Criptografía Simétrica - Parte 3

Miguel Angel Astor Romero

4 de junio de 2019

Agenda

Tipos de cifrado

Cifrado simétrico

Conjunto de algoritmos y técnicas de cifrado que utilizan una única clave de cifrado secreta, compartida entre los participantes de la comunicación cifrada.

Cifrado asimétrico

Conjunto de algoritmos y técnicas de cifrado que utiliza dos claves de cifrado: una secreta o privada conocida solo a su dueño, y otra publica conocida por todo el mundo.

Modelo Básico de Criptografía Simétrica

Cuando es Posible Romper Algoritmos de Cifrado

En general, es posible romper un criptosistema si se posee alguno de los siguientes:

- Conocimiento del algoritmo aplicado.
- Propiedades estadísticas del texto cifrado.
- Muchos textos cifrados de ejemplo.

Criptoanálisis por Análisis de Frecuencia

A	12,53	**B**	1,42	**C**	4,68	**D**	5,86	**E**	13,68	**F**	0,69
G	1,01	**H**	0,70	**I**	6,25	**J**	0,44	**K**	0,01	**L**	4,97
M	3,15	**N**	6,71	**Ñ**	0,31	**O**	8,68	**P**	2,51	**Q**	0,88
R	6,87	**S**	7,98	**T**	4,63	**U**	3,93	**V**	0,90	**W**	0,02
X	0,22	**Y**	0,90	**Z**	0,02						

- En español las vocales suelen ocupar el 45 % del texto.
- La E y la A son las letras más fáciles de identificar.
- Las consonantes más frecuentes son: S, R, N, D, L y C.
- Las menos frecuentes son: Z, J, Ñ, X, W y K.
- También se aplica por frecuencia de palabras.

Examen de Kasiski

Se aplica al cifrado de Vigenère. Ayuda a estimar la longitud de la clave.

CLAVE	ABCDABCDABCDABCDABCDABCDABCDABCD
Texto plano	**CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY
Cifrado	**CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

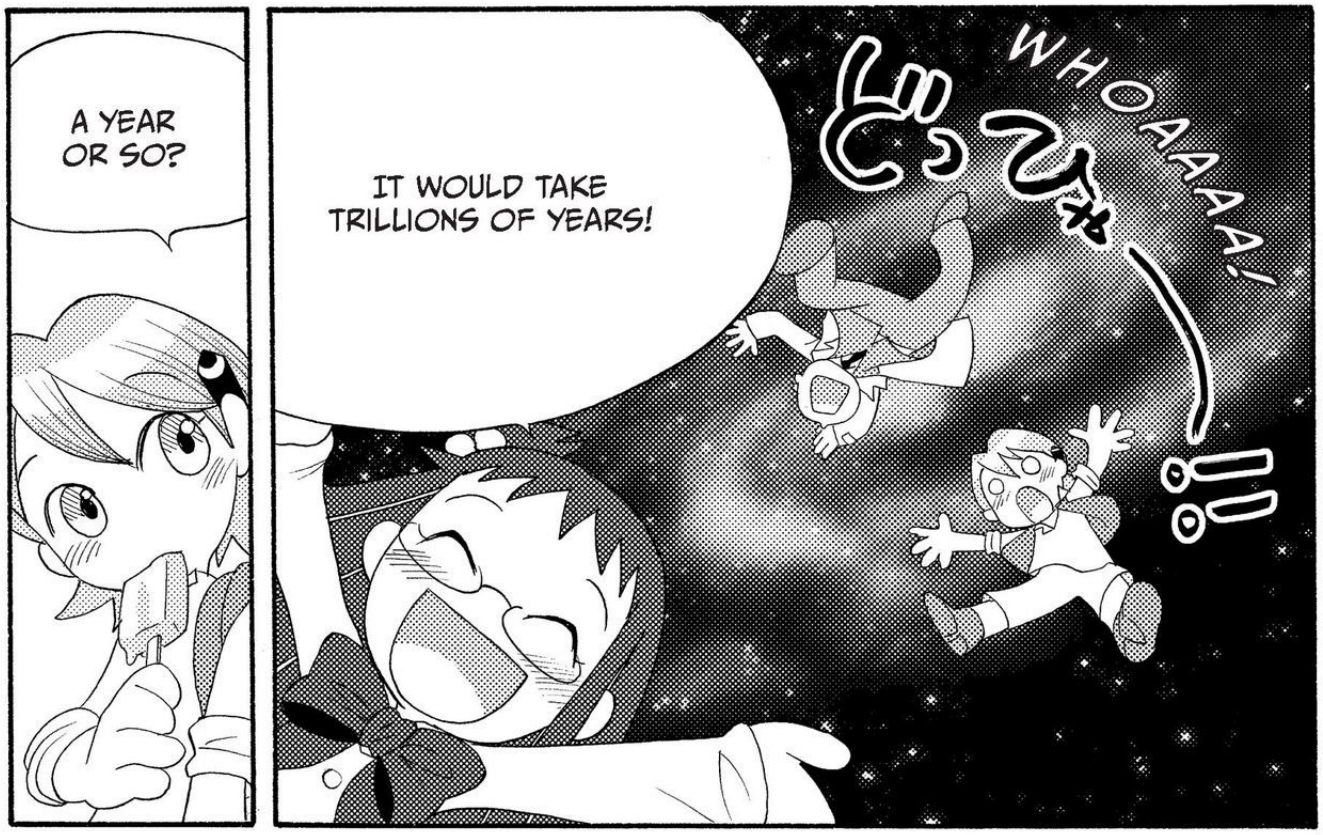
Criptoanálisis a Criptosistemas Digitales

- Se distinguen tres clases principales de criptoanálisis para cifrados de flujo y bloques:

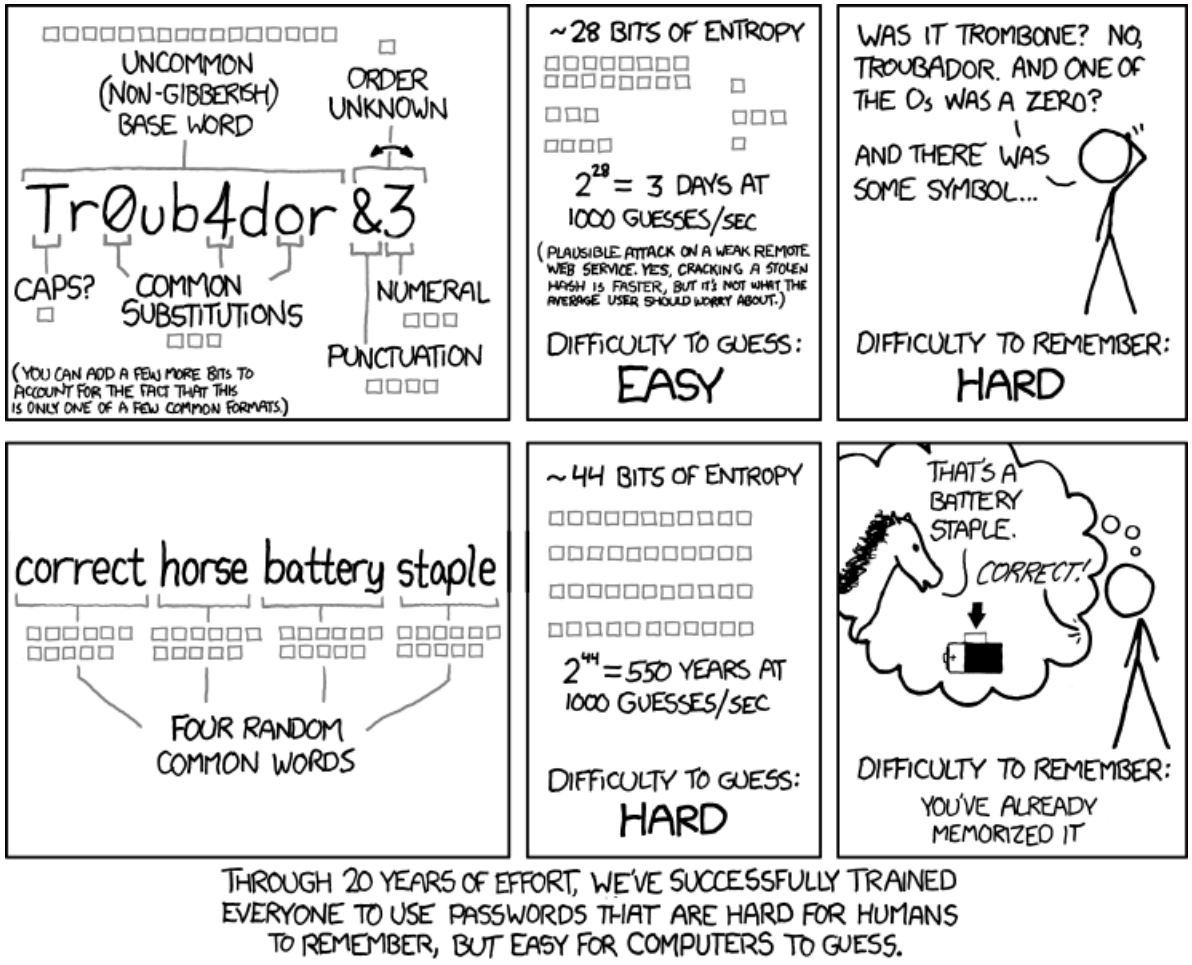
Lineal	búsqueda de aproximaciones afines al algoritmo de cifrado.
Diferencial	análisis de la transformación que realiza el algoritmo sobre el texto plano.
Fuerza bruta	búsqueda exhaustiva en el espacio de claves.

Ataques de Fuerza Bruta

Ataques de Fuerza Bruta



Fuerza del Espacio de Claves



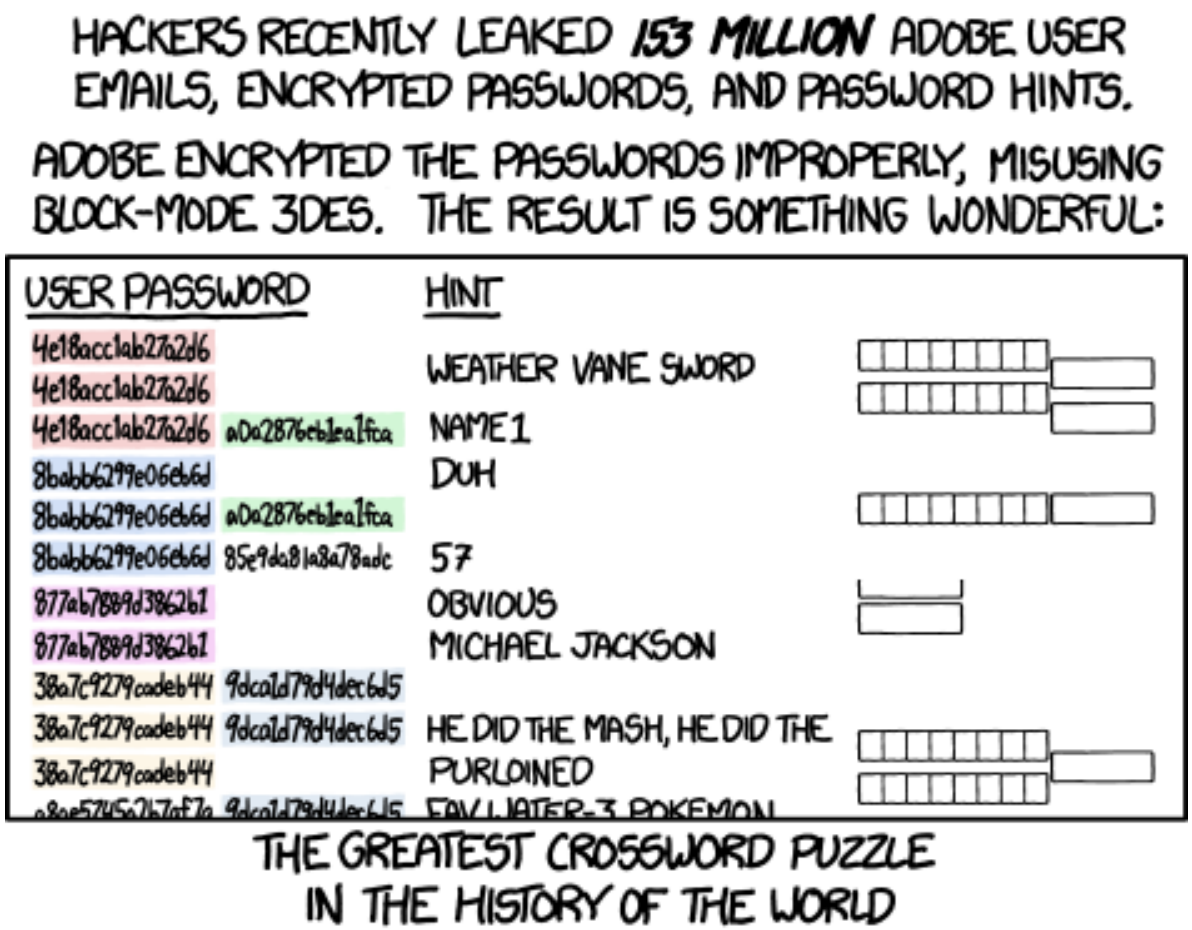
Salado de Contraseñas

- Mecanismo inventado para el sistema operativo UNIX en 1970.
- Consiste en concantenar una sal aleatoria a las contraseñas antes de almacenarlas.
- Las contraseñas saladas no se almacenan directamiente, sino su *hash*.
- Archivo `/etc/shadow/`.

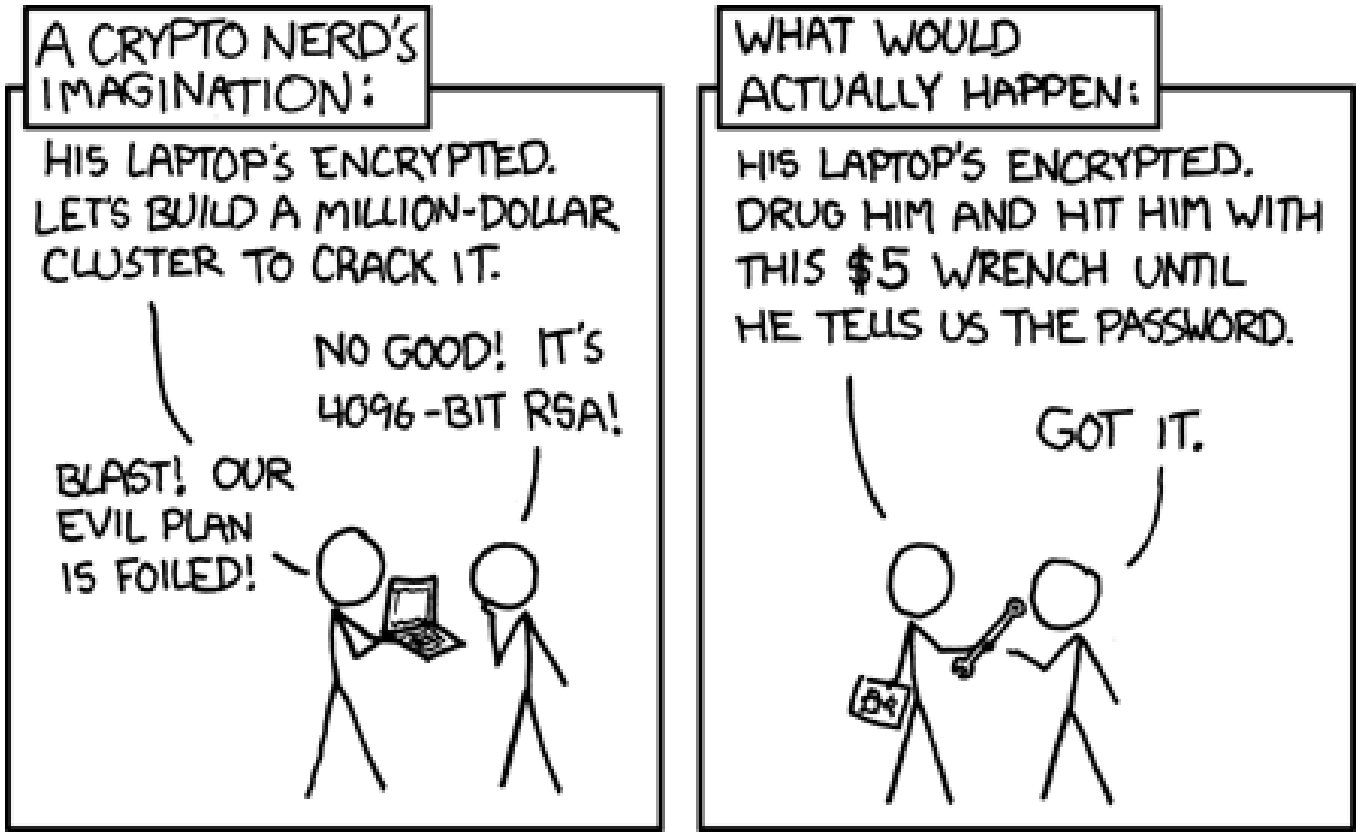
Sal Aleatoria

Número aleatorio concatenado a una contraseña antes de almacenarla.

Que Pasa si no se Salan las Contraseñas



Rubber Hose Cryptanalysis



Generadores Pseudo-Aleatorios

Basados en una pareja de funciones:

$$f : X \to X$$

$$g : X \to Y$$

donde

X conjunto grande de números.

Y $\{0, 1\}$

Dada una semilla $s \in X$, se define la suseción:

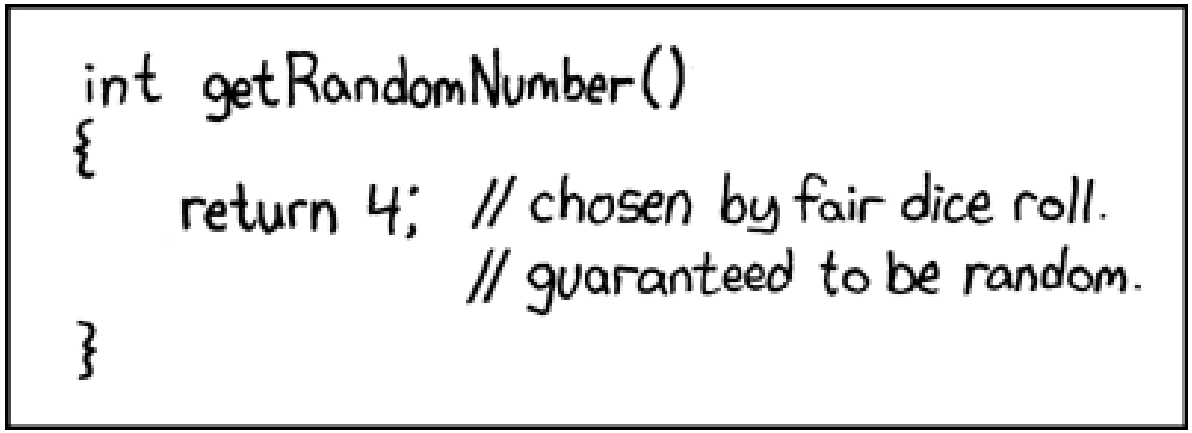
$$\begin{cases} x_0 = s \\ x_i = f(x_{i-1}) \end{cases}$$

Finalmente, la sucesión aleatoria $y_0, y_1, y_2, \ldots$ se define como:

$$y_i = g(x_i) \quad \forall\ i \geqslant 0$$

El Problema de la Generación de Números Aleatorios

Las computadoras son máquinas determinísticas por naturaleza.



Generador RC4

Generación de Claves

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := j + S[i]
    j := j + key[i % keylength]
    j := j % 256
    swap(S[i], S[j])
endfor
```

Generación Pseudo-Aleatoria

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) % 256
    j := (j + S[i]) % 256
    swap(S[i], S[j])
    K := S[(S[i] + S[j]) % 256]
    print(K)
endwhile
```

Interfaces de Linux para Generación de Números Aleatorios

- Linux introdujo el concepto de generación de números aleatorios en el *kernel* del sistema operativo.
- Se proveen dos interfaces:
  - Los archivos especiales `/dev/random/` y `/dev/urandom`.
  - La llamada al sistema `getrandom()`.

¿Que ventajas tiene generar números aleatorios en el *kernel*?

/dev/random - random(4)

- Introducido en 1994 por Theodore Ts'o.
- Basado en funciones *hash* en lugar de criptosistemas.
  - Evade las leyes de exportación de Estados Unidos.
- Considerado obsoleto.

Procedimiento

- Mantener un *pool* de entropía.
- Al solicitar N bits del archivo, retornar el hash de los primeros N bits del pool si están disponibles.
  - La lectura es bloqueante si no están disponibles los bits.

/dev/urandom - random(4)

- Utiliza el *pool* de entropía para alimentar un generador de números pseudo-aleatorios.
- No es bloqueante.
- Apto para uso en criptografía si se da tiempo suficiente para alimentar el *pool* de entropía.

```
$ head -200 /dev/urandom | cksum | cut -f1 -d " "
```

getrandom(2)

```
#include <sys/random.h>
ssize_t getrandom(void *buf,
                  size_t buflen,
                  unsigned int flags);
```

Banderas Disponibles

`GRND_RANDOM` usar `/dev/random` en lugar de `/dev/urandom`.

`GRND_NONBLOCK` llamada no bloqueante bajo ninguna circunstancia.

Valor de Retorno

Bytes aleatorios almacenados en `buf`.

Definición

- Steganos: oculto – Graphos: escritura.
- Técnica de ocultación de mensajes.
- Provee confidencialidad y anonimato.

Portador

Esteganograma

Condiciones de la Esteganografía

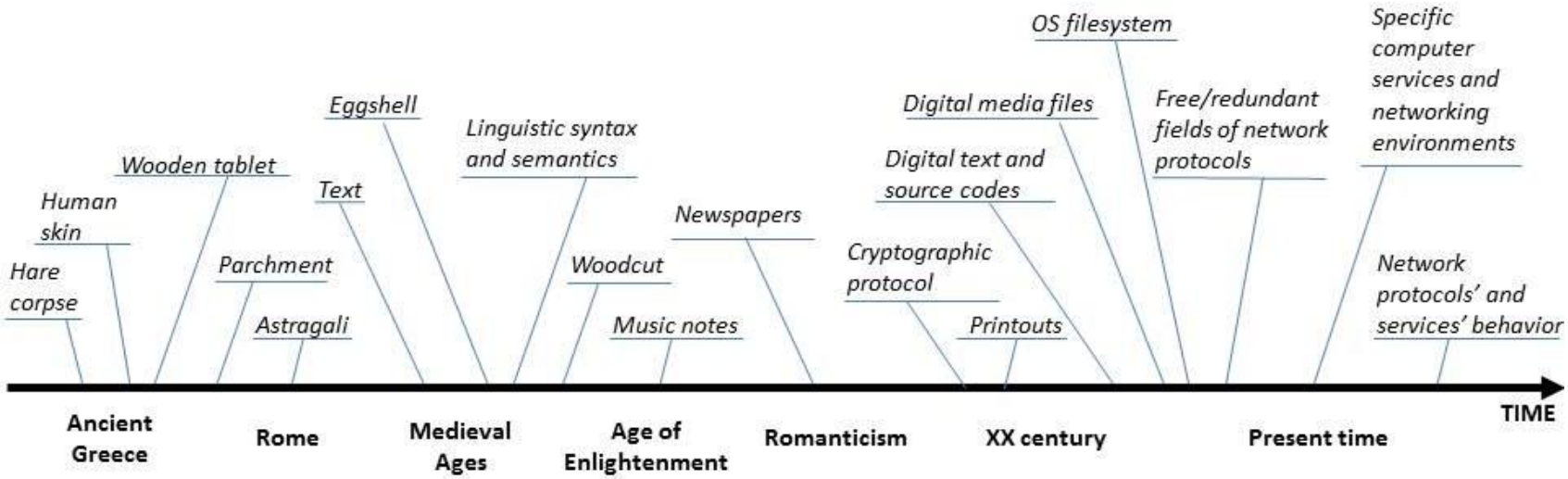
- El objetivo es transmitir un mensaje garantizando confidencialidad.
- El mensaje confidencial debe ir embebido en un mensaje portador aparentemente inocente.
- La confidencialidad viene dada por que tan bien se puede confundir el mensaje portador con otros mensajes legítimos similares.

Señal Portadora

Comparación con la Criptografía

		Criptografía	Esteganografía
Objetivo		Ofuscar el contenido de la comunicación.	Oculta el hecho de comunicación.
Características	Confidencialidad	Mensaje visible pero ilegible.	Mensaje invisible a un observador incauto.
	Seguridad	Depende de la clave de cifrado.	Depende del método de inserción del mensaje.
	Robustés	Depende del algoritmo de cifrado.	Invisibilidad perceptual, estadísitica o de protocolo.
	Ataques	Detección simple, extracción compleja.	Detección y extaccion complejas.
Contramedidas	Técnicas	Ingeniería inversa, criptoanálisis.	Estegoanálisis.
	Legales	Leyes de exportación.	Especificaciones rígidas.

Historia de la Esteganografía



Esteganografía Moderna

- Esteganografía lingüistica.
- Esteganografía en medios digitales.
- Esteganografía en sistemas de archivos.
- Esteganografía en redes.

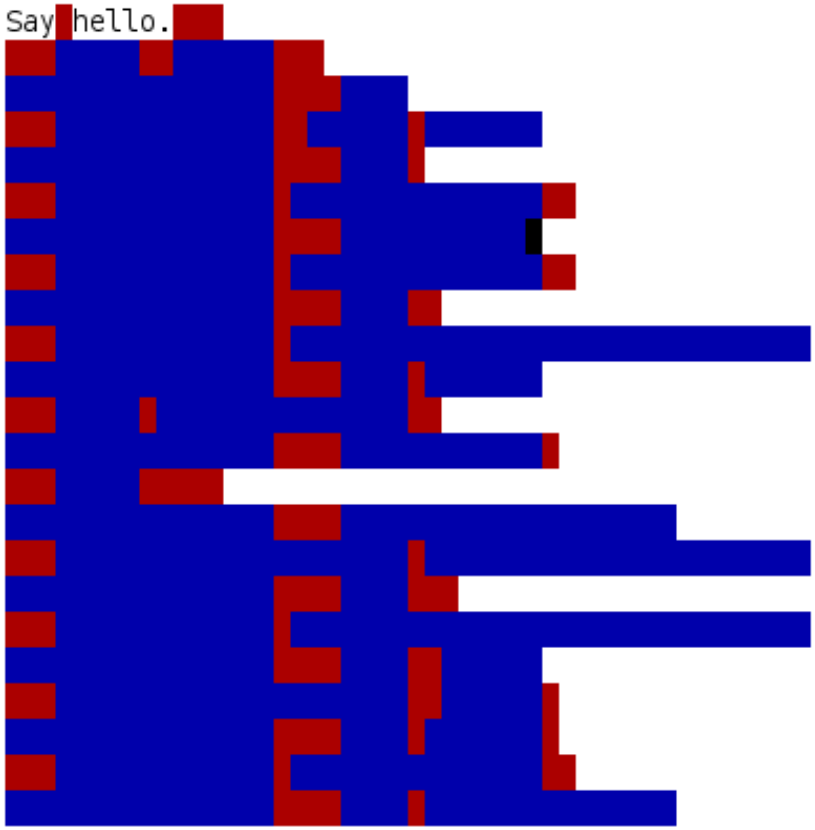
Esteganografía Lingüistica

- Uso del espaciado y/o signos de puntuación:
  - Lenguajes esotéricos.
  - Macros e interpretes automáticos.
- Selección y ordenamiento cuidadoso de palabras y sinónimos.
- SPAM!

Lenguajes Esotéricos

```
++++++++[>++++[>++>+++>+++>+<<<
<-]>+>+>->>+[<]<-]>>.>---.+++++
++..+++.>>.<-.<.+++.------.----
----.>>+.>++.
```

Whitespace



7,8-32 Anfang

Esteganografía en Medios Digitales

Imágenes

- Por dominio espacial o dominio de frecuencia.
- Aprovechando características de los formatos.
  - JPEG $\rightarrow$ Stegosploit.
- Puede usarse para firmar imágenes.

Audio

- Enmascaramiento de frecuencia, ocultación en ecos, codificación de fase, técnicas de espectro disperso.
- Códigos de corrección de errores.

Esteganografía en Sistemas de Archivos

- Inventados por Anderson, Needham y Shamir (1998):
  - Oculta los archivos y la metadata de los mismos.
  - Los archivos solo se pueden recuperar con sus respectivas claves.
  - Provee negación plausible.
  - Dos métodos:
    - Archivos aleatorios con vectores marcadores.
    - Particiones aleatorias.
- StegFS, Pang et al. 2003.

Dos Ejemplos Simples

- Concatenación en archivos binarios.
- Nombres de archivos.

Figura: Narbonic, ©2000-2006 por Shaenon K. Garrity.

Narbonic

rednaeroc darnoc lrac skoob dlo This inscription could be seen on the glass door of a small shop but naturally this was only the way it looked if you were inside the dimly lit shop looking out at the street through the plate-glass door Outside it was a gray cold rainy November morning The rain ran down the the glass and over the ornate letters Through the glass there was nothing to be seen but the rain-splotched wall across the street endquote
Meanwhile Im saving my money I want to buy one of those yellow inflatable life rafts Also Im looking around for a really intelligent chicken endquote

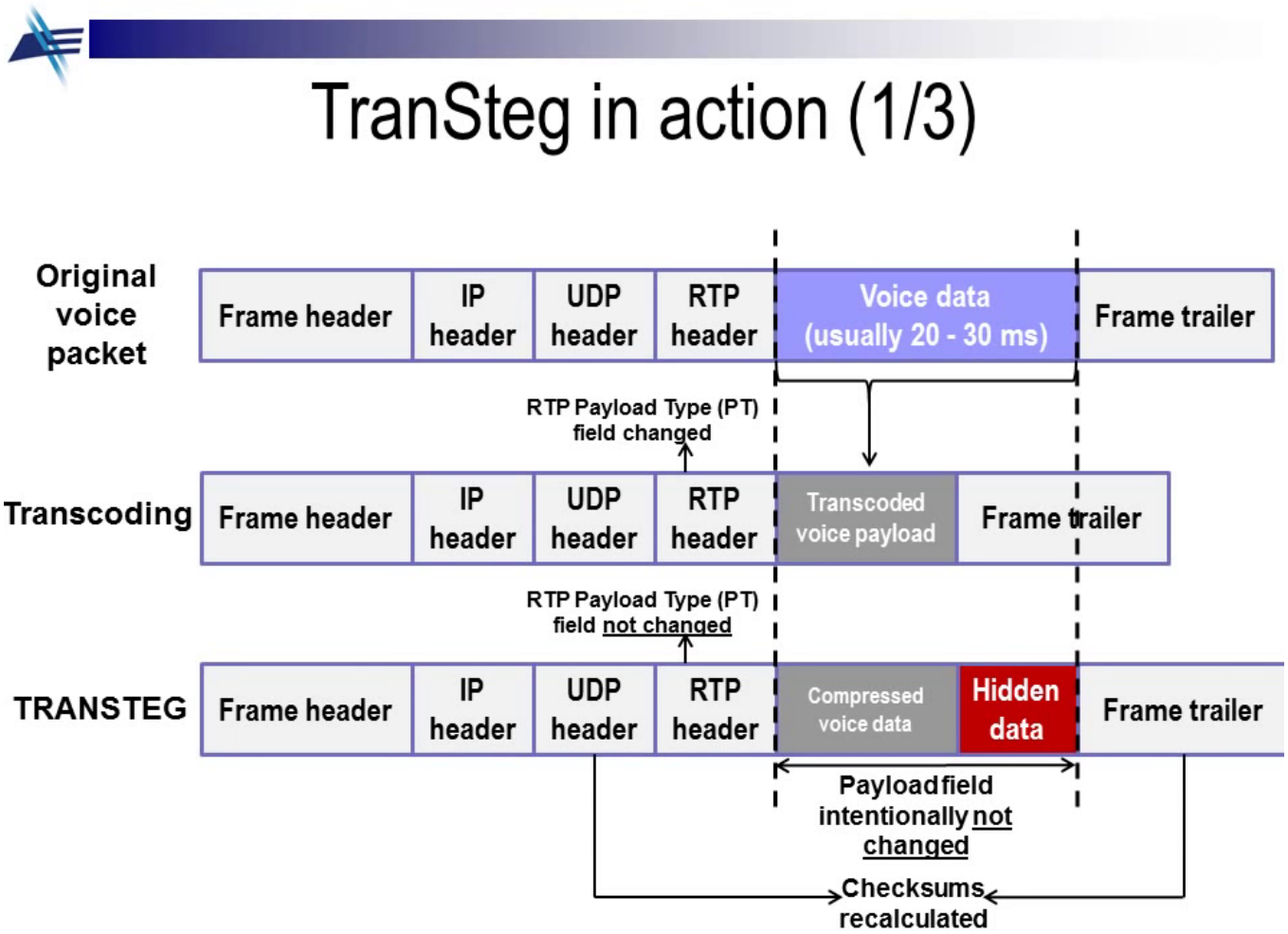
Esteganografía en Redes

- Explotar características de protocolos de red.
- Intra-protocolo o inter-protocolo.
- Aprovecha las siguientes características de las redes:
  - La existencia de retrasos o errores en la transmisión.
  - Información redundante o reservada en los protocolos.
  - Libertad de implementación en los protocolos.
- Tecnologías VoIP y de streaming de video pueden ser susceptibles a esteganografía de audio y de redes.

Modos de Inserción del Mensaje

- Modificación del PDU, el payload o ambos.
- Alteración de la secuencia de envío de mensajes.
- Codificar el mensaje en retrasos controlados.
- Introducir "errores" en los mensajes.
- Esteganografía de transcoding (TranSteg):
  - Utiliza principalmente el protocolo RTP.

TranSteg


TranSteg in action (1/3)
Original voice packet
Frame header
IP header
UDP header
RTP header
Voice data (usually 20 - 30 ms)
Frame trailer
RTP Payload Type (PT) field changed
Transcoding
Frame header
IP header
UDP header
RTP header
Transcoded voice payload
Frame trailer
RTP Payload Type (PT) field not changed
TRANSTEG
Frame header
IP header
UDP header
RTP header
Compressed voice data
Hidden data
Frame trailer
Payload field intentionally not changed
Checksums recalculated

Ejemplos con Protocolos Específicos

- SkyDe (2 Kbps):
  - Utiliza paquetes de Skype.
  - Esconde los mensajes en los silencios.
- StegTorrent (270 bps):
  - Utiliza el mecanismo de números de secuencia de µTP.
- WiPad (1.5 Mbps):
  - Utiliza el padding de frames en redes inalámbricas que usan OFDM.

Conclusiones

- Se estudiaron varias clases de criptoanálisis.
- Usualmente el eslabón más debil de un criptosistema son sus usuarios.
- La generación de números aleatorios es un problema dificil para las computadoras.
- La esteganografía es fascinante.

Tarea

- Hay 1 mensaje oculto en esta presentación.
- La tarea es identificarlo y realizar la actividad que indica.

Próxima Clase

- Taller 1:
  - Critpografía Simétrica
  - Esteganografía.
  - Estegoanálisis.
  - Stegosploit.

¿Preguntas?