



Cryptography

Basic Concepts

Banamex.com | Tarjetas de ...

Citigroup Inc. (US) | https://www.banamex.com

Banamex

Bancas en Línea
 Banamex te da acceso a todas sus soluciones en línea

Iniciar sesión en...

Gente Banamex
 Intégrate a nuestro equipo de trabajo.

Centro de Seguridad
 Encuentra lo que debes saber para mantenerte protegido.

General Media Permissions Security

Website Identity

Website: **www.banamex.com**
 Owner: **Citigroup Inc.**
 Verified by: **Symantec Corporation**

View Certificate

Privacy & History

Have I visited this website prior to today?	No
Is this website storing information (cookies) on my computer?	No
Have I saved any passwords for this website?	No

View Cookies View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
 The page you are viewing was encrypted before being transmitted over the Internet.
 Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

CUENTA PERFILES Más dinero por tu dinero

TE PROTEGEMOS Seguros Banamex

MÚLTIPLES BENEFICIOS Tarjetas de Crédito

GANAR BOLETOS Banamex

SI VAS A VIAJAR AL EXTRANJERO ¡Avisanos!

SOLICITA AQUÍ TU TARJETA DE CRÉDITO y descubre todos sus beneficios.

TRANSFER BANAMEX Activa tu cuenta aquí y úsala desde tu celular.

SHCP SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT Servicio de Administración Tributaria

SAT Trámites Información Comercio exterior Aduanas Declaraciones

SAT > FICHAS TEMÁTICAS > FIEL

Imprimir

Twitter 446

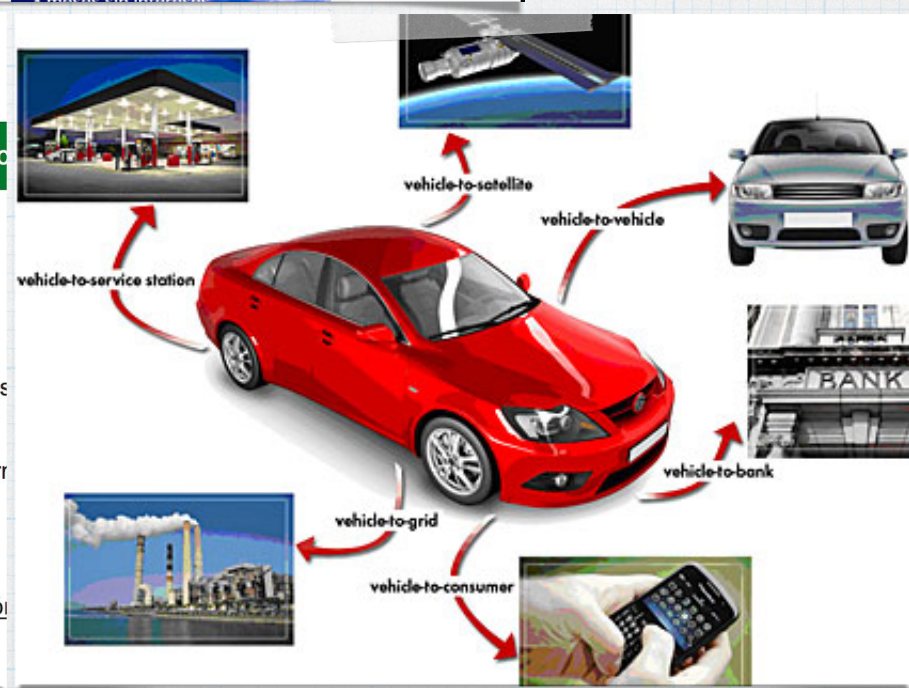
FIRMA ELECTRÓNICA

La Firma Electrónica es un archivo digital que te identifica al realizar trámites otras dependencias del Gobierno de la República.

Tu Firma Electrónica es única, es un archivo seguro y cifrado que incluye tu firma.

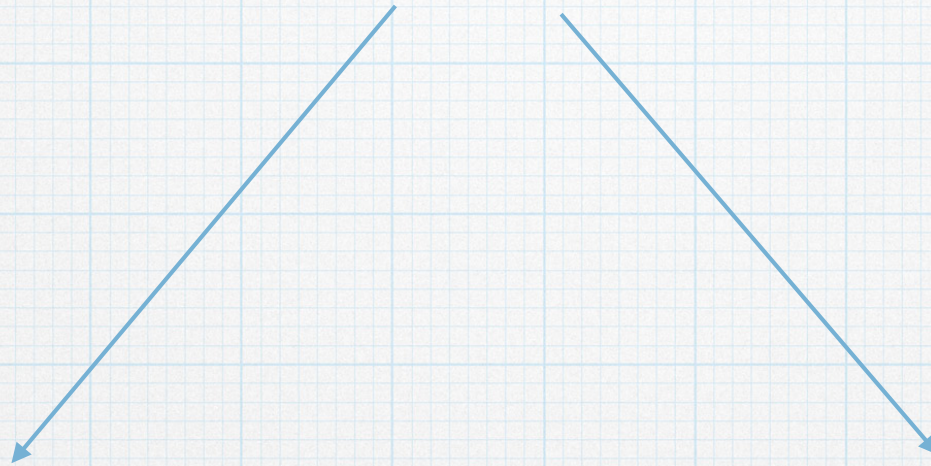
Por sus características, es segura y garantiza tu identidad.

Cómo obtener tu Firma Electrónica | Cómo renovar tu Firma Electrónica | Cómo



Cryptology

The study of codes or the art of writing and solving them



Cryptography



Cryptanalysis



What is cryptography?

From the Greek: **cryptos**, meaning **hidden**
and **graphien**, meaning **to write**.

“The art of secret writing”
(Merriam-Webster dictionary)

Definition of cryptography

“Cryptography is the study of mathematical techniques related to aspects of information security such as:

- confidentiality,
- data integrity,
- entity authentication and
- data origin authentication”

(Handbook of applied cryptography)

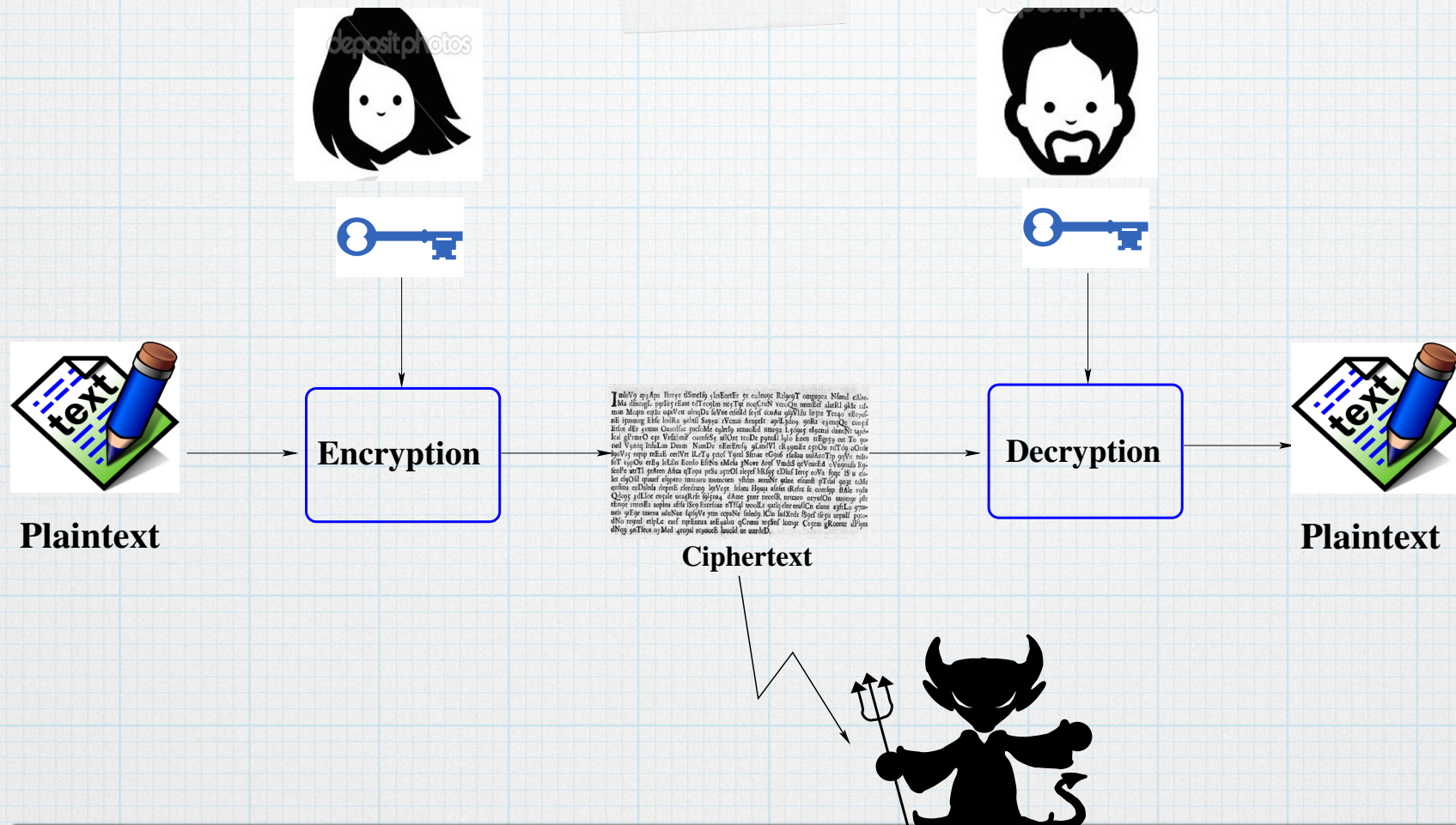


Alfred Menezes

Cryptographic services

- * Privacy or confidentiality
- * Integrity
- * Authentication
- * Non-repudiation

Privacy

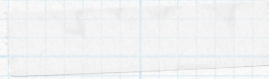
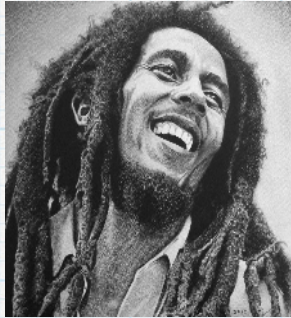


To provide secret communication between two parties,
who must share certain information in advance

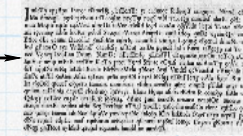
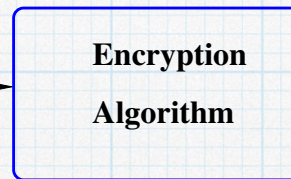
Public-key cryptography

- * Each entity has two keys: private and public.
- * **Public key** is used to **encrypt**
- * **Private key** is used to **decrypt**

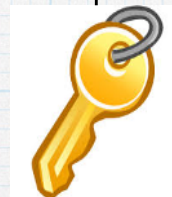




Plaintext



Ciphertext



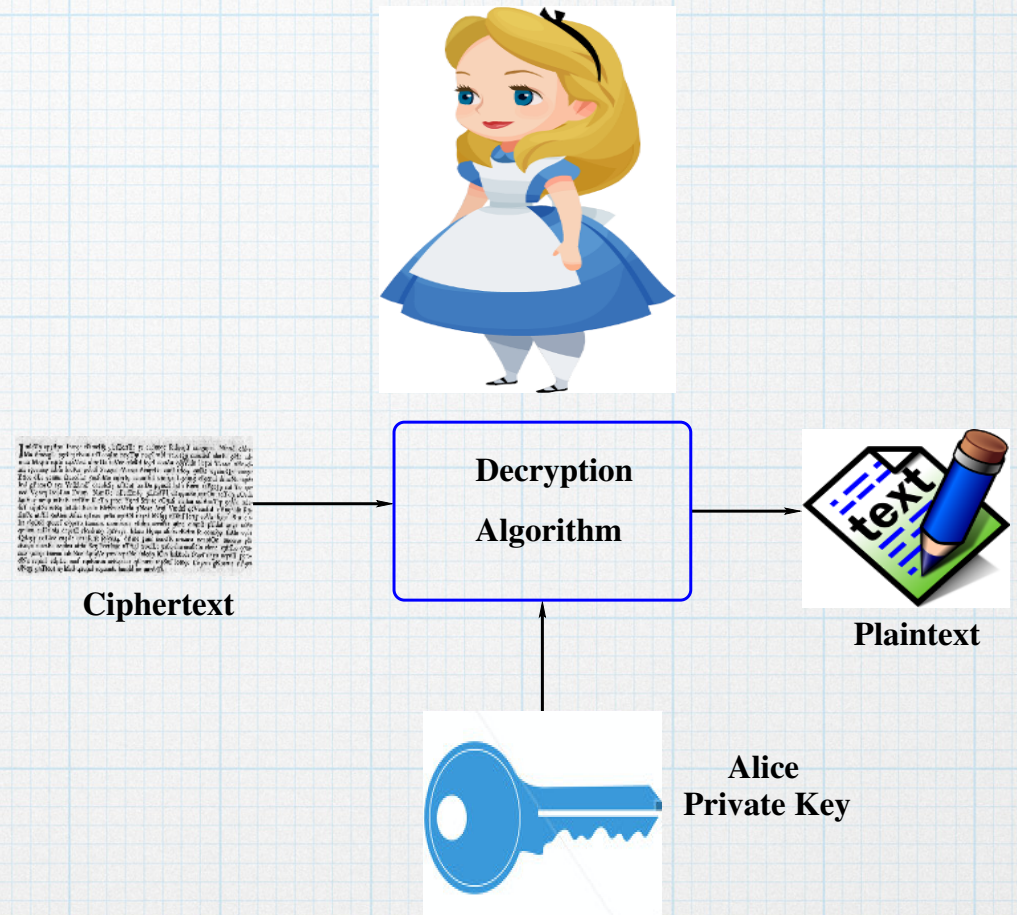
Alice
Public Key

Encryption

with **asymmetric** cryptography

Decryption

with asymmetric
Cryptography



Integrity



Interception

Replaced info



To prevent unauthorised alteration of data

Authentication



To guarantee that each entity in a communication
is who claims to be

Non-repudiation

A white rectangular card with a torn top edge is centered on a blue grid background. The card features a handwritten signature in black ink that reads "Steven Jobs".

It prevents an entity from denying previous commitments or actions

Cryptographic system

$$(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- * \mathcal{M} Plaintext space
- * \mathcal{C} Ciphertext space
- * \mathcal{K} Key space
- * Encryption algorithm $\mathcal{E} : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$
- * Decryption algorithm $\mathcal{D} : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$

Type of attacks

- * Ciphertext only attack (eavesdropping)
- * Known plaintext attack
- * Chosen plaintext attack (CPA)
- * Chosen cipher text attack (CCA)

On July 11, 2014 Lang Lang performed together with Placido Domingo, Ana Maria Martinez, Maestro Eugene Kohn, the Orchestra Sinfonica Brasileira, Paula Fernandez and other musicians for World Cup Concert at HSBC Arena in Rio de Janeiro Brasil

X: Plaintext

E_K



ue4n32EAf/UEF6JLrap10B
EY4V4Z3vLpN3AgAhObP2eUFU29EJAQpo3j
6E+Gc4iumM1725JNahJz15ED33LFdZ6
tAqTk572zdZbrCtSgcthrN/uxbJSN
XFG1J8oaLpRV499m71Nfo+ZV2HrR
MdKMvb+DZ9GVoi jUixH+gbci9qvC3kt
1qHXSukK648DgpWS2oxJvmGuf/YKn+FF

Ciphertext

Ciphertext only attack

Known plaintext attack

- * Adversary has access to cipher text for some plaintext.
- * Cryptosystem is broken if an adversary is able to find plaintext of other cipher text

CPA attack

- * An adversary has access to **encryption** machinery
- * She is able to choose messages
- * She gets the corresponding cipher text



CCA attack

- * An adversary has access to **decryption** machinery.
- * She is able to choose cipher texts and obtain the corresponding plaintexts.
- * Her goal is to find plaintexts of other cipher texts.