Cifrados que preservan el formato

Trabajo terminal No. 2017-B008

Daniel Ayala Zamorano
daz2727@hotmail.com

Laura Natalia Borbolla Palacios
ln.borbolla42@gmail.com

Ricardo Quezada Figueroa
qf7.ricardo@gmail.com

Escuela Superior de Cómputo
Instituto Politécnico Nacional

Febrero de 2018

Contenido

Contenido

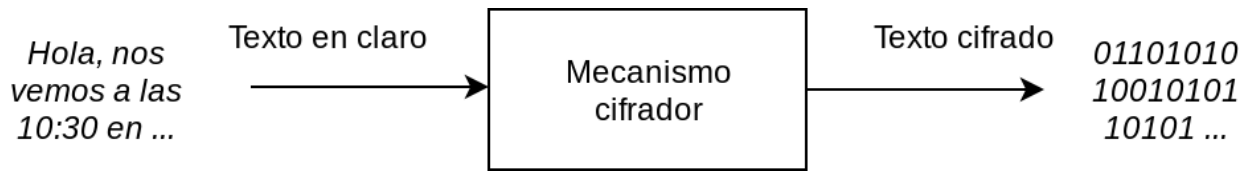
Contenido

Contenido

Introducción a FPE

Planteamiento del problema

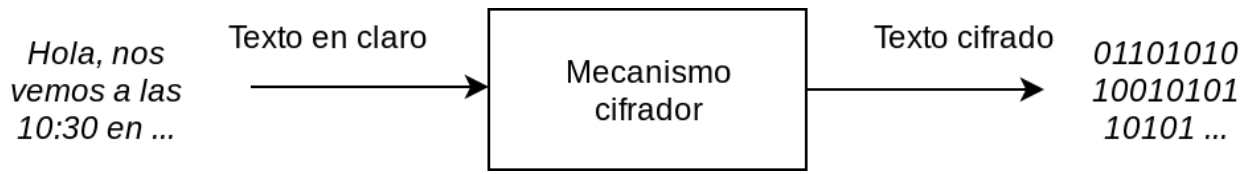
Los cifradores estándar (por ejemplo, AES) convierten un mensaje en una cadena binaria.



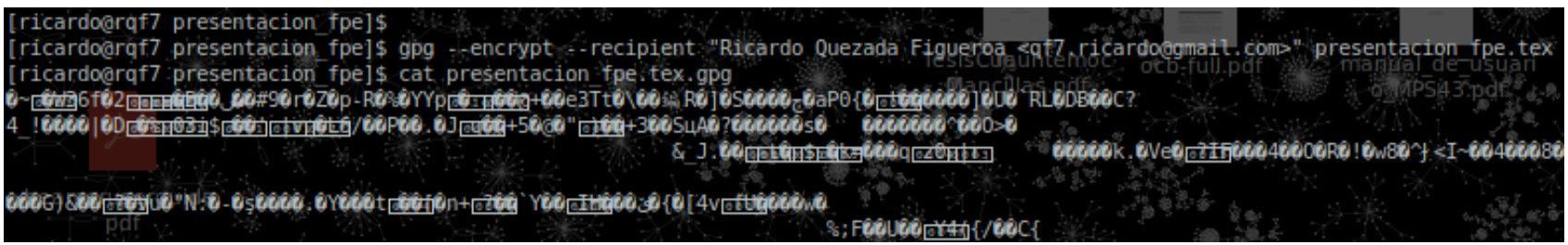
Introducción a FPE

Planteamiento del problema

Los cifradores estándar (por ejemplo, AES) convierten un mensaje en una cadena binaria.



La cual, al ser interpretada, se compone principalmente de caracteres no imprimibles.



Introducción a FPE
Planteamiento del problema

Los cifradores estándar (por ejemplo, AES) convierten un mensaje en una cadena binaria.

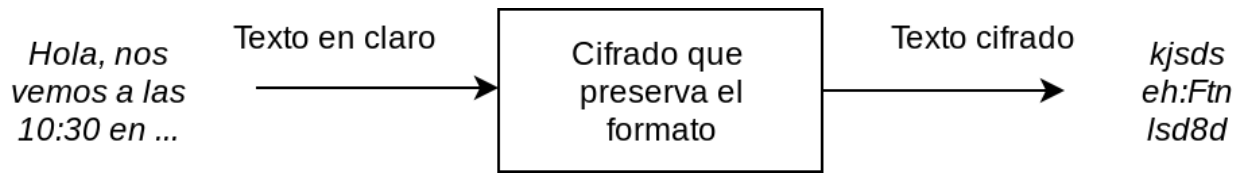
La cual, al ser interpretada, se compone principalmente de caracteres no imprimibles.

Generalización de ejemplo a pdf e imagenes: no se espera que un pdf cifrado siga siendo un pdf válido; o que una imagen cifrada se siga podiendo ver con un visor de imágenes.

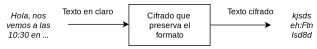
Introducción a FPE

Planteamiento del problema

El objeto de los cifrados que preservan el formato (*Format-preserving Encryption*, FPE) es convertir un texto en claro con un formato dado en un texto cifrado con el mismo formato.



El objeto de los cifrados que preservan el formato (*Format-preserving Encryption*, FPE) es convertir un texto en claro con un formato dado en un texto cifrado con el mismo formato.

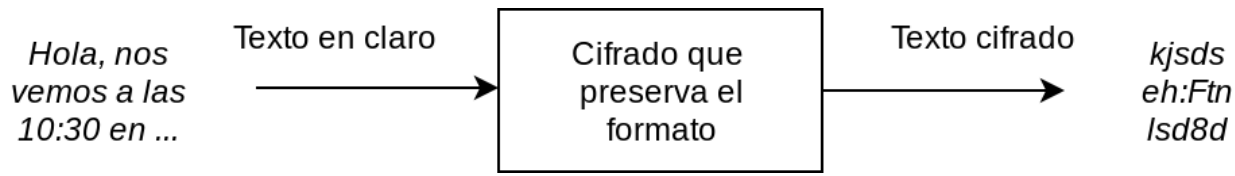


Para el ejemplo de la figura (un formato de los caracteres ASCII imprimibles), no existen muchas aplicaciones reales; es solo con fines ilustrativos.

Introducción a FPE

Planteamiento del problema

El objeto de los cifrados que preservan el formato (*Format-preserving Encryption*, FPE) es convertir un texto en claro con un formato dado en un texto cifrado con el mismo formato.



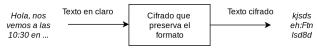
Formalmente, se busca obtener una permutación

$$\mathcal{E} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$$

que sea difícil de invertir sin el conocimiento de la llave.

Introducción a FPE
Planteamiento del problema

El objeto de los cifrados que preservan el formato (*Format-preserving Encryption*, FPE) es convertir un texto en claro con un formato dado en un texto cifrado con el mismo formato.



Formalmente, se busca obtener una permutación

$$\mathcal{E} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$$

que sea difícil de invertir sin el conocimiento de la llave.

En realidad la ecuación es casi la definición de cifrado común; lo único que hay que hacer notar es que *el formato* de $\mathcal{X}$ se debe poder reproducir en el texto cifrado.

También hay que hacer notar cómo, si se ve al formato como una cadena binaria, entonces los cifradores estándar son por sí mismos cifrados que preservan el formato.

Introducción a FPE

Aplicaciones

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

Hablar de en qué contextos se quiere preservar el formato de este tipo de datos: bases de datos que los usan como índices, o aplicaciones en las que se usan como identificadores.

Introducción a FPE

Aplicaciones

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

- Números de tarjetas de crédito.
  `5827 5423 6584 2154` $\rightarrow$ `6512 8417 6398 7423`

Introducción a FPE

Aplicaciones

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

- Números de tarjetas de crédito.
  `5827 5423 6584 2154` $\rightarrow$ `6512 8417 6398 7423`
- Números de teléfono.
  `55 55 54 75 65` $\rightarrow$ `55 55 12 36 98`

Introducción a FPE

Aplicaciones

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

- Números de tarjetas de crédito.
  `5827 5423 6584 2154` $\rightarrow$ `6512 8417 6398 7423`
- Números de teléfono.
  `55 55 54 75 65` $\rightarrow$ `55 55 12 36 98`
- CURP.
  `GHUJ887565HGBTOK01` $\rightarrow$ `QRGH874528JUHY01`

La utilidad de los cifrados que preservan el formato se centra principalmente en *agregar* seguridad a sistemas y protocolos que ya se encuentran en un entorno de producción. Estos son algunos ejemplos de dominios comunes en FPE:

- Números de tarjetas de crédito.
  `5827 5423 6584 2154` → `6512 8417 6398 7423`
- Números de teléfono.
  `55 55 54 75 65` → `55 55 12 36 98`
- CURP.
  `GHUJ887565HGBTOK01` → `QRGH874528JUHY01`

En algunos casos, se debe mantener cierta parte del texto en claro en el texto cifrado (más adelante se hablará de las tarjetas de crédito), como en el ejemplo del teléfono.

Prueba [1].

Bibliografía I


Debrup Chakraborty y Francisco Rodríguez-Henríquez. "Block Cipher Modes of Operation from a Hardware Implementation Perspective". En: *Cryptographic Engineering*. Ed. por Çetin Kaya Koç. Springer, 2009, págs. 321-363. ISBN: 978-0-387-71816-3. DOI: 10.1007/978-0-387-71817-0_12. URL: https://doi.org/10.1007/978-0-387-71817-0_12 (vid. pág. 19).