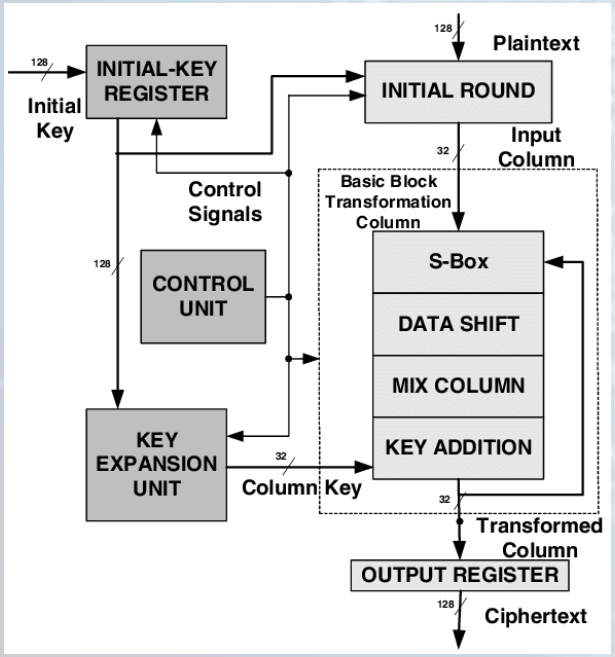
Desconectarse de Internet para detener el robo de datos y dinero

Encriptación de datos

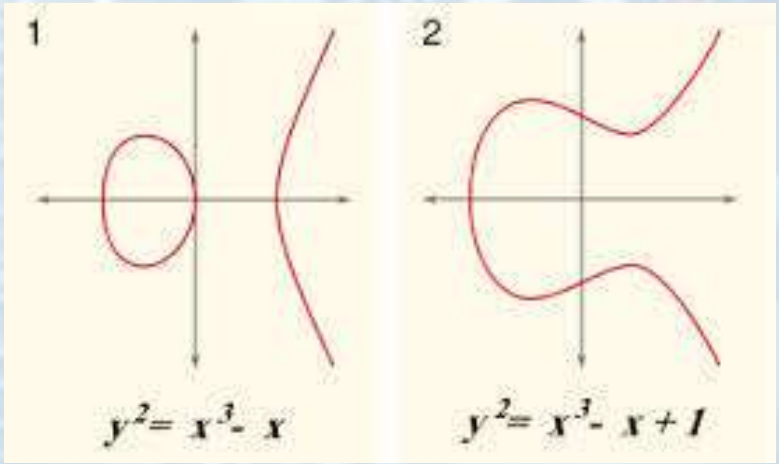
Ransomware Sodinokibi

Ransomware Sodinokibi

Advanced Encryption Standard (AES 2001)



Intercambio de llaves de Diffie-Hellman sobre curvas elípticas



Algoritmo Salsa20 (2005)

FUENTE: https://protecciondatos-lopd.com/empresas/sodinokibi/

Las Matemáticas, el Motor de la Ciberseguridad

Gracias