

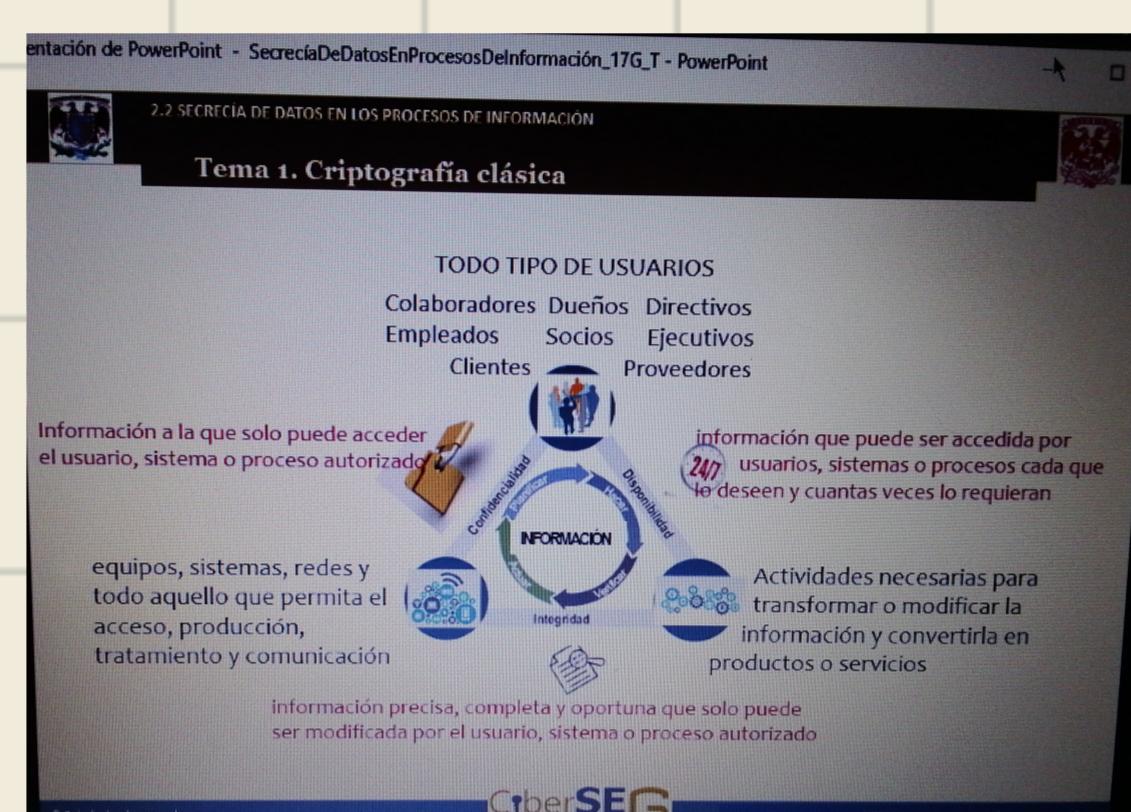
Criptografía Clásica: ¿Por qué es necesario proteger los procesos de información?

Porque existe desconfianza o peligro de que la info sea modificada, destruida, falsificada o revelada por algún usuario o proceso indeseado.

Se requiere mantener oculta y resguardada la info.

Criptografía: Ciencia encargada de transformar la información

Información:
Confidencialidad
Integridad
Disponibilidad



Cueva arte rupestre data hace 31,000 años

1096 - 1291 DC Las Cruzadas

Técnicas clásicas de cifrado

Sustitución

Transposición

↓
monoalfabética

Polialfabética

Polybios

César

Afín

monoalfabética

Polialfabética

Playfair

Hill

inversa, simple, doble, grupos, series columnas, filas, máscaras rotativas

Periodica No periodica

- Alfabeti
- Bazarics
- Vigenere
- Beaufort

- Vernam
- Enigma

Sistema Criptográfico / Criptosistemas

Clave, mensaje claro, algoritmo de cifrado o de descifrado

Enigma 2da Guerra Mundial 1939-1945

Enigma (2001) → Relis en las diapositivas

Esteganografía vs Criptografía

↓
Oculta la información
en un portador de
modo que no sea advertida
su existencia

↳ Se utiliza para cifrar
información de manera que
sea ininteligible para todo
intruso

Criptosistema



Cifrado simétrico → una clave DES y AES

Cifrado asimétrico → dos claves RSA, Diffie-Hellman, El Gamal

Funciones Hash: algoritmo matemático que transforma

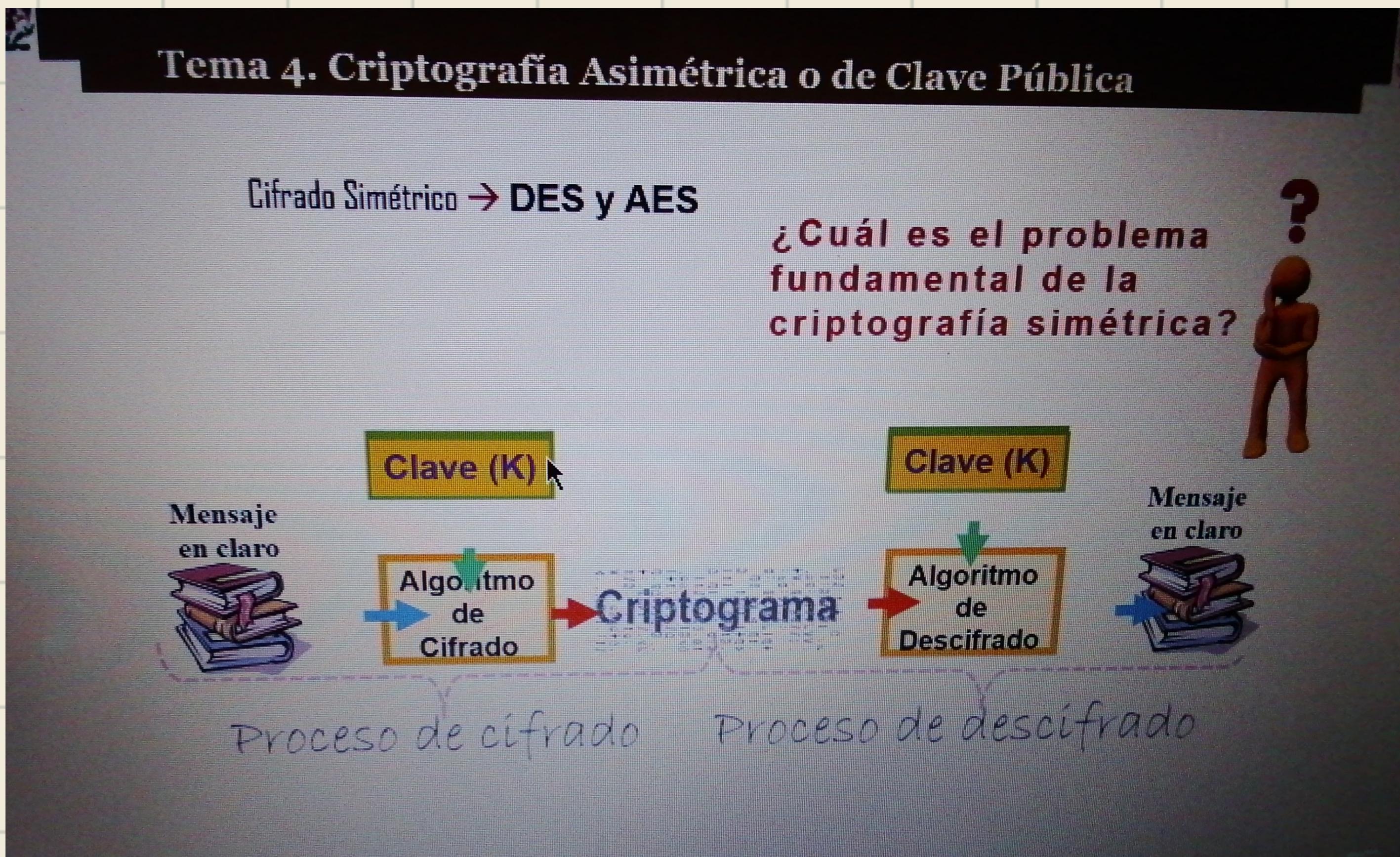
Características de los algoritmos de cifrado

Característica de las funciones hash

Integridad de los mensajes autenticidad de mensajes y su origen

AES predecesor DES, es rápido tanto en software

Tema 4. Criptografía Asimétrica o de Clave Pública



Diffie-Hellman Clave pública desarrollado por Whitfield Diffie

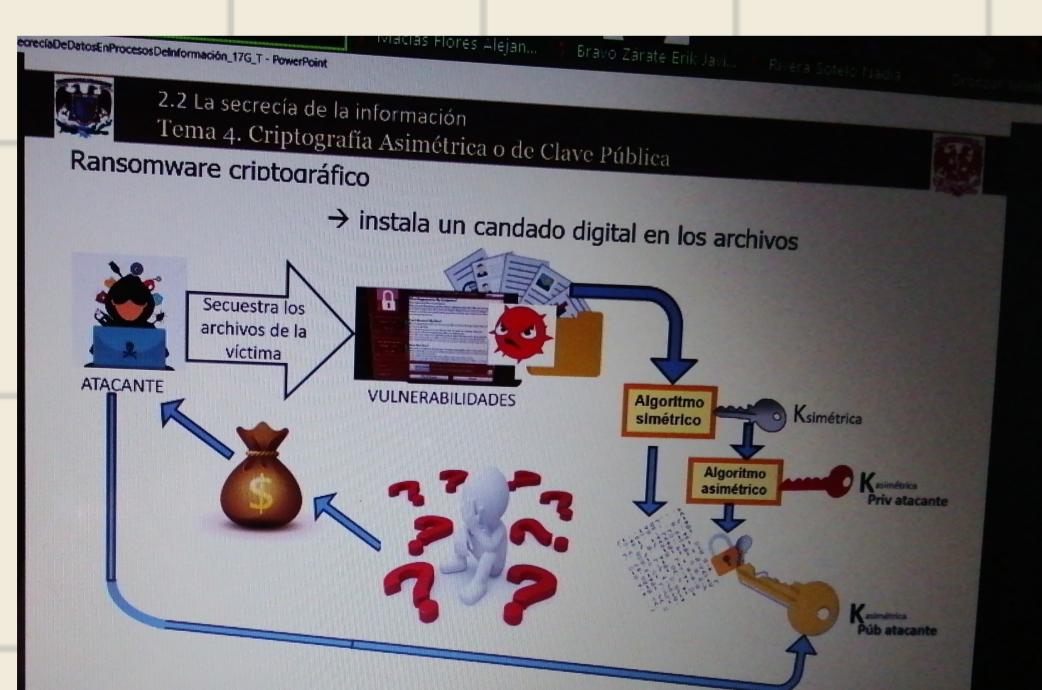
Forma totalmente nueva

RSA más conocido y representativo

↳ factorización de números muy grandes, la obtención de la clave pública consiste en multiplicación de 2 números primos p y q que por lo menos sean de 200 dígitos cada uno

algoritmos asimétricos para proteger mensajes cortos creando claves de 8-16 dígitos ↳ resguardar clave simétrica

Ransomware: Malware que impide a usuario



Blockchain: (cadena de bloques), funciona de manera distribuida

Nos da confianza, anonimato, integridad, redundancia

descentralización y transparencia

Uso: Criptomonedas, contratos inteligentes, salud, reclamos de Seguro, compraventa de propiedades