Charla introductoria. . .

Nathan C. Ryan

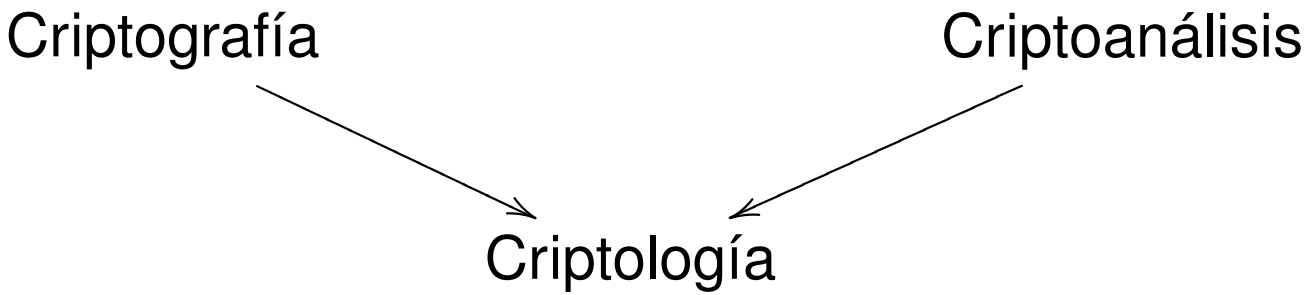
nryan@fing.edu.uy

10 de marzo de 2014

¿Qué es la criptografía?

- κρυπτoζ – oculto
  γραφειν – escribir
- De Wikipedia:

> *. . . tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.*


Criptografía
Criptoanálisis
Criptología

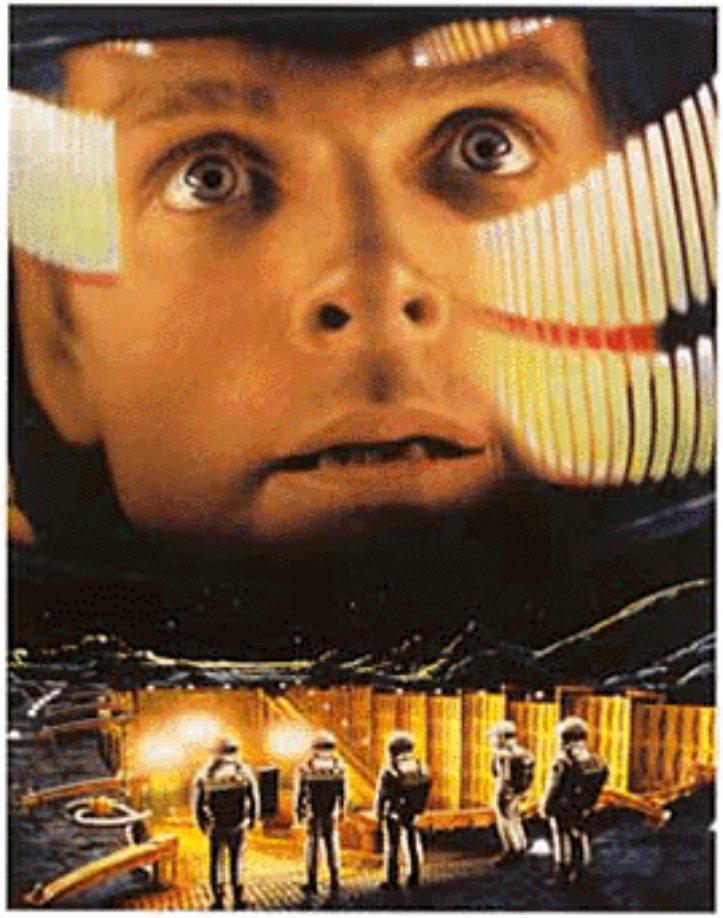
Sistemas convencionales de criptografía (una clave)

- **Cifrado rotado** Se cambia cada letra con la letra que sucede k pasos más adelante en el alfabeto.
- Por ejemplo, si $k = 5$,

$$\texttt{HOLA} \Rightarrow \texttt{MTPF}$$

- Según Suetonius, Julio César usó este cifrado con $k = 3$, y por eso se llama el cifrado César.

Un ejemplo famoso. . .



Dos clases de cifrados

- **Cifrado de sustitución**: cambiar cada letra con otra
- **Cifrado de transposición**: permutar las letras

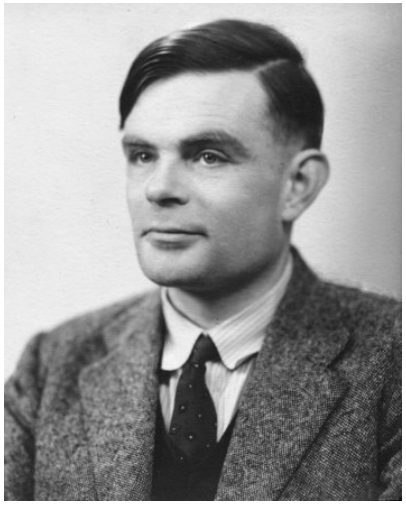
Estas dos clases de cifrados se pueden romper con computadoras y métodos estadísticos.
Cifrados modernos son combinaciones de los dos tipos.

Enigma

- Diseñado por A. Scherbius en los 1920s y usado por los alemanes en la segunda guerra mundial.

Rompiendo Enigma

- Roto por M. Rejewski, H. Zygalski y J. Rozyski en los 1930s. A. Turing y, entre otros, M. Batey siguieron mejorando las herramientas que desarrollaron los polacos.



Cifrados modernos

- **Data Encryption Standard** (DES)
  - NIST (NBS) 1977
  - $2^{56} \approx 10^{17}$ claves
  - actualmente se usa solamente como 3-DES, NIST 1999
- **Advanced Encryption Standard** (AES)
  - NIST 2001, recomendad más que 3-DES
  - 2^{128} ó 2^{192} ó 2^{256} claves
- Partículos en el universo $\approx 2^{240}$.

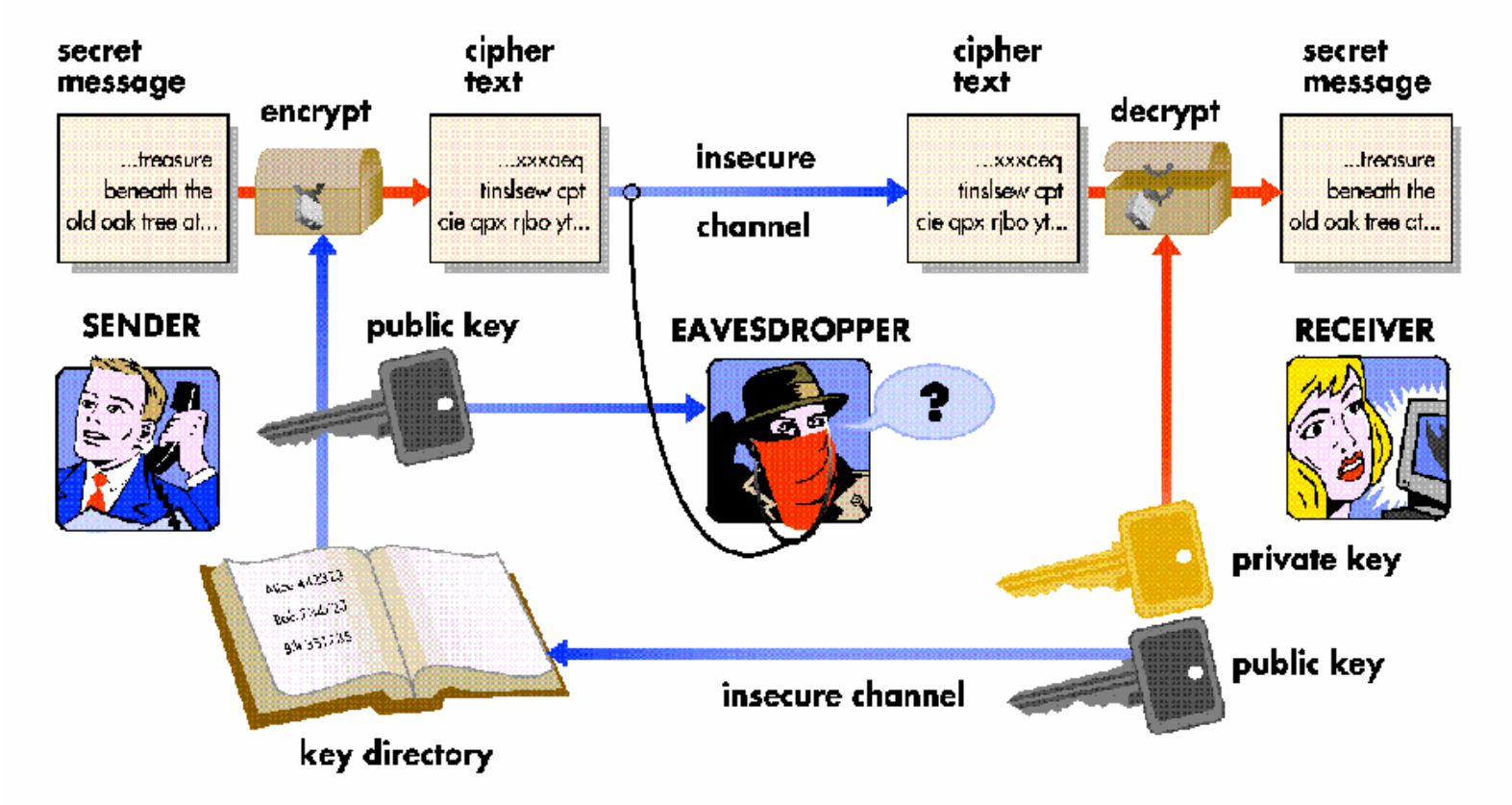
Cifrados con claves simétricas

- Estos sistemas usan la misma clave para cifrar (convertir texto plano a text cifrado) y para descifrar (convertir texto cifrado a texto plano).
- No tienen que ser idénticas pero una es una transformación simple de la otra.
- Todos los sistemas mencionados hasta ahora son de este tipo.
- Estos sistemas requieren un secreto compartido y él que quiere cifrar y la que quiere descifrar tienen que compartir las claves de alguna manera.

¿Cómo se comparten las claves?

- **Pregunta**: ¿Cómo se puede transmitir seguramente la clave secreta (y compartida) al usuario?
- Dos soluciones (W. Diffie y M. Hellman, 1976):
  - criptografía con clave pública
  - protocolos para establecer claves

Cifrados con clave pública (dos claves)



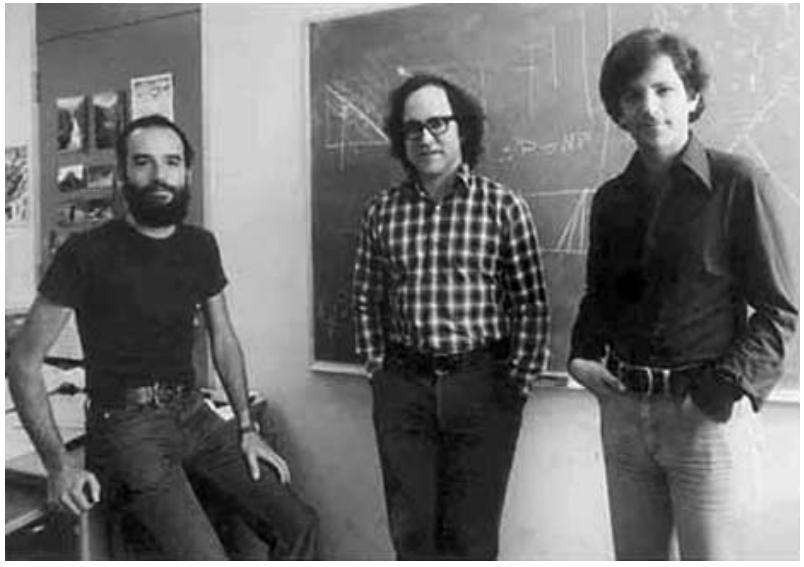
Personajes importantes en la creación de PKC

- Oficialmente PKC era inventada por W. Diffie y M. Hellman en Stanford en 1976.

- También, secretamente, era inventada por J. Ellis en GCHQ Gran Bretaña, unos años antes.

- La **seguridad** de un sistema de clave pública o de un protocolo para establecer claves tiene como base algún **problema matemático** que es pensado (aunque típicamente no es probado) ser muy **difícil**.
- La idea es que un advesario tendría que resolver una instancia de este problema difícil para **romper** el sistema.
- En general, el problema matemático viene de la **teoría de números**.

- El sistema de uso más general es **RSA** (**R**ivest, **S**hamir, **A**dleman, 1978).



- Como base tiene el **Problema Factorización de Enteros**, o sea, dado un entero, hallar sus factores primos

$$422978060257941524295951520503452 3 =$$
$$4657890876549877 03 \times 9080892435402941$$

Como usar PKC

- Cada usuario tiene una clave pública e para cifrar y una clave privada d para descifrar.
- Para mandar un mensaje confidencial m a **Alice**, el usuario **Bob** encuentra la clave pública e de **Alice**, cifra el mensaje m con e y manda el mensaje

$$c = E_e(m)$$

como text cifrado.

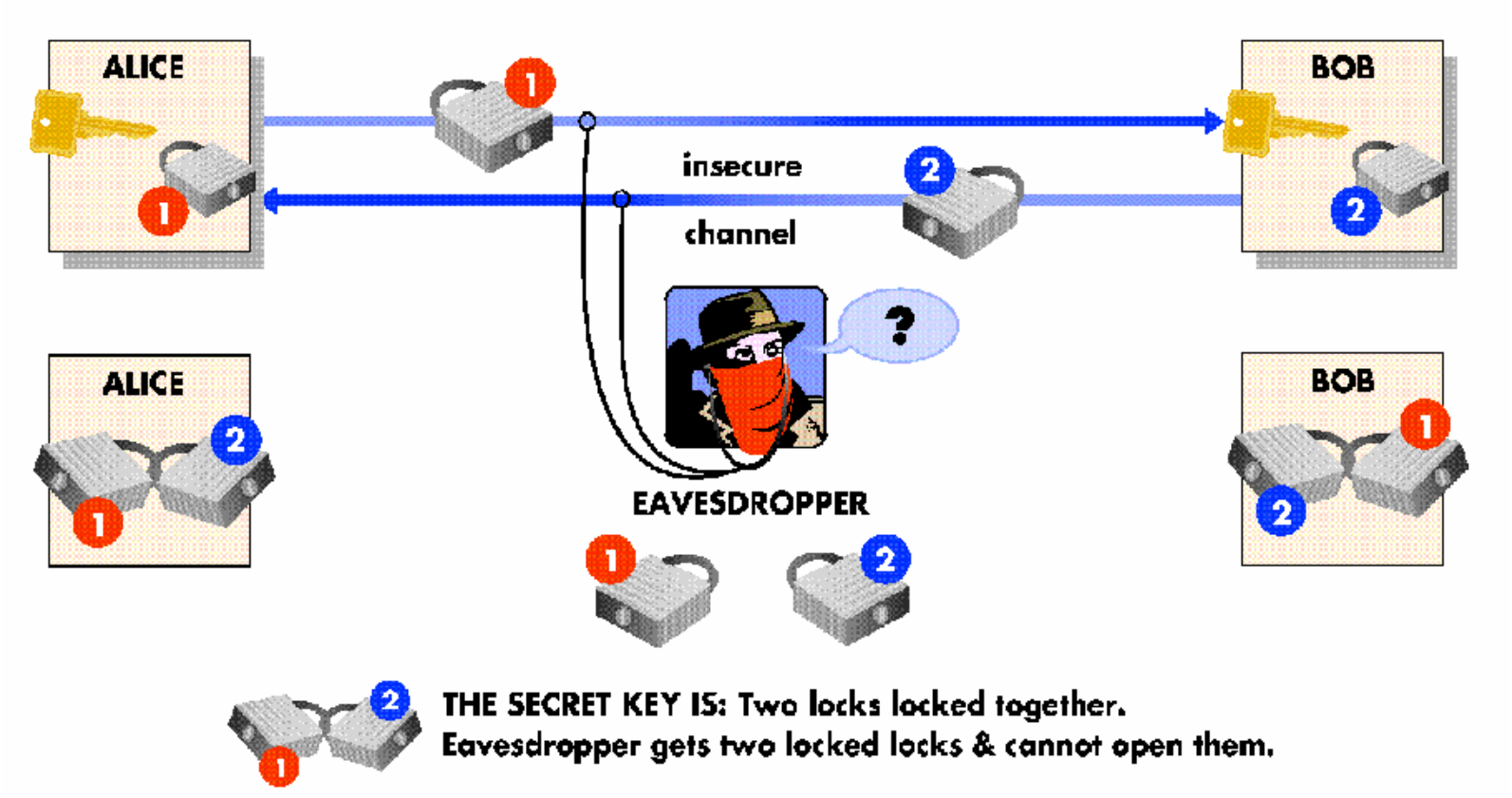
- **Alice** entonces descifra c con su clave privada d para obtener

$$D_d(c) = D_d(E_e(m)) = m.$$

Desventajas de sistemas de claves públicas

- Son más lentos de sistemas convencionales por un factor de 1000 a 1500.
- En el contexto de cifrar en general se usan casi siempre para compartir claves en una manera segura y, usando estas claves compartidas, el cifrado se hace con sistemas convencionales (como AES).

Protocolo para establecer claves



Protocolos más comunes

- PKC
- Protocolo de Diffie-Hellman (DH) (W. Diffie y M. Hellman, 1976)
- Criptografía con curvas elípticas (ECC)
- La seguridad de DH y de ECC tiene como base el problema del logaritmo discreto (DLP) para cuerpos finitos y curvas elípticas, respectivamente.

¿Qué se puede hacer con criptografía moderna?

- **Confidencialidad**: mantener secreto los datos de todos excepto aquellos que estén autorizados a verlo
- **Integridad de data**: asegurando que los datos no hayan sido alterados por medios no autorizados cambiado
- **Autenticación de origen de data**: corroborar la fuente de los datos
- **Autenticación de entidad**: corroborar la identidad de una entidad
- **No repudiación**: prevenir una entidad negar compromisos o acciones anteriores

Firmas digitales

- Una medida para **autenticación** y **no repudiación**.
- Factible usando PKC.
- Para firmar un mensaje m, Alice "descifra" m con su clave privada d para obtener $s = D_d(m)$ y manda el par (m, s) a Bob.
- Bob busca la clave pública e de Alice y "cifra" s con e para obtener

$$E_e(s) = E_e(D_d(m)) = m.$$

Sistemas existentes

- **Digital Signature Algorithm** (DSA), NIST 2000
- **RSA**, ANSI X9.31, 1998
- **Elliptic Curve Digital Signature Algorithm** (ECDSA), ANSI X9.62

¿Cuál es la relación entre criptografía y seguridad de datos?

Constantmente escuchamos de

- worms, viruses, Trojan horses
- páginas de web desfigurados
- computadoras hackeadas
- robo de identidad
- phisheando
- warwalking y wardriving
- robo de números de tarjetas de crédito

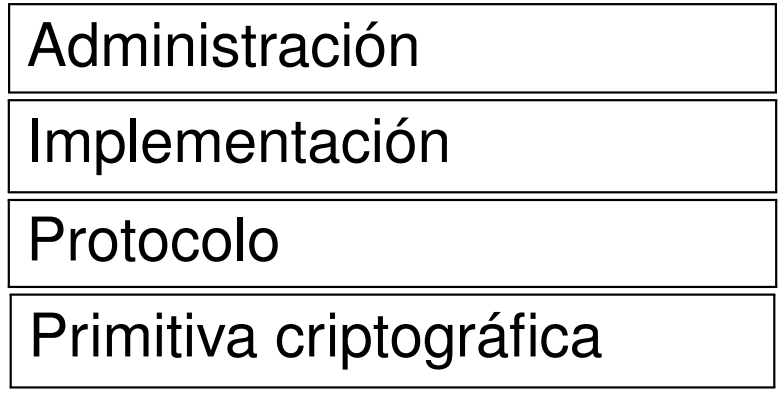
¿Quién tiene la culpa? ¿Criptografía?

Primitiva criptográfica

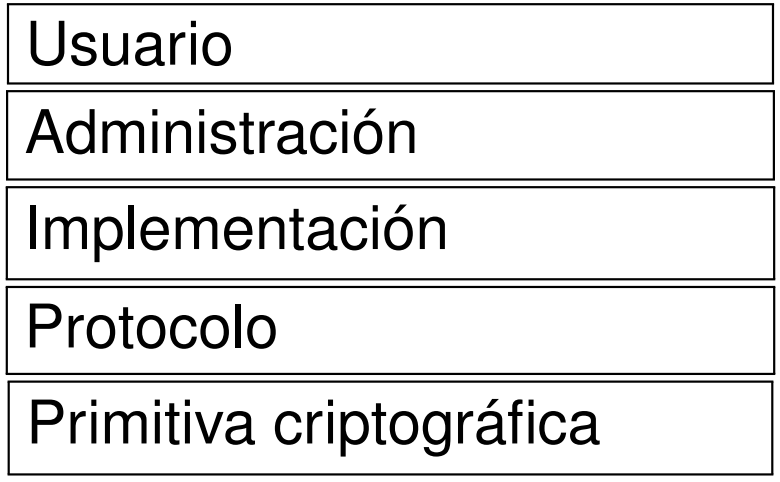
¿Quién tiene la culpa? ¿Criptografía?

¿Quién tiene la culpa? ¿Criptografía?

¿Quién tiene la culpa? ¿Criptografía?



¿Quién tiene la culpa? ¿Criptografía?



Primitiva

Una herramienta rota

- **SHA-1** (**S**ecure **H**ash **A**lgorithm **1**) es una **función hash**.
- Se usan funciones hash para prevenir falsificación de firmas digitales.
- En 2005, X. Wang y H. Yu de la Universidad Shandong y Y.L Yin, un consultador independiente, encontraron una colisión en SHA-1 2000 veces más rápido que fuerza bruta.

Protocolo

Suplantación

- Gary sustiya la clave pública e_A de Alice con su propia clave pública e_G.
- Bob cifra un mensaje m para Alice usando e_G, pensando que está usando e_A.
- Gary intercepta el texto cifrado c de Bob y lo descifra.
- **Peor**: Recibe el mensaje de Bob y lo cambia con otra mensaje y lo manda a Alice. Ella piensa que se está comunicando con Bob.

Implementación

Claves predecibles

- En vez de generar una clave en una manera aleatoria, se incorpora información predecible (p.ej., la fecha, la dirección IP de la máquina,etc.) en la generación de la clave.
- Si uno usa un “pseudo-aleatorio” generador de bits, el generado no arranca un “seed” diferente cada vez.

Administración

Falla de instalar:

- patches y upgrades
- software contra virus
- upgrades de la red
- cortafuegos
- software para cifrar
- seguridad física

Usuario

- mala administración de su propia computadora
- mala elección de contraseña (o no contraseña)
- usando la misma contraseña para varios sistemas y para mucho tiempo
- compartiendo contraseñas
- acceso fácil a la computadoras