Criptografía simétrica

Seguridad y ataques

Isaac A. Canales Martínez

Octubre 1, 2023

Contenido

- Seguridad de esquemas de cifrado
- Ataques a esquema de cifrado
  - Búsqueda exhaustiva
  - Criptoanálisis algebraico
  - Criptoanálisis lineal
  - Criptoanálisis diferencial
  - Ataque de canal lateral

Seguridad de esquemas de cifrado

Seguridad de un sistema criptográfico

- Seguridad se define con base en
  - Objetivo del adversario
  - Capacidades del adversario
- Sistema criptográfico no seguro: adversario logra su objetivo dadas sus capacidades
- Si no es el caso, el sistema *se puede considerar* seguro

Seguridad de un sistema criptográfico

- La seguridad de un sistema criptográfico no debe depender de mantener su diseño en secreto, sino solo en mantener la llave en secreto (Kerckhoffs)
- Suponemos que el adversario tiene completo conocimiento del sistema

Seguridad de esquemas de cifrado

Objetivo del adversario

- Obtener la llave

- Recuperar el mensaje

vs `x2aj&0@r4`

- Distinguir entre texto cifrado o información aleatoria

Seguridad de esquemas de cifrado

Capacidades del adversario

- Tiempo de cómputo
- Información disponible
  - Textos cifrados
  - Textos cifrados y mensajes correspondientes
  - Mensajes escogidos por el adversario y textos cifrados correspondientes
  - Mensajes y textos cifrados escogidos por el adversario

Secreto perfecto

- Un esquema de cifrado es perfectamente secreto si el texto cifrado no proporciona absolutamente ninguna información acerca del mensaje
- Formalmente, para todos los mensajes p, p' y textos cifrados c

$$\Pr[E(k,p) = c] = \Pr[E(k,p') = c]$$

- Ejemplo: One-time pad

Secreto perfecto

- Matemáticamente estos esquemas son *irrompibles* (*i. e.*, seguros)
  - Incluso si el adversario tiene capacidad computacional ilimitada
- Secreto perfecto implica que la llave tenga al menos la misma longitud que el mensaje y que se use una sola vez

Seguridad computacional

- En práctica, un esquema de cifrado se puede considerar seguro si
  - el texto cifrado proporciona muy poca información del mensaje, y
  - el adversario tiene límite en su poder de cómputo
- Un esquema de cifrado es computacionalmente seguro si el adversario logra su objetivo dado su límite de cómputo con probabilidad despreciable
- Esta es la manera común de definir seguridad

Seguridad en la práctica

- Las nociones de seguridad anteriores no necesariamente implican seguridad en práctica
- Implementaciones pueden introducir vulnerabilidades

Criptología

Criptografía

Criptoanálisis

Ataques a sistemas criptográficos

- Detectar vulnerabilidades en los diseños
- Proponer sistemas no vulnerables a ataques conocidos
- Eliminar puntos vulnerables en sistemas existentes

Ataques a esquemas de cifrado

Algunas técnicas

- Búsqueda exhaustiva (o fuerza bruta)
- Criptoanálisis algebraico
- Criptoanálisis lineal
- Criptoanálisis diferencial
- Ataque de canal lateral

Búsqueda exhaustiva

Búsqueda exhaustiva

- Objetivo: 
- Idea: probar todas las posibilidades hasta encontrar la correcta

Búsqueda exhaustiva

Ejemplo:

- AES con llave de 128 bits
- Possibles llaves: $2^{128} = 340282366920938463463374607431768211456$
- Computadora a 4GHz (2^{32} ops. por segundo)
  - $2^{128}/2^{32}$ segundos = $79228162514264337593543950336 \approx 2.51 \times 10^{21}$ años
  - Edad del universo: 13.7×10^{9} años

Búsqueda exhaustiva

- Muy poco práctica
- Fácil de ejecutar en paralelo
- Búsqueda exhaustiva parcial:
  - Misma idea pero aplicada solamente a una parte

  - Utilizada en otras técnicas de criptoanálisis

Criptoanálisis algebraico

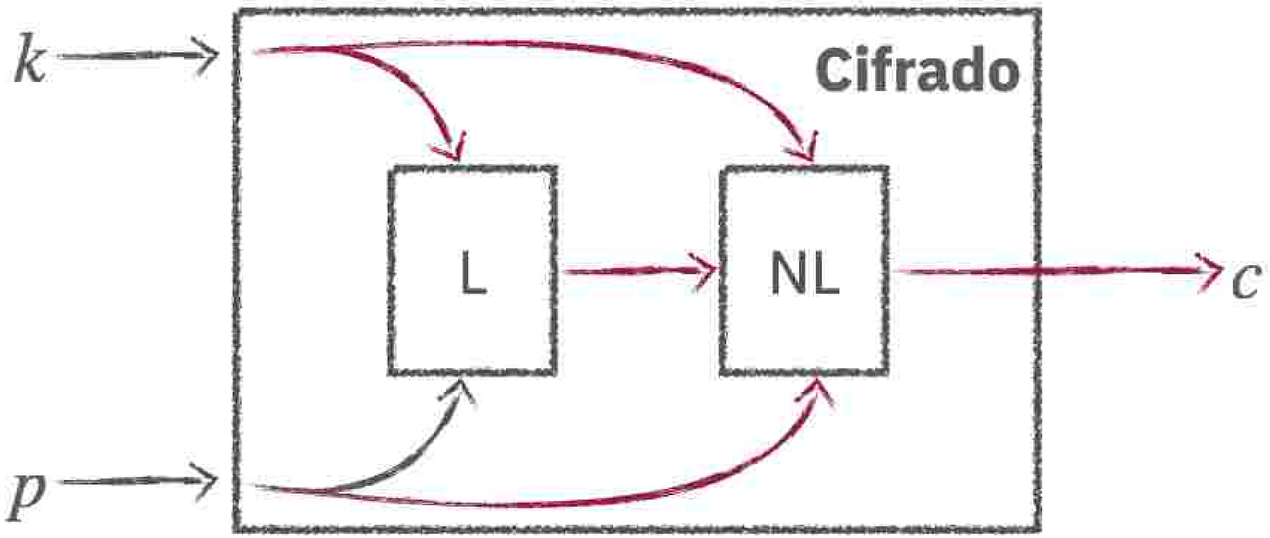
Ataques algebraicos

- Objetivo: 
- Idea: recuperar la llave resolviendo ecuaciones (no lineales) en términos de la llave, mensaje y texto cifrado

Ataques algebraicos

- Comprende dos fases:
  - Encontrar ecuaciones no lineales (grado bajo o con cierta estructura)
  - Resolver las ecuaciones y recuperar los bits de la llave

Ataques algebraicos



- $p_1 k_1 = c_1$
- $p_2 k_3 + p_1 p_3 = c_3$
- ...

Linealización

$$
\begin{aligned}
x_1 + x_2 x_3 &= 1 \\
x_1 x_2 + x_1 x_3 + x_1 &= 0 \\
x_2 x_3 + x_2 &= 0 \\
x_1 x_2 + x_1 + x_3 + x_2 &= 0 \\
x_1 + x_1 x_2 + x_3 &= 0 \\
x_2 x_3 + x_1 + x_2 &= 1
\end{aligned}
$$

$$\mathbf{A}$$

Linealización

$$
\begin{aligned}
x_1 + x_2x_3 &= 1 \\
x_1x_2 + x_1x_3 + x_1 &= 0 \\
x_2x_3 + x_2 &= 0 \\
x_1x_2 + x_1 + x_3 + x_2 &= 0 \\
x_1 + x_1x_2 + x_3 &= 0 \\
x_2x_3 + x_1 + x_2 &= 1
\end{aligned}
\quad \Longrightarrow \quad
\begin{aligned}
x_1 &= y_1 \\
x_2 &= y_2 \\
x_3 &= y_3 \\
x_1x_2 &= y_4 \\
x_1x_3 &= y_5 \\
x_2x_3 &= y_6
\end{aligned}
$$

A

Linealización

$$
\begin{aligned}
x_1 + x_2x_3 &= 1 \\
x_1x_2 + x_1x_3 + x_1 &= 0 \\
x_2x_3 + x_2 &= 0 \\
x_1x_2 + x_1 + x_3 + x_2 &= 0 \\
x_1 + x_1x_2 + x_3 &= 0 \\
x_2x_3 + x_1 + x_2 &= 1
\end{aligned}
$$

A

$\Rightarrow$

$$
\begin{aligned}
x_1 &= y_1 \\
x_2 &= y_2 \\
x_3 &= y_3 \\
x_1x_2 &= y_4 \\
x_1x_3 &= y_5 \\
x_2x_3 &= y_6
\end{aligned}
$$

$\Rightarrow$

$$
\begin{aligned}
y_1 + y_6 &= 1 \\
y_4 + y_5 + y_1 &= 0 \\
y_6 + y_2 &= 0 \\
y_4 + y_1 + y_3 + y_2 &= 0 \\
y_1 + y_4 + y_3 &= 0 \\
y_6 + y_1 + y_2 &= 1
\end{aligned}
$$

B

Linealización

- Aplicando eliminación de Gauss

$$
\begin{aligned}
y_1 &= 1 \\
y_2 &= 0 \\
y_3 &= y_5 \\
y_4 &= y_5 + 1 \\
y_5 &= * \\
y_6 &= 0
\end{aligned}
$$

Linealización

- Aplicando eliminación de Gauss

$$
\begin{aligned}
y_1 &= 1 \\
y_2 &= 0 \\
y_3 &= y_5 \\
y_4 &= y_5 + 1 \\
y_5 &= * \\
y_6 &= 0
\end{aligned}
$$

- Soluciones: $(1,0,0,1,0,0)$ y $(1,0,1,0,1,0)$.

Linealización

- Una solución es correcta y la otra no
- Linealización *destruye* información
- Solución para **A**, solución para **B**
- Solución para **B**, no siempre es una solución para **A**

Otras técnicas

- Basadas en bases de Gröbner
  - Análogo a eliminación de Gauss para ecuaciones no lineales
- Interpolación
- Higher order differential attack y cube attack

Criptoanálisis lineal

Criptoanálisis lineal

- Objetivo: 
- Idea: recuperar la llave resolviendo ecuaciones lineales en términos de la llave, mensaje y texto cifrado

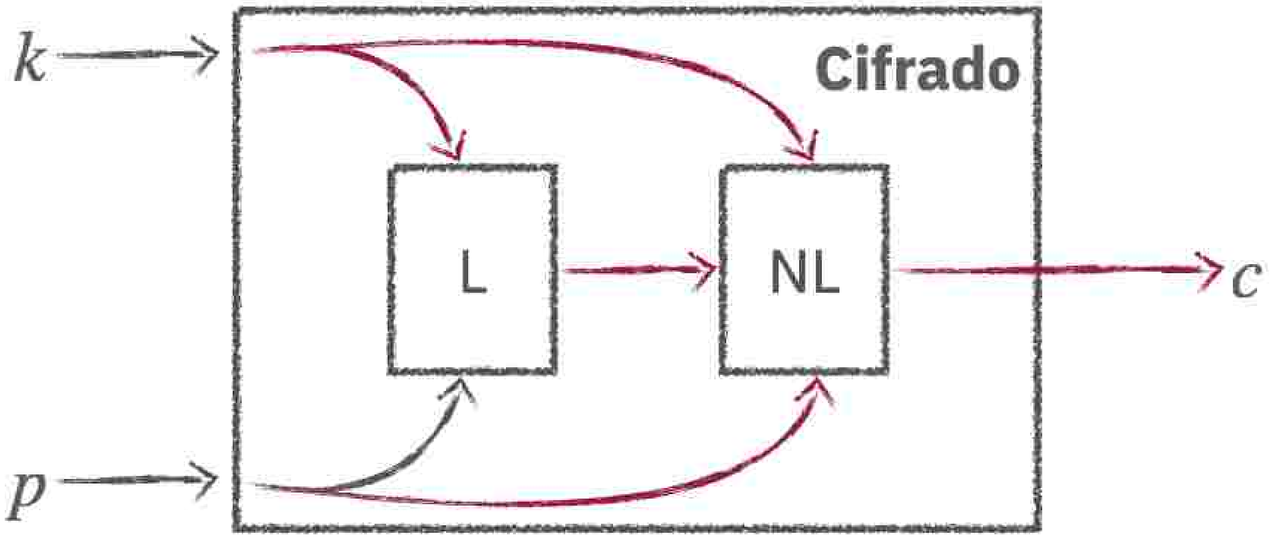
Criptoanálisis lineal

- Comprende dos fases:
  - Encontrar ecuaciones lineales
  - Recuperar los bits de la llave usando pares de mensajes y textos cifrados

Criptoanálisis lineal

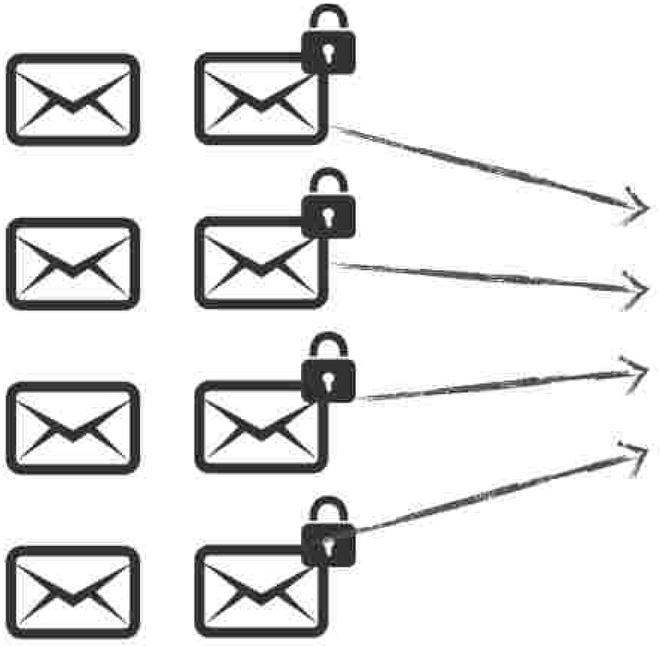
- Esquema de cifrado no es una operación lineal
- Las ecuaciones son satisfechas con cierta probabilidad
    - *Aproximaciones lineales* (con probabilidad > 0.5)

Criptoanálisis lineal



- $p_1 + c_2 \approx k_2 + k_3$
- $p_3 + c_4 + c1 \approx k_1 + k_2$
- ...

Criptoanálisis lineal



- $p_1 + c_2 \approx k_2 + k_3$
- $p_3 + c_4 + c1 \approx k_1 + k_2$
- $c_1 + p_2 + c3 \approx k_4$
- $p_2 + p_5 + c6 \approx k_1 + k_3$
- ...

Criptoanálisis lineal

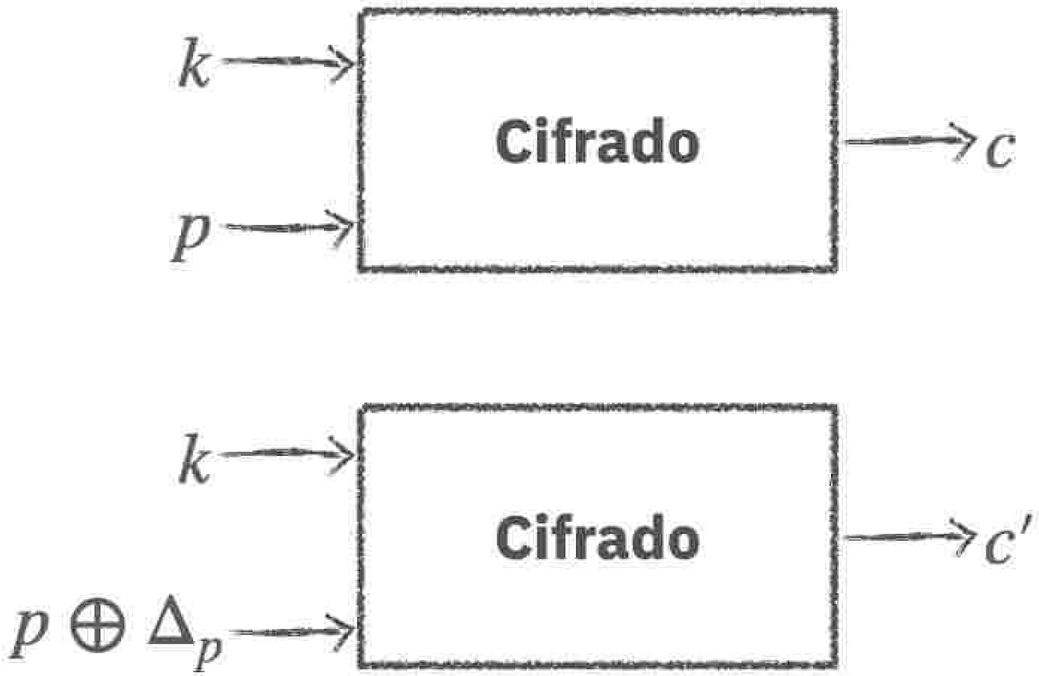
- *Llave parcial* se obtiene de las aproximaciones con mas valores ✅
- Para el resto de la llave
  - Repetir el proceso con otras aproximaciones
  - Búsqueda exhaustiva parcial

Criptoanálisis diferencial

Criptoanálisis diferencial

- Objetivo: 
- Idea: cifrar mensajes con diferencias conocidas y analizar estadísticamente las diferencias en los mensajes cifrados
- Principalmente, aplicable a cifradores por bloques

Criptoanálisis diferencial



$$\Delta_c = c \oplus c'$$

Criptoanálisis diferencial

- Se espera que ciertas Δ_c sean mas frecuentes
  - Distinguir el texto cifrado de bits aleatorios
- Posible obtener la llave utilizando un ataque para distinguir

Ataque de canal lateral

Ataque de canal lateral

- Ataque basado en información obtenida de la implementación
- Algunas clases
  - Sincronización
  - *Caché*
  - Monitoreo de consumo energético
  - Electromagnético
  - Fallos diferenciales
  - ...

Sincronización

- Adversario analiza el tiempo de ejecución de un algoritmo criptográfico
- Ejecución de código diferente de acuerdo al valor de información sensible
  - *E. g.*, si un bit de la llave es 1 o 0
- La vulnerabilidad Spectre emplea este tipo de ataque

Caché

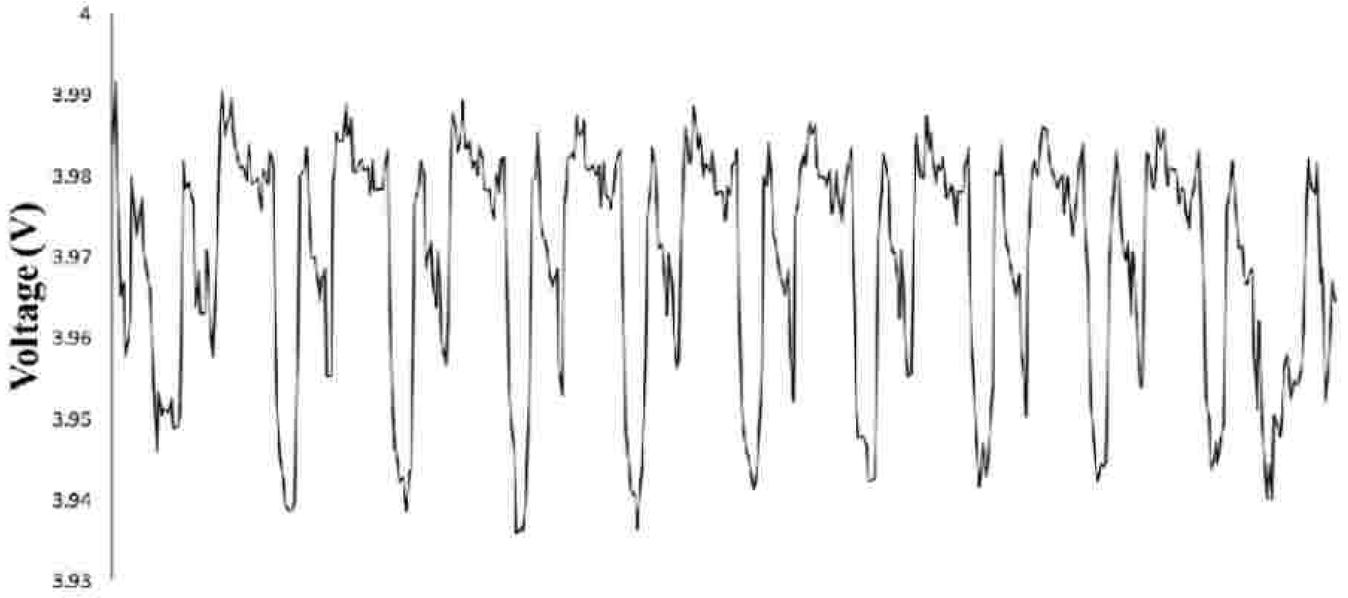
- Adversario puede monitorear los accesos a la memoria caché
- Funciona observando las operaciones críticas del algoritmo
- La llave de cifrado se deduce a partir de los accesos realizados (o no realizados) a la memoria

- La vulnerabilidad Meltdown + este ataque = acceso a memoria del sistema operativo y otros procesos

Monitoreo de consumo energético

- Adversario analiza el consumo de energía del procesador o hardware criptográfico
- Tipos
  - Análisis simple
  - Análisis diferencial

Monitoreo de consumo energético



Análisis simple en AES-128