

Seguridad en Sistemas de Información

Curso en Tamaulipas [Q2 2014]



Luis J. Dominguez Perez
Cinvestav, Mayo 19 de 2014

Contenido, sección I

Criptología: criptografía y criptoanálisis

Cifradores históricos

Ataques

Enigma

Cifradores contemporáneos

Introducción

Cifradores de Flujo

Cifradores de Bloque

Numeros Aleatorios

DES

Modos de operación

AES

Criptografía Pública

Introducción

Cuando escuchamos la palabra criptografía, las primeras cosas que podrían venirse a nuestra mente podrían ser:

- cifrado de correo
- acceso seguro a sitios web
- smart cards para aplicaciones bancarias
- el rompimiento de códigos durante la segunda guerra mundial, como el ataque a la máquina Enigma.

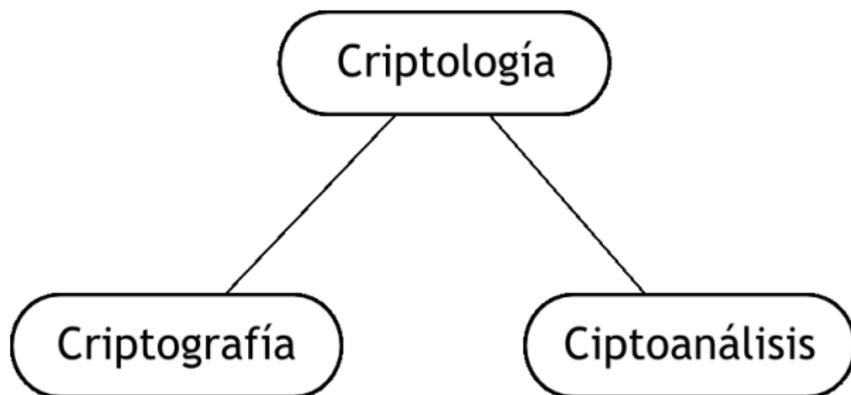


Inicios

La criptografía parece estar relacionada a la comunicación electrónica moderna. Sin embargo, la criptografía es un negocio viejo, sus primeros usos datan del año 2000 A.C. en el antiguo Egipto.

En la era moderna, hacemos uso intensivo de la computación. La criptografía es una aplicación de la computación muy importante, de hecho, la criptografía ¡es la primer aplicación de las computadoras! (junto con la balística).

Criptología

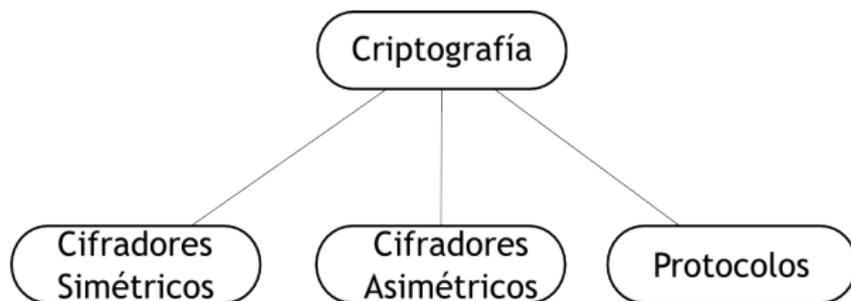


Criptografía y criptoanálisis

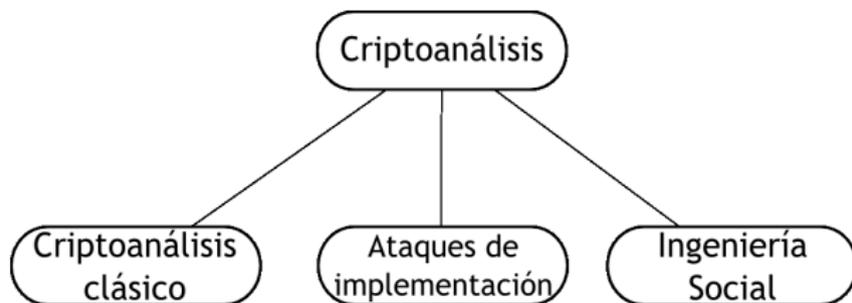
La criptología se divide en criptografía y criptoanálisis:

- **Criptografía.** Es la ciencia de escribir secretamente con la finalidad de ocultar el significado de un mensaje.
- **Criptoanálisis.** Es la ciencia y algunas veces el arte de romper criptosistemas.

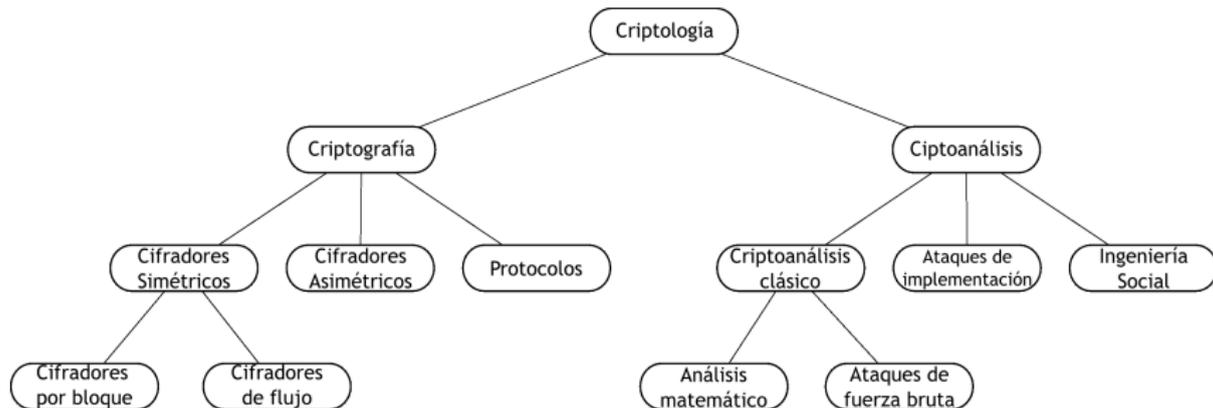
Criptografía



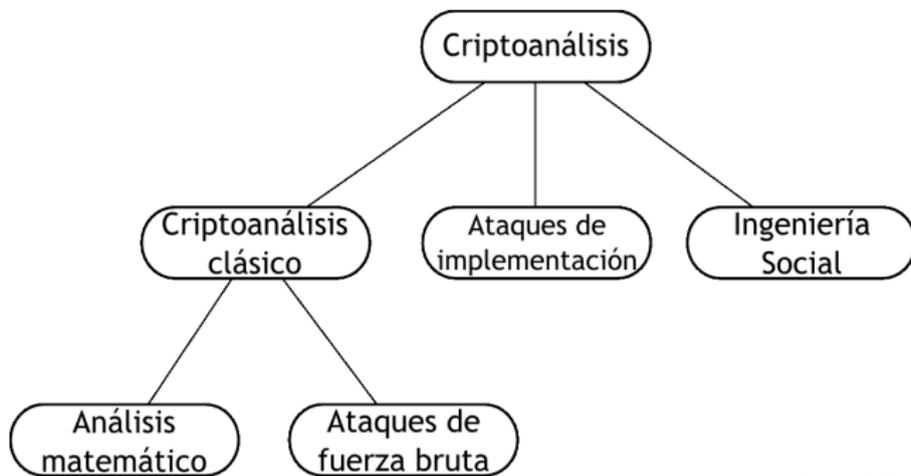
Criptoanálisis



Criptología



Áreas del criptoanálisis



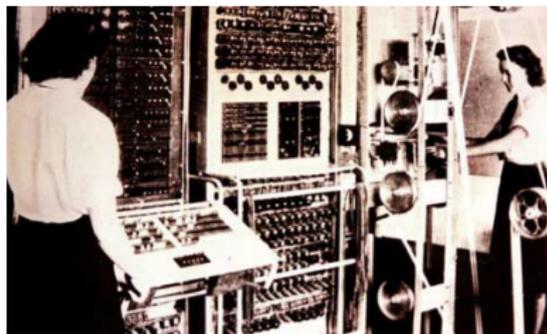
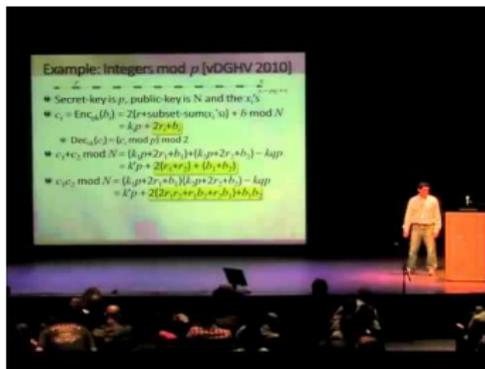
Criptoanálisis

Uno podría pensar que romper códigos es para la comunidad de servicios de inteligencia, o quizá de organizaciones criminales, y no debería de incluirse en una clasificación seria de las disciplinas científicas.



Criptoanálisis

Sin embargo, la mayoría de los criptoanálisis son realizados por investigadores respetables en la academia. El criptoanálisis es un área de importancia vital para los criptosistemas modernos: sin gente que intente romper los métodos de cifrado, nunca sabríamos si un método es realmente seguro o no.



Paradoja del cumpleaños

La probabilidad de que yo tenga el mismo cumpleaños que alguno de ustedes es:

$$1 - \left(\frac{365 - 1}{365} \right)^n .$$

¹uniformemente distribuida

Paradoja del cumpleaños

La probabilidad de que yo tenga el mismo cumpleaños que alguno de ustedes es:

$$1 - \left(\frac{365 - 1}{365} \right)^n .$$

¿Qué pasa si se replantea el problema a: la probabilidad de que cualquiera de nosotros tenga el mismo cumpleaños que otro?

Si se tienen 367 personas, la probabilidad es del 100%¹, sin embargo, con 57 aún se tiene un 99% de probabilidad.

¹uniformemente distribuida

Paradoja del cumpleaños

La probabilidad de que yo tenga el mismo cumpleaños que alguno de ustedes es:

$$1 - \left(\frac{365 - 1}{365} \right)^n .$$

¿Qué pasa si se replantea el problema a: la probabilidad de que cualquiera de nosotros tenga el mismo cumpleaños que otro?

Si se tienen 367 personas, la probabilidad es del 100%¹, sin embargo, con 57 aún se tiene un 99% de probabilidad....y con 23 se tiene cerca del 50%

¹uniformemente distribuida

Paradoja del cumpleaños

La probabilidad de que yo tenga el mismo cumpleaños que alguno de ustedes es:

$$1 - \left(\frac{365 - 1}{365} \right)^n .$$

¿Qué pasa si se replantea el problema a: la probabilidad de que cualquiera de nosotros tenga el mismo cumpleaños que otro?

Si se tienen 367 personas, la probabilidad es del 100%¹, sin embargo, con 57 aún se tiene un 99% de probabilidad....y con 23 se tiene cerca del 50% de ahí lo de paradoja.

¹uniformemente distribuida

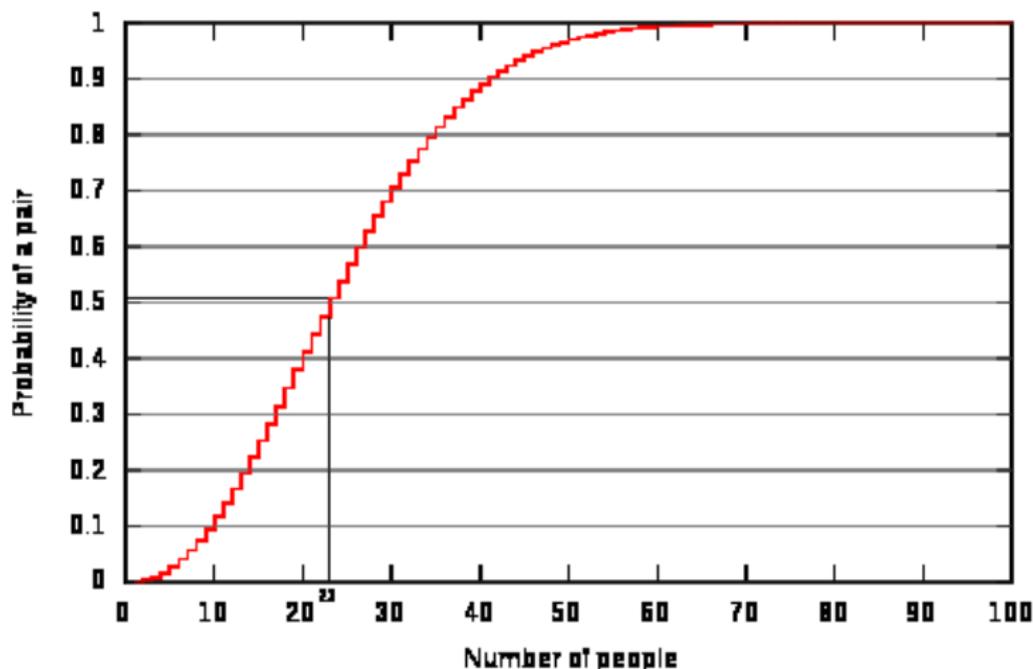
Probabilidad

La probabilidad de que no ocurra la colisión, depende en el número de personas. La fórmula viene dada por:

$$\begin{aligned}\bar{p}(n) &= 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \cdots \times \left(1 - \frac{n-1}{365}\right) \\ &= \frac{365 \times 364 \times \cdots \times (365 - n + 1)}{365^n} \\ &= \frac{365!}{365^n (365 - n)!} = \frac{n! \binom{365}{n}}{365^n} = \frac{{}^{365}P_n}{365^n}\end{aligned}$$

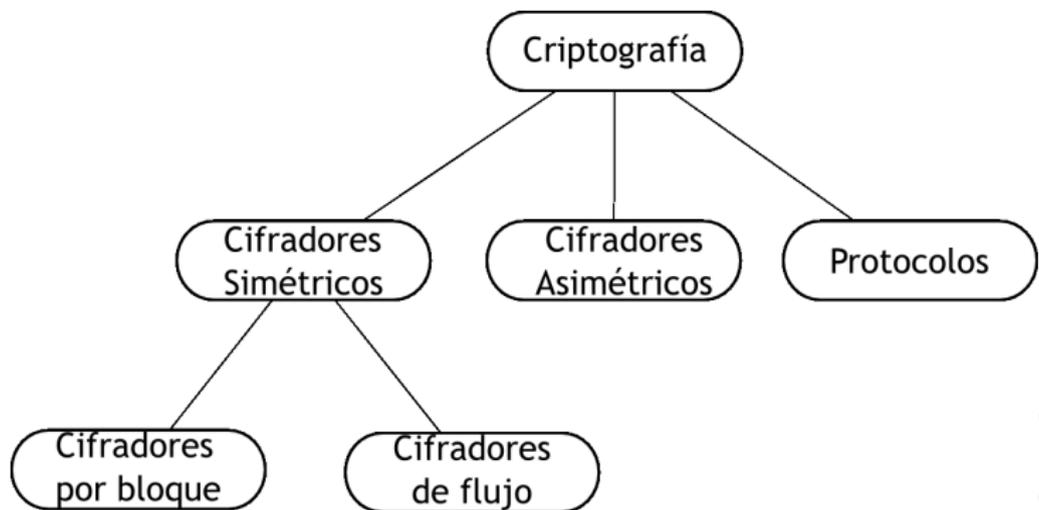
Entonces, la probabilidad de una colisión es: $p(n) = 1 - \bar{p}$.

Valores



Ejercicio: encontrar una colisión entre los participantes, y 2 de sus parientes.

Áreas de la criptografía



Criptografía, 1/3

La criptografía se divide en 3 partes principales:

- **Algoritmos simétricos.** Son lo que la mayoría de la gente piensa de la criptografía: dos partes tienen un método de cifrado y descifrado, y comparten una clave secreta.

La criptografía desde tiempos ancestrales hasta 1976 era exclusivamente simétrica. La criptografía simétrica sigue siendo fundamental hoy en día.



Criptografía, 2/3

- **Algoritmos asimétricos.** En 1976, un tipo diferente de cifrado fue introducido por Whitfield Diffie, Martin Hellman, y Ralph Merkle (aunque este último es generalmente menos reconocido).

En la criptografía de clave pública, un usuario posee una clave secreta como en los algoritmos simétricos, pero también una clave pública.

Podemos utilizar este tipo de criptografía para firmas digitales y el establecimiento de llaves, así como para el cifrado de datos tradicional.



Criptografía 3/3

- **Protocolos.** Hablando en términos concretos, los protocolos criptográficos es la aplicación de los algoritmos criptográficos.

Los algoritmos simétricos y asimétricos se pueden ver como los bloques de construcción, o cajas negras con las que las aplicaciones como la comunicación segura en internet se realiza.

Criptografía 3b/3

El esquema de Seguridad de Capa de Transporte (TLS), el cual es utilizado por todos los navegadores Web, es un ejemplo de un protocolo criptográfico.



Criptografía 3b/3

El esquema de Seguridad de Capa de Transporte (TLS), el cual es utilizado por todos los navegadores Web, es un ejemplo de un protocolo criptográfico.



Hablaremos de este protocolo más adelante.

Sistemas híbridos

En la práctica, la mayoría de las aplicaciones criptográficas utilizan tanto algoritmos simétricos como asimétricos (así como funciones picadillo). Esto es conocido, en algunas ocasiones, como esquemas híbridos.

La razón para utilizar ambos esquemas, es que cada uno tiene sus fortalezas y debilidades...

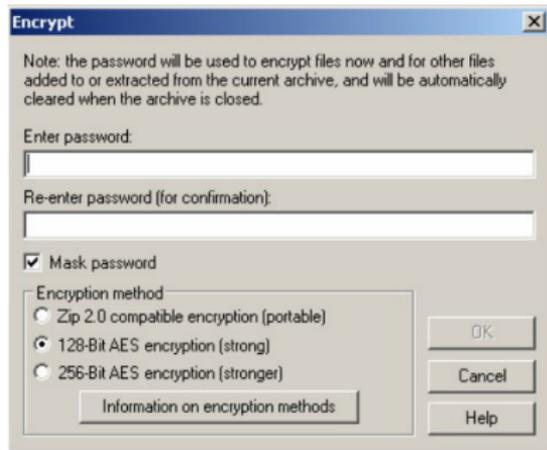
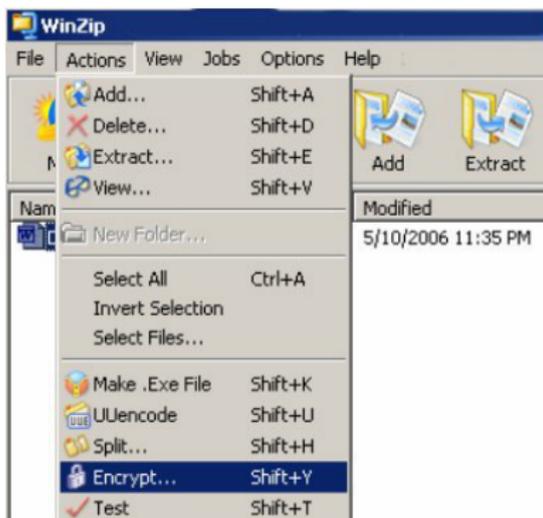
Sistemas híbridos

En la práctica, la mayoría de las aplicaciones criptográficas utilizan tanto algoritmos simétricos como asimétricos (así como funciones picadillo). Esto es conocido, en algunas ocasiones, como esquemas híbridos.

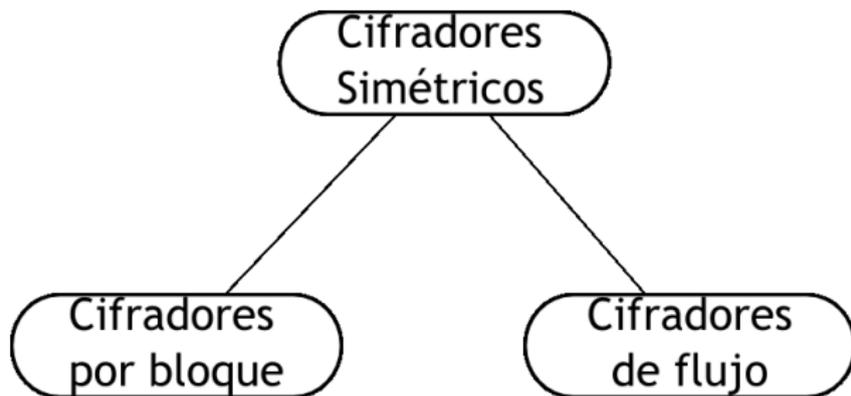
La razón para utilizar ambos esquemas, es que cada uno tiene sus fortalezas y debilidades... las cuales veremos a continuación.

Criptografía simétrica

Los esquemas de criptografía simétrica también son referidos como esquemas o algoritmos de clave-simétrica, clave-secreta, o clave-única.



Tipos de cifradores simétricos



Ejemplo

Dados Alice, y Bob, que se quieren comunicar a través de un canal inseguro (como internet, el aire, etc.)...

Ejemplo

Dados Alice, y Bob, que se quieren comunicar a través de un canal inseguro (como internet, el aire, etc.)...

El problema comienza cuando un tercero: Eve, Charlie u Oscar; tienen acceso al canal: metiéndose a un enrutador, escuchando las señales del radio del WiFi, etc.

Este tipo de escuchas no autorizadas se le conoce como *eavesdropping*. Existen muchos casos en los que Alice y Bob preferirían comunicarse sin ser escuchados.

Diagrama inseguro

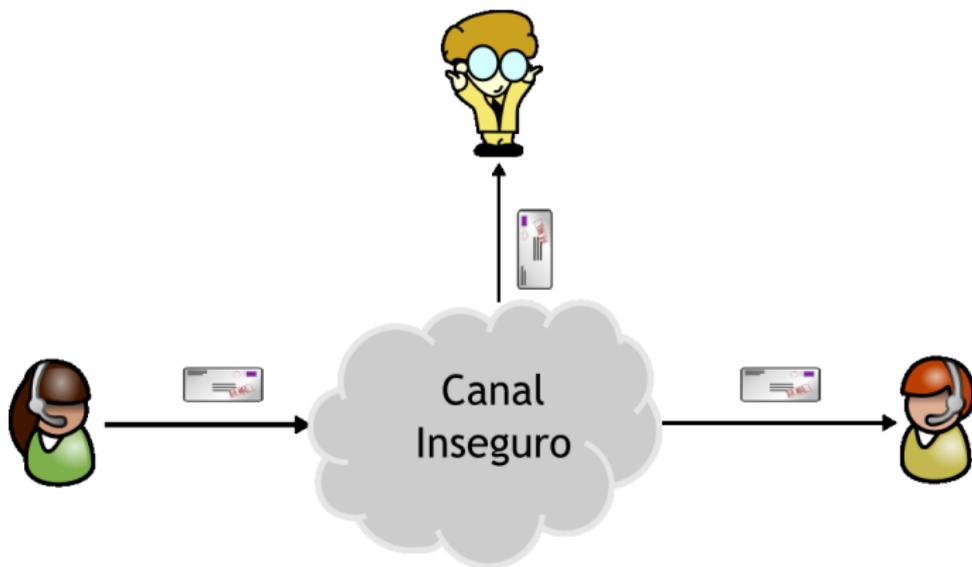
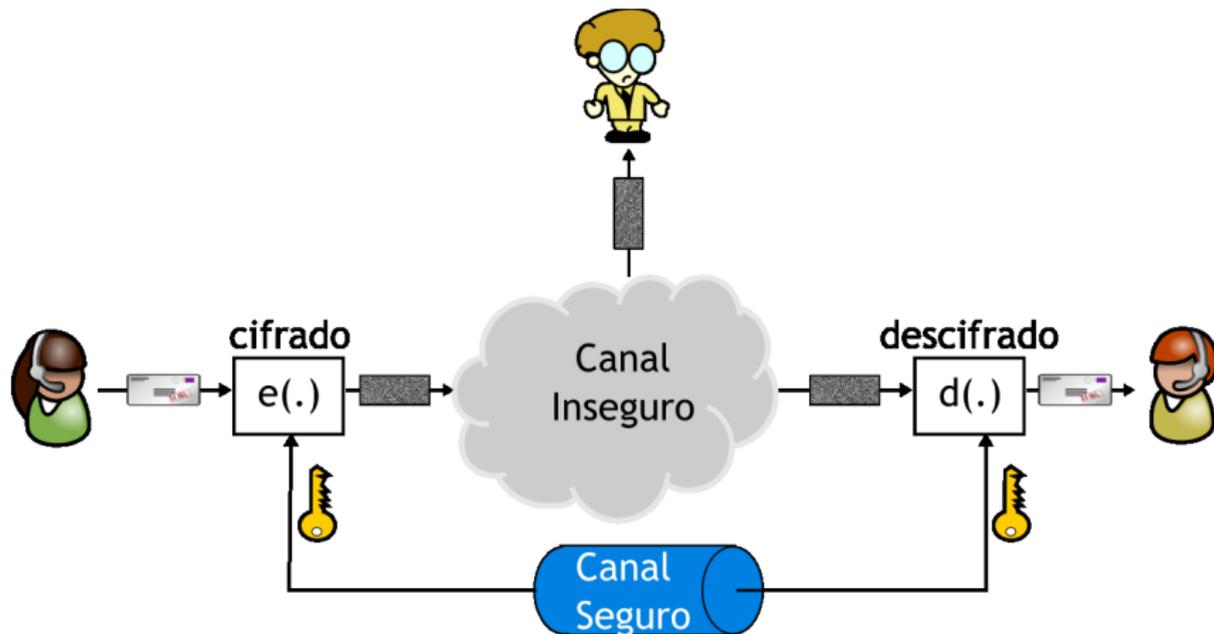


Diagrama con protección



Principio de Kerckhoff

En 1883 Augusto Kerckhoff escribió dos artículos en la revista La Cryptographie Militaire, en donde establecía seis principios de diseño para los cifradores militares:

- El sistema debe de ser prácticamente, si no es que matemáticamente, indescifrable.
- No debe de ser un requerimiento el que sea secreto, y debe de ser posible que caiga en manos del enemigo sin resultar ser un inconveniente.
- Sus claves deben de ser comunicables y retenibles sin la ayuda de notas escritas, y canjeables o modificables a discreción de los corresponsales.
- ...

Principio de Kerckhoff 2

- ...
- Debe de ser aplicable a la correspondencia telegráfica.
- Debe de ser portable, y su uso y funcionamiento no debe de requerir la presencia de varias personas.
- Finalmente, es necesario que, dadas las circunstancias que requieran su aplicación, que el sistema sea fácil de usar, no requiriendo esfuerzo mental ni el conocimiento previo de una larga serie de reglas que seguir.

Dado el poder computacional actual, algunos ya no son relevantes, sin embargo, el segundo axioma es vital y se conoce como el Principio de Kerckhoff

Contenido, sección 2

Criptología: criptografía y criptoanálisis

Cifradores históricos

Ataques

Enigma

Cifradores contemporáneos

Introducción

Cifradores de Flujo

Cifradores de Bloque

Numeros Aleatorios

DES

Modos de operación

AES

Criptografía Pública

Cifrador por sustitución

También conocido como cifrador por reemplazo, es uno de los métodos más simples para cifrar un texto.

La idea es sustituir cada letra del alfabeto por otra (o la misma), de tal manera que el texto no pueda entenderse a simple vista:

Ejemplo:

$$A \rightarrow L$$
$$B \rightarrow C$$
$$C \rightarrow J$$
$$\vdots$$

BABA = CLCL

Ataques al cifrador por sustitución

- Fuerza bruta, búsqueda exhaustiva.

El atacante tiene el texto cifrado gracias a que escuchó la conversación; además tiene una parte del texto original, por ejemplo: la cabecera del mensaje (i.e. `%PDF-1.4, PK, GIF87a, 0xFFD8`)

Ahora solo tiene que probar atacar el inicio del texto con todas claves posibles hasta que coincida.

Ataque por fuerza bruta

Formalmente,

Búsqueda exhaustiva básica de clave o ataque de fuerza bruta

Dada una pareja (x, y) , el texto en claro y el texto cifrado, y sea $K = \{k_0, \dots, k_{n-1}\}$ sea el espacio de todas las posibles claves. Un ataque de fuerza bruta verifica a todo $k_i \in K$ si:

$$d_{k_i}(y) \stackrel{?}{=} x,$$

Si la relación lógica se mantiene, entonces se ha encontrado la clave y se detiene el proceso, de otro modo, se continua.

$d(\cdot)$ es la función de descifrado. En la práctica depende del protocolo.

Ataques por fuerza bruta

En principio, todos los cifradores *simétricos* son susceptibles a ataques por fuerza bruta. Que sea factible o no, depende del espacio de la clave (el número de posibles claves).

Por ejemplo, el NIP de las tarjetas es de 4 dígitos, existen 10^4 posibles NIPs. En este caso, robar dinero de un cajero automático tardaría nada si no fuera porque los bancos bloquean las tarjetas ante ataques.

Ataques por fuerza bruta

En cambio, si al realizar un ataque utilizando alguna computadora moderna toma mucho tiempo (i.e. décadas), se dice que el cifrador es *computacionalmente seguro* ante ataques de fuerza bruta.

En el caso del cifrador por sustitución, la letra A se sustituyó por la letra L , pero teníamos 26 opciones. La letra B se sustituyó por la letra C , de las 25 opciones restantes. Y así sucesivamente.

El número de posibles sustituciones en un ataque por fuerza bruta es:

Ataques por fuerza bruta

En cambio, si al realizar un ataque utilizando alguna computadora moderna toma mucho tiempo (i.e. décadas), se dice que el cifrador es *computacionalmente seguro* ante ataques de fuerza bruta.

En el caso del cifrador por sustitución, la letra A se sustituyó por la letra L , pero teníamos 26 opciones. La letra B se sustituyó por la letra C , de las 25 opciones restantes. Y así sucesivamente.

El número de posibles sustituciones en un ataque por fuerza bruta es:

$$26 \cdot 25 \cdots 1 = 26! \approx 2^{88}.$$

¿Cuánto es 2^{88} ?

- Un procesador Intel Core i7 @3.4 GHz realiza alrededor de 2^{31} ciclos de reloj por segundo, aunque tiene 4 cores...



Ciclos de reloj

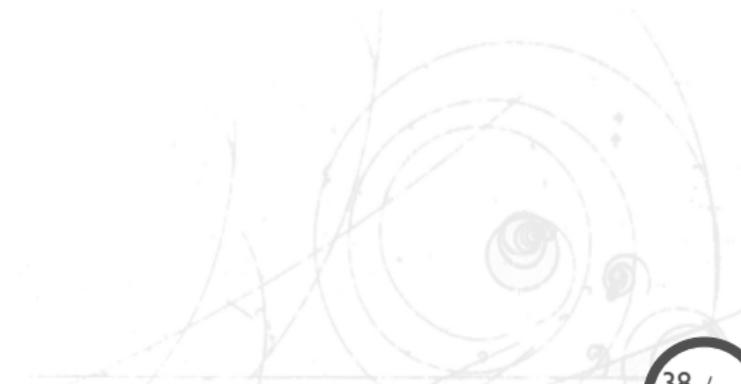
- Para realizar 2^{32} ciclos de reloj, se requieren el doble de cores que el nivel anterior (2^{31}), esto es, el procesador realiza 2^{33} ciclos de reloj en total.
- tenemos $88 - 32 = 55$, hay que duplicar la cantidad de cores 55 veces.
- Es un crecimiento geométrico, tal como la leyenda del Ambalappuzha Paal Payasam (granos de arroz y el ajedrez)

Ciclos de reloj

- Para realizar 2^{32} ciclos de reloj, se requieren el doble de cores que el nivel anterior (2^{31}), esto es, el procesador realiza 2^{33} ciclos de reloj en total.
- tenemos $88 - 32 = 55$, hay que duplicar la cantidad de cores 55 veces.
- Es un crecimiento geométrico, tal como la leyenda del Ambalappuzha Paal Payasam (granos de arroz y el ajedrez)



- Sin embargo, eso es sólo 1 segundo. . .



- Sin embargo, eso es sólo 1 segundo. . . además de que en algunos casos hay que analizar la información.

Para fines de benchmarking, normalmente no se utiliza el TurboBoost, además que en un ataque aumentaría la radiación térmica.

Entonces se dice que este esquema es seguro ante ataques de fuerza bruta...

- Sin embargo, eso es sólo 1 segundo. . . además de que en algunos casos hay que analizar la información.

Para fines de benchmarking, normalmente no se utiliza el TurboBoost, además que en un ataque aumentaría la radiación térmica.

Entonces se dice que este esquema es seguro ante ataques de fuerza bruta... (a menos que el *bruto* haya sido el que seleccionó la clave)

Un ataque *diferente*

En el ataque por fuerza bruta, tomamos al cifrador como una caja negra, sin analizarla internamente.

El cifrador por sustitución puede romperse mediante un ataque analítico.

La principal debilidad del cifrador, es que cada símbolo del texto en claro tiene una única representación en el texto cifrado. Esto es, que las propiedades estadísticas del texto en claro se preservan en el texto cifrado.

Letras en los idiomas

La letra que más se repite en el idioma inglés es la letra “e” (alrededor del 13% de los textos), después la “t” con un 9%, y la “a” con un 8%.

En español, la frecuencia es similar (la “e” también es la más utilizada). Se puede construir una tabla para el idioma español tomando cualquier libro y contando la ocurrencia de cada una de las letras.

Letras en los idiomas

La letra que más se repite en el idioma inglés es la letra “e” (alrededor del 13% de los textos), después la “t” con un 9%, y la “a” con un 8%.

En español, la frecuencia es similar (la “e” también es la más utilizada). Se puede construir una tabla para el idioma español tomando cualquier libro y contando la ocurrencia de cada una de las letras.

Pero aquí están ordenadas de mayor a menor frecuencia: E A O S
R N I D L C T U M P B G V Y Q H F Z J Ñ X W K

Notas sobre el conteo de letras

- En un diccionario, la letra que más se repite tiende a ser la “a”
- En un libro, como en el Quijote, se mantiene el orden antes mencionado.
- Aunque hay excepciones.
- además, existen muchas frases cortas en el español que van con la “e”: qué, le, sé, etc.

Finalmente, con la estadística es muy fácil descifrar un texto por sustitución.

Cifrado de Cæsar

El cifrador de César es un tipo especial del cifrador por sustitución en el cual los valores del alfabeto se rotaban una cantidad de letras en particular.

Por ejemplo, si la clave era 13, entonces la tabla de sustitución es:

$$A \rightarrow N$$
$$B \rightarrow \tilde{N}$$
$$C \rightarrow O$$
$$\vdots$$

Para el idioma español.

Cifrado de Cæsar

El cifrador de César es un tipo especial del cifrador por sustitución en el cual los valores del alfabeto se rotaban una cantidad de letras en particular.

Por ejemplo, si la clave era 13, entonces la tabla de sustitución es:

$$A \rightarrow N$$
$$B \rightarrow \tilde{N}$$
$$C \rightarrow O$$
$$\vdots$$

Para el idioma español.

¿Cuál es el espacio de claves?

Máquina enigma

La máquina enigma era una especie de máquina de escribir con un determinado número de rotores en serie que giraban de diferente forma a cada pulsación de una tecla, de tal manera que la salida de un rotor era la entrada para el siguiente, y así sucesivamente.

Estos rotores podían cambiar su posición inicial (que era la clave), de tal manera que cada vez que se enviaba un mensaje, se utilizaba una configuración diferente.

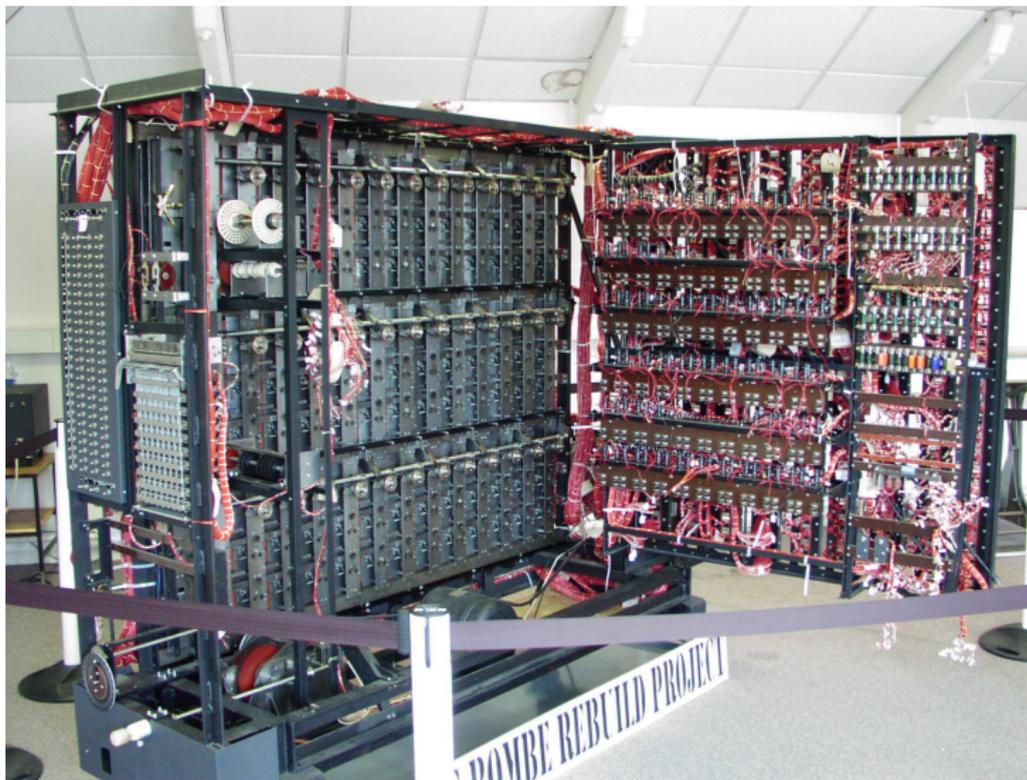
Segunda Guerra Mundial

Durante el Franquismo, los nazis proveyeron a Francisco Franco de unas máquinas limitadas para comunicarse, y probarlas.

Ya probadas, se utilizaron extensamente durante la Segunda Guerra mundial para enviar instrucciones a las líneas de batalla.

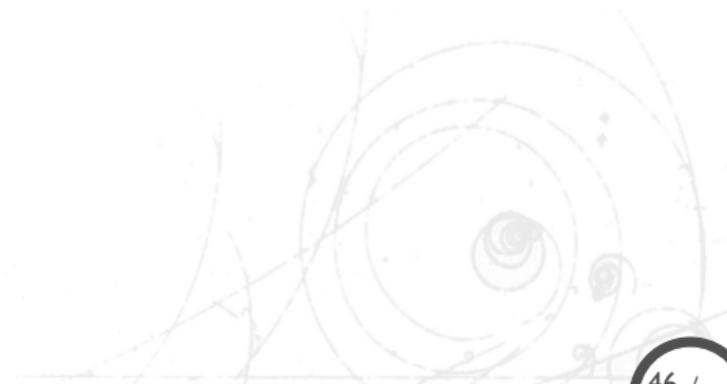
Todos los ataques alemanes eran sorpresa y 100% efectivos. Fue hasta que los británicos con su laboratorio en Bletchley Park (liderado por Alan Turín), y las máquinas polacas *bombe*, que pudieron descifrar los mensajes, y salvar millones de vidas.

Bombes polacas



Simulador máquina enigma

En línea



Contenido, sección 3

Criptología: criptografía y criptoanálisis

Cifradores históricos

Ataques

Enigma

Cifradores contemporáneos

Introducción

Cifradores de Flujo

Cifradores de Bloque

Numeros Aleatorios

DES

Modos de operación

AES

Criptografía Pública

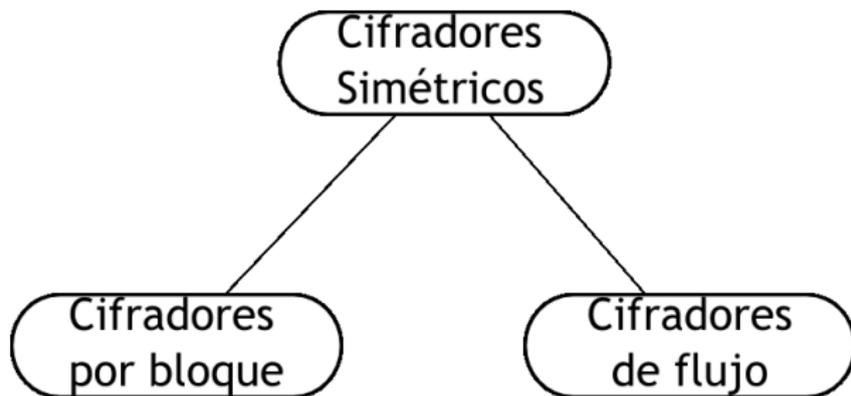
Criptosistema

Un *criptosistema* es una 5-tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, con las siguientes condiciones:

- \mathcal{P} es el conjunto finito de todos los textos en claro posibles
- \mathcal{C} es el conjunto finito de todos los textos cifrados posibles
- \mathcal{K} , el *espacio de claves*, es el conjunto finito de todas las *claves* posibles
- $\forall K \in \mathcal{K}, \exists E_K \in \mathcal{E}$ (regla de cifrado), $\exists D_K \in \mathcal{D}$ (regla de descifrado)

Cada $E_K : \mathcal{P} \rightarrow \mathcal{C}$, $D_K : \mathcal{C} \rightarrow \mathcal{P}$, son funciones tal que $\forall x \in \mathcal{P}$, $D_K(E_K(x)) = x$.

Tipos de cifradores simétricos



Cifradores simétricos

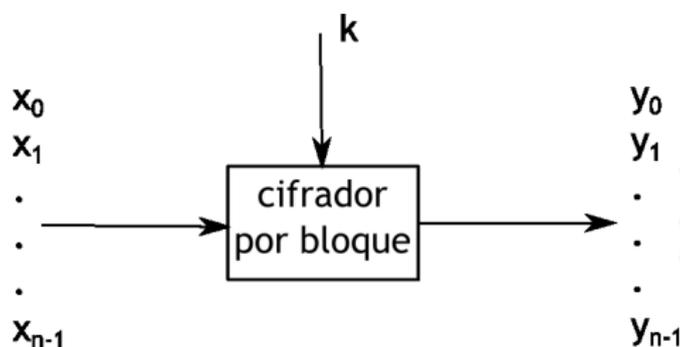
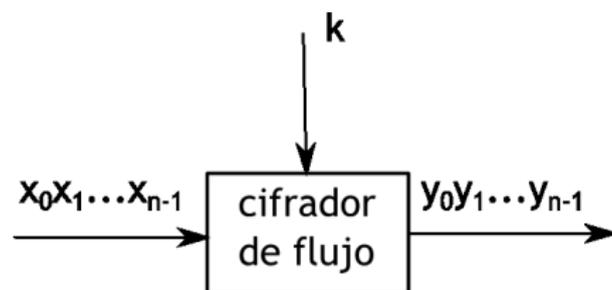
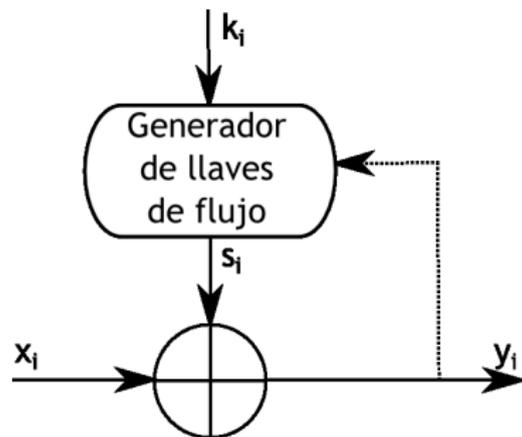


Diagrama cifradores de flujo



Cifradores de flujo.

Cifran bits individualmente. Esto se hace al añadir un bit de un flujo de la llave a un bit del texto en claro.

Los esquemas *síncronos* son en los que la línea punteada en el diagrama no está presente (el cifrado depende exclusivamente de la llave). Son *asíncronos*, cuando existe la dependencia del bit cifrado con los bits cifrados anteriormente (la línea punteada está activa).

Operación

Cifrado y Descifrado de flujo

El texto en claro, el texto cifrado, y el flujo de la llave consiste en bits individuales: $x_i, y_i, s_i \in \{0, 1\}$

- Cifrado: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \pmod{2}$
- Descifrado: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \pmod{2}$



Nota: La suma módulo 2 equivale a la operación xor.

Cifradores de Bloque

Cifradores de bloque.

Cifran un bloque completo de bits del texto en claro a la vez con la misma llave. Esto significa que el cifrado de cualquier bit del texto en claro en un bloque dado depende de los otros bits del bloque. En la práctica, la mayoría de los cifradores de bloque esperan bloques de 128 bits (AES), o 64 bits (DES).

Números aleatorios

Generadores de números verdaderamente aleatorios.



- Los generadores de números realmente aleatorios (TRNGs) se caracterizan por el hecho de que su salida no puede ser reproducida. Por ejemplo, si echamos 100 volados y registramos los resultados como una secuencia de bits, dicha secuencia es virtualmente irrepetible (la probabilidad de repetirla es de $1/2^{100}$).
- Los TRNGs están basados en procesos físicos.

Número pseudo-aleatorios

Generadores de números pseudo-aleatorios.

- Los generadores de números pseudo-aleatorios (PRNGs) generan secuencias que pueden ser calculadas a partir de un valor inicial llamado semilla (seed).

Por ejemplo, la función `rand(.)` del ANSI C es algo así:

$$s_0 = 12345$$

$$s_{i+1} \equiv 1103515245 \cdot s_i + 12345 \pmod{2^{31}}, i = 0, 1, \dots$$

Generadores de números pseudo-aleatorios criptográficamente seguros

Un **generador de números pseudo-aleatorios criptográficamente seguros** (CSPRNGs) es un tipo especial de generador que es impredecible. Dada una secuencia de bits, no existe un algoritmo polinomial que determine el siguiente bit con una probabilidad mayor al 50%. Igualmente, dada una secuencia de bits, es imposible determinar el anterior.

La impredecibilidad de los CSPRNGs es única para la criptografía, por lo que si se toma un generador no diseñado específicamente para criptografía, probablemente no sirva para un producto comercial.

Incondicionalmente seguro

Incondicionalmente seguro.

Un criptosistema es incondicionalmente seguro (o seguro en términos de la teoría de la información) si no puede ser roto aún con recursos informáticos infinitos.

Suponga un criptosistema simétrico con una llave de 10,000 bits que solo pueda ser roto mediante búsqueda exhaustiva (fuerza bruta). Se necesitarían $2^{10,000}$ computadoras. El sistema no es incondicionalmente seguro, pero es computacionalmente seguro (se estima que existen entre 2^{239} y 2^{289} átomos en el universo)

One-time pad

Aquí está un criptosistema incondicionalmente seguro:

One-time pad

Es un cifrador de flujo en el cual:

- el flujo de la llave s_0, s_1, \dots es generador por un TRNGs
- el flujo de la llave es solamente conocido por los extremos de la comunicación
- cada bit del flujo de la llave s_i es utilizado una única vez.

se le conoce como one-time pad. El one-time pad es incondicionalmente seguro.

Más sobre el one-time pad.

Cada bit del texto cifrado se forma de la siguiente manera:

$$y_0 \equiv x_0 + s_0 \pmod{2}$$

$$y_1 \equiv x_1 + s_1 \pmod{2}$$

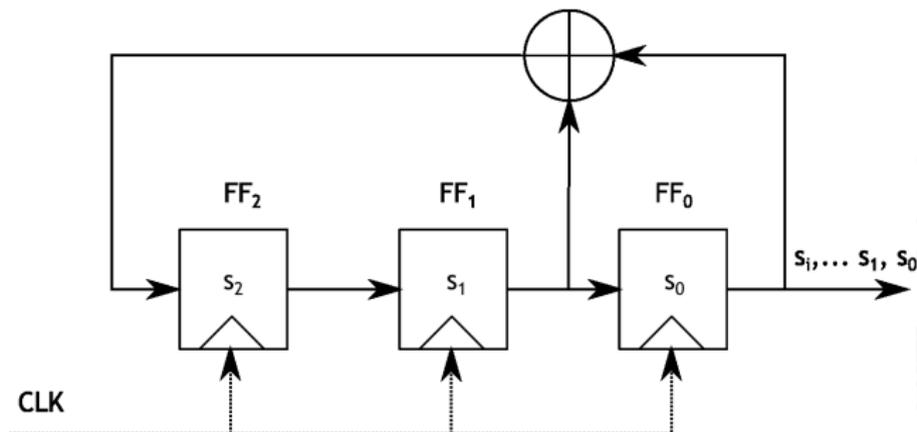
⋮

$$y_{n-1} \equiv x_{n-1} + s_{n-1} \pmod{2}$$

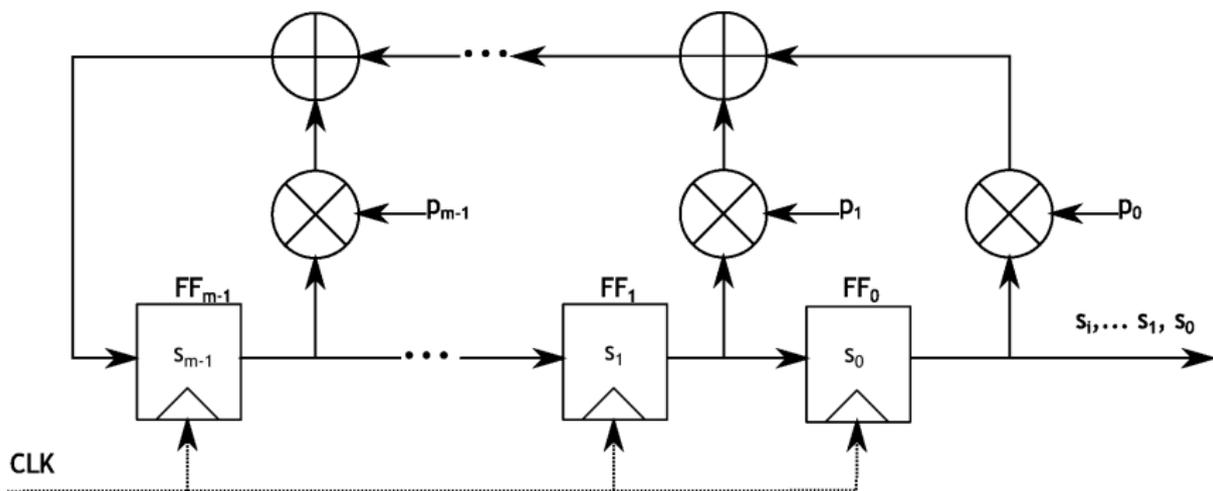
es una ecuación con dos incógnitas por cada bit. Aún si se conoce y_i , los valores de $x_i \in \{0, 1\}$ tienen exactamente la misma probabilidad si se utilizó un TRNG. Sin embargo, los bits aleatorios no se pueden reutilizar, lo que nos lleva al problema de distribución de claves.

Linear Feedback Shift Register

Un **LFSR** consiste en elementos de almacenamiento sincronizados (flip-flops) y una ruta de retroalimentación. El número de elementos de almacenamiento establece el grado del LFSR. La red de retroalimentación calcula la entrada del último flip-flop como una suma módulo 2 (XOR) de ciertos flip-flops en el registro.

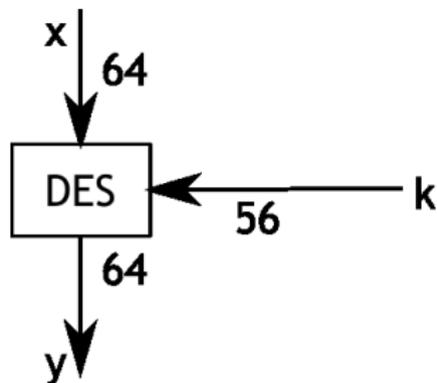


LFSR

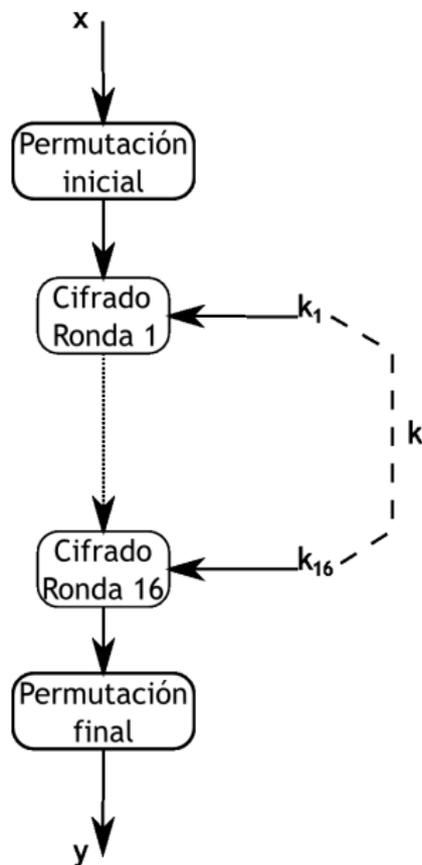


DES caja negra

El DES es un cifrador que toma bloques de 64-bits de longitud con una llave de 56-bits.



DES estructura general



Ataques

- 1977 - Diffie y Hellman sugirieron un diseño de un chip VLSI que puede probar 10^6 llaves/seg. Un equipo con 10^6 de estos circuitos podría romper la clave en cuestión de 10 horas.
Costo: USD \$20'000,000.00
- 1990 - Eli Biham y Adi Shamir sugirieron un criptoanálisis diferencial
- 1993 - Mitsuru Masui sugirió un criptoanálisis lineal

Modos de operación

Hemos dicho que DES trabaja con bloques de 64-bits, ¿qué pasa si requerimos cifrar más de 64 bits? Agarramos de 64 bits en 64 bits?

Modos de operación

Hemos dicho que DES trabaja con bloques de 64-bits, ¿qué pasa si requerimos cifrar más de 64 bits? Agarramos de 64 bits en 64 bits? (no)

Modos de bloques

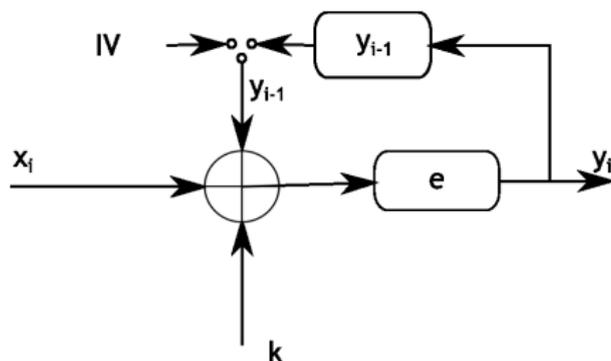
- ECB - Electronic Codebook Block
- CBC - Cipher Block Chaining

Modos de flujo

- CFB - Cipher Feedback
- OFB - Output Feedback

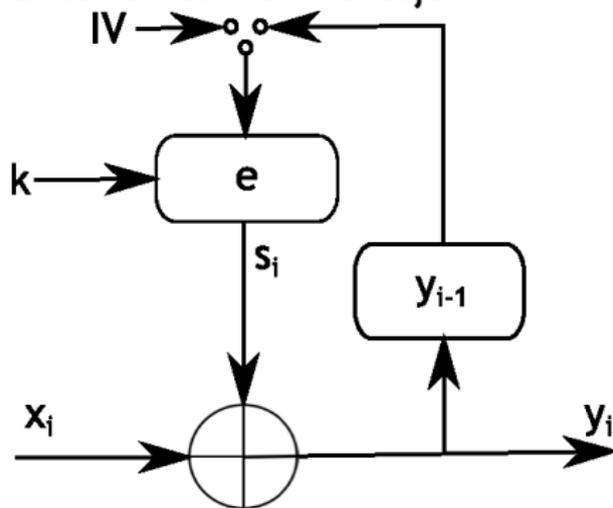
Por bloques

- ECB - El mensaje se rompe en bloques de 64-bits (se rellena con ceros).
- CBC - Hace un xor de la salida anterior con el bloque a cifrar (requiere vector de inicialización).

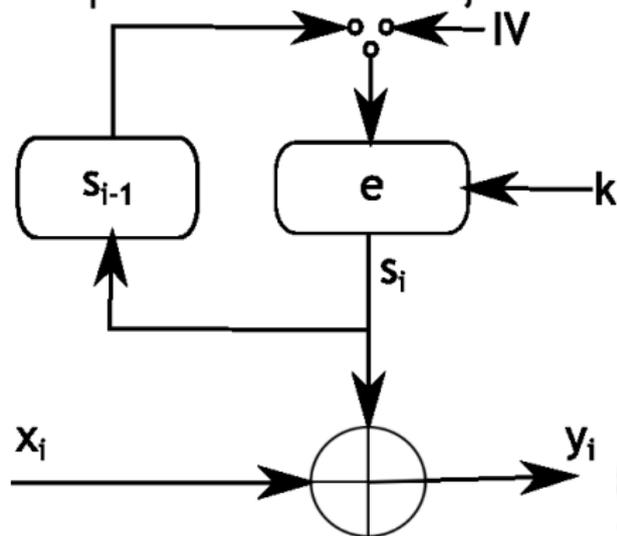


Por flujo

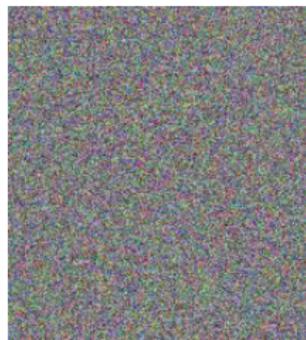
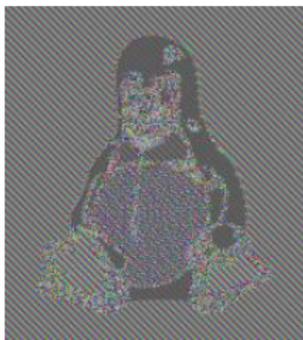
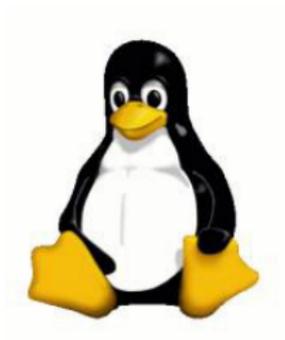
CFB - Se hace un xor de la salida anterior con el mensaje anterior



OFB - El feedback es independiente del mensaje actual



Comparativa

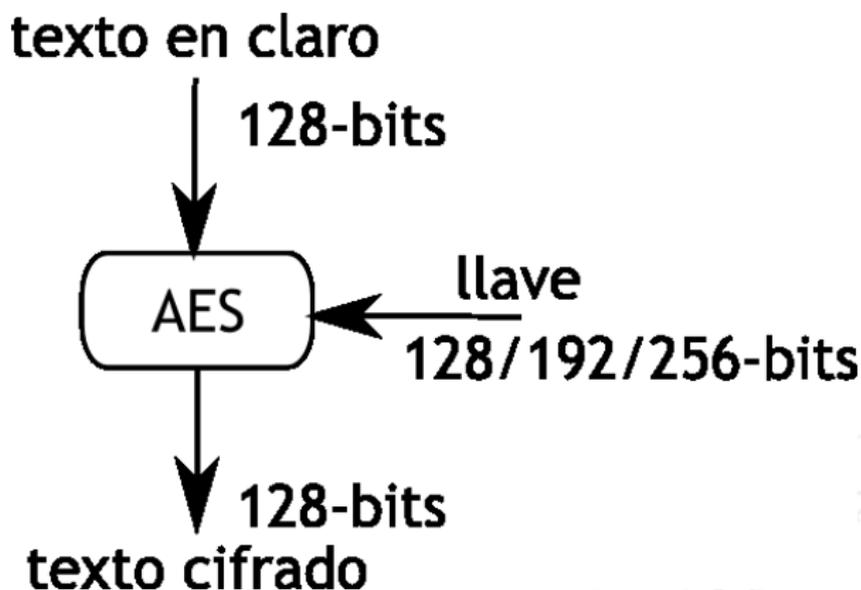


AES - Advanced Encryption Standard

¿Porqué un estándar nuevo?

- Ataques de fuerza bruta
- La solución (Triple DES) lo hace el triple de lento
- DES es eficiente solo para hardware
- Nuevos tipos de ataques
- Utilizar bloques de 64-bits no es útil para todos los escenarios

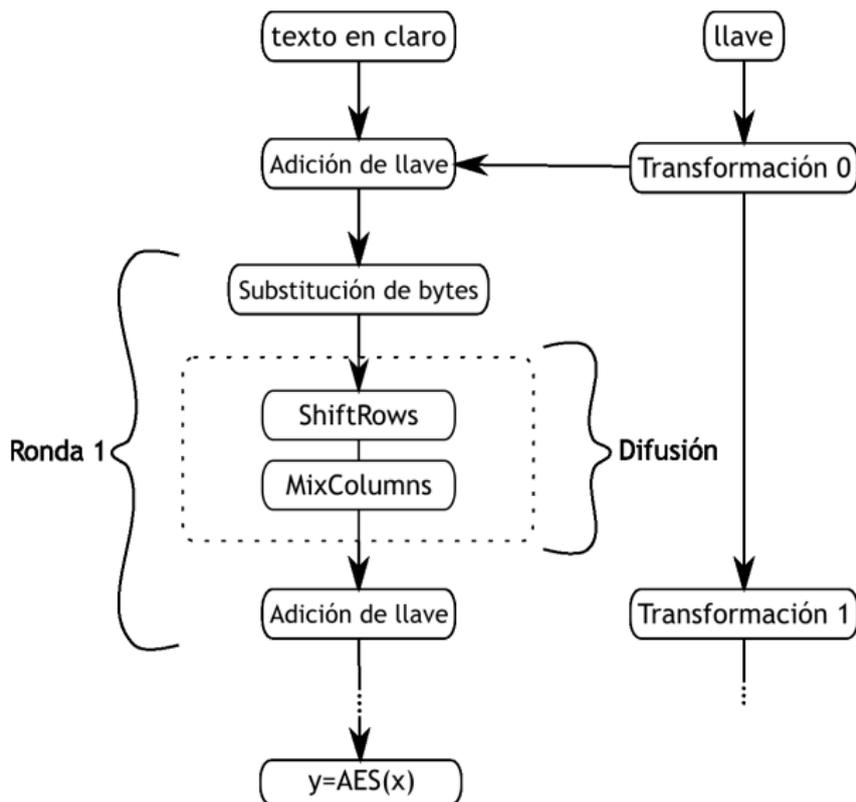
AES - Caja negra



AES - descripción

- AES no utiliza una función Feistel, se desea cifrar todo un bloque por ronda
- Se necesitan 10, 12 o 14 rondas para cifrar con claves de 128, 192 o 256 bits
- En cada ronda hay 3 capas: Adición de llave, de Sustitución de bytes, y de difusión
- la capa de difusión se subdivide en: ShiftRow, que permuta datos a nivel de byte; y MixColumn, que mezcla bloques de 4-bytes dentro de una matriz

AES - rondas



El nacimiento de la criptografía de llave pública

- En 1976, Whitfield Diffie y Martin Hellman publicaron su famoso artículo: “Nuevas direcciones en criptografía” (New Directions in Cryptography)
- Poco antes, Ralph Merkle inventó una construcción de llave pública para sus clases. Su trabajo se tituló: “Comunicación segura sobre canales inseguros” en 1982 (Secure communication over insecure channels)

El nacimiento de la criptografía de llave pública

- El concepto fue originalmente descubierto por James Ellis, aunque se mantuvo en secreto ya que era información clasificada de la GCHQ de 1969 a 1997.
- Adicionalmente, Malcolm Williamson y Clifford Cocks de la GCHQ, descubrieron el intercambio de llave Diffie-Hellman, y el cifrado RSA.

El nacimiento

- Antes de la publicación de “New Directions. . .”, la investigación sobre cifrado en los E.E.U.U. era dominio de la Agencia Nacional de Seguridad (NSA).
- Hasta mediados de 1990’s, la exportación de algoritmos criptográficos era penada con traición.
- Después, solamente prohibía la exportación de algoritmos de seguridad alta si eran leíbles por máquinas (código fuente, ejecutables, etc.).

Curiosidades

- Los algoritmos criptográficos se convirtieron en “municiones” para el gobierno
- La gente se hacía playeras con código RSA amenazando con salir del país
- Hubo quien incluso se hizo tatuajes

Curiosidades

- Los algoritmos critográficos se convirtieron en “municiones” para el gobierno
- La gente se hacía playeras con código RSA amenazando con salir del país
- Hubo quien incluso se hizo tatuajes

- Las penas por viajar de los E.E.U.U. a Europa de esta manera llegaban a los 10 años de prisión.
- Ahora es posible comprar implementaciones seguras

Criptografía Pública

- El término Criptografía de Clave Pública (o criptografía pública) es intercambiable con el de Criptografía Asimétrica, denotan lo mismo, y son sinónimos.
- Aunque fue hecha pública en 1976 por Diffie, Hellman, and Merkel, en 1997 se desclasificaron documentos británicos de 1972, en donde James Ellis, Clifford Cocks and Graham Williamson del Government Communications Headquarters (GCHQ, Reino Unido), descubrieron la criptografía pública.

Criptografía simétrica vs. asimétrica

Simétrica



- La misma llave secreta se utiliza para cifrar y descifrar
- La función de cifrado y descifrado son muy parecidas, la misma en algunos casos
- Distribución de llaves
- Número de llaves
- Colusión

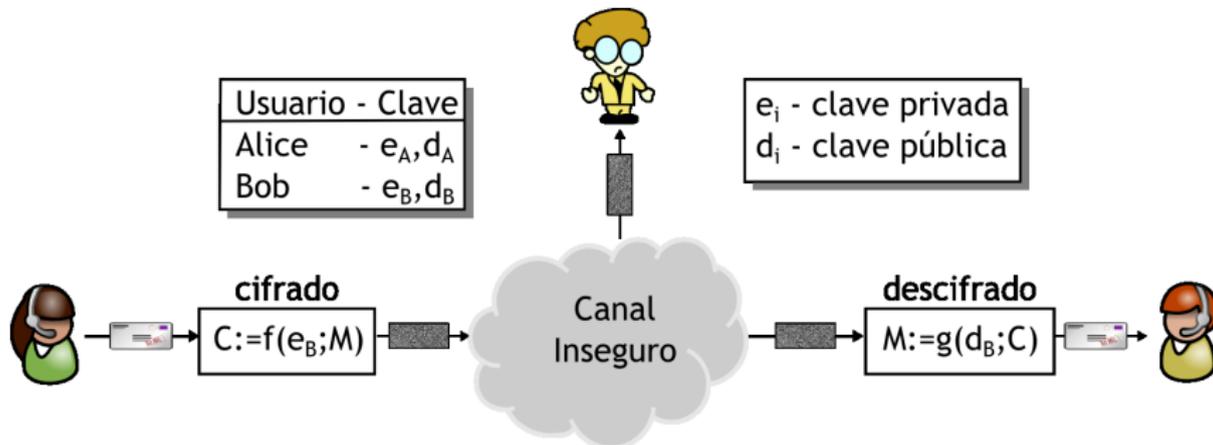
Criptografía simétrica vs. asimétrica

Asimétrica



- Sólo se publica la parte pública de la llave, cada quien la baja sobredemanda
- Que haya muchas claves es irrelevante
- Se puede proteger de la colusión
- Ahora se tiene un par de llaves: pública y privada
- La función de cifrado y descifrado son diferentes
- En algunos protocolos hay que intercambiar llaves

Esquema General de la Criptografía Pública



Usos de la criptografía de clave pública

Además de cifrar datos, la criptografía de clave pública puede utilizarse en lo siguiente:

- **Establecimiento de llaves.** Existen protocolos para la compartición de claves secretas sobre medios inseguros (para utilizar criptografía simétrica).
- **No repudiación.** Proveen no repudiación e integridad de mensajes mediante firmas digitales: RSA, DSA, ECDSA
- **Identificación.** Mediante mecanismos de desafío-respuesta junto con firmas digitales: para smart cards y teléfonos móviles.
- **Cifrado.**

El único pendiente es la autenticación de las claves públicas; para esto, se utilizan los certificados digitales.

Algoritmos relevantes

Los tres tipos relevantes en la criptografía de clave pública son:

- **Esquemas de factorización de enteros.** Basados en la dificultad de factorizar números enteros grandes
- **Esquemas de Logaritmos Discretos.** Basados en la dificultad del problema del logaritmo discreto sobre campos finitos
- **Esquemas de Curvas Elípticas.** Generalización del problema anterior a esquemas basados en curvas elípticas

Nivel de seguridad

Dado que los ataques a los sistemas criptográficos son más eficientes en los esquemas asimétricos, se define como nivel de seguridad equivalente: el número de bits en un criptosistema asimétrico que equivalen en resistencia a uno simétrico.

Esto es: esto es, si rompemos una clave simétrica de 80 bits en 1 segundo con 2^{80} computadoras, ¿cuántos bits debe de tener una clave asimétrica para que son 2^{80} computadoras también nos tardemos 1 segundo?

Niveles de seguridad

| Familia | Criptosistema | Nivel de seguridad | | |
|----------------------|------------------|--------------------|----------|-----------|
| | | 128 | 192 | 256 |
| Factorización entera | RSA | 3072 bit | 7680 bit | 15360 bit |
| Logaritmo discreto | DH, DSA, Elgamal | 3072 bit | 7680 bit | 15360 bit |
| Curvas elípticas | ECDH, ECDSA | 256 bit | 384 bit | 512 bit |
| Clave simétrica | | 128 bit | 192 bit | 256 bit |