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

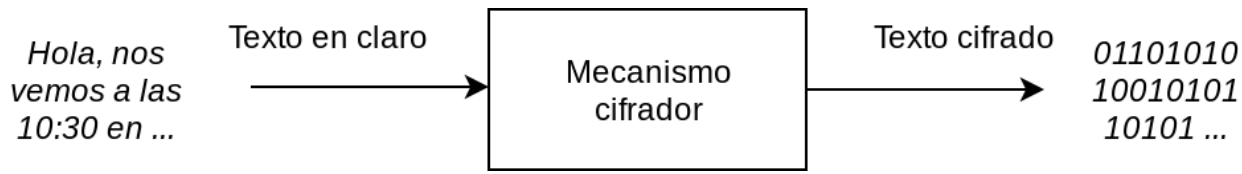
Contenido

Contenido

Introducción a FPE

Planteamiento del problema

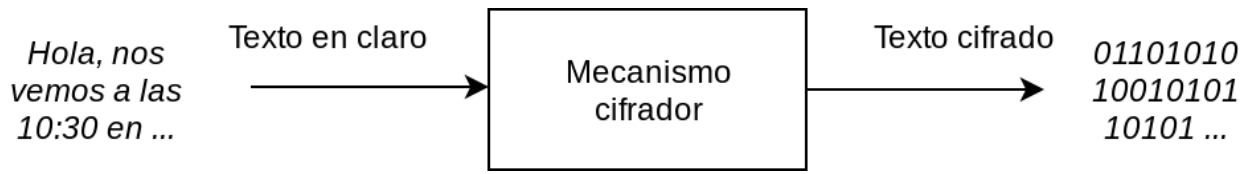
Los cifradores estándar (por ejemplo, AES) convierten un mensaje en una cadena binaria.



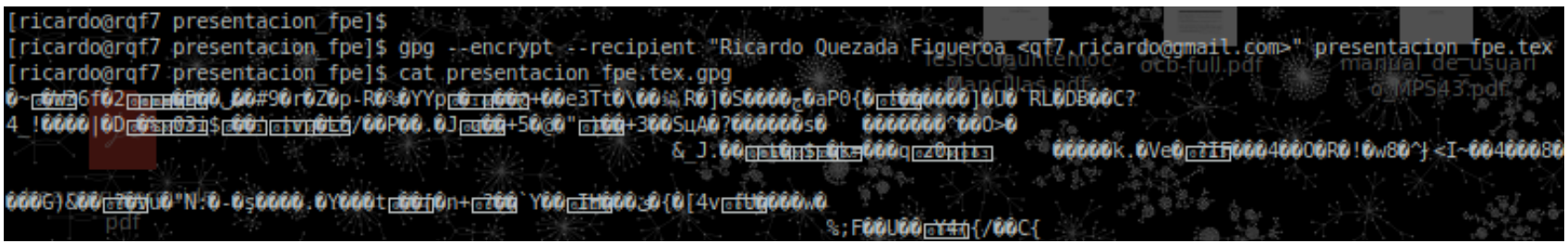
Introducción a FPE

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.

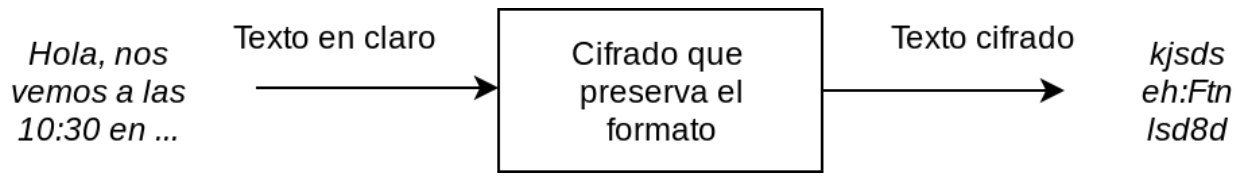
La cual, al ser interpretada, se compone principalmente de caracteres no imprimibles.

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

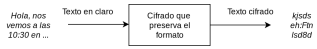
Introducción a FPE

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.

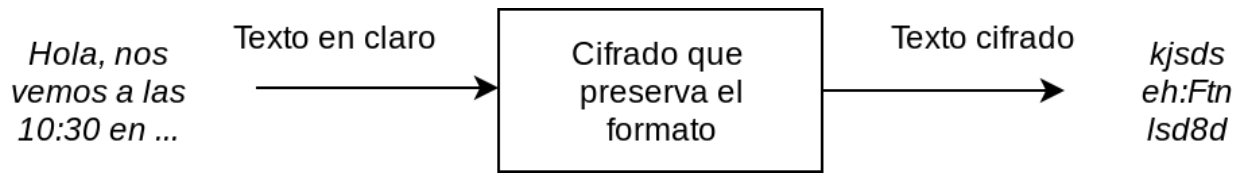


Para el ejemplo de la figura (un formato de los caracteres ASCII imprimibles), no existen muchas aplicaciones reales; es solo con fines ilustrativos.

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.



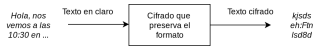
Formalmente, se busca obtener una permutación

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

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 **modos˙de˙operacion**

Anatomía de un número de tarjeta

Sobre el PAN

Un número de tarjeta (PAN, por sus siglas en inglés), se compone por tres partes:

Los números están regidos por el ISO/IEC-7812. La longitud del número de tarjeta puede ir desde 12 hasta 19 dígitos.

Anatomía de un número de tarjeta

Sobre el MII

El primer dígito de la tarjeta se refiere al *Major Industry Identifier* (MII). La relación entre dígitos e industrias es la siguiente:

- 1,2: Aerolíneas
- 3: Viajes y entretenimiento (American Express, JBC)
- 4, 5: Bancos e industria financiera (Visa, Electron; Mastercard)
- 6: Comercio (Discover, Laser, China UnionPay)
- 7: Industria petrolera
- 8: Telecomunicaciones
- 9: Asignación nacional

Anatomía de un número de tarjeta

Sobre el IIN

El *Issuer Identification Number* (IIN) comprende los primeros 6 dígitos, incluyendo el MII. El IIN puede proveer los siguientes datos:

- Banco emisor de la tarjeta
- Tipo de la tarjeta (crédito o débito)
- Marca de la tarjeta (Visa, MasterCard, Discover)
- Nivel de la tarjeta (Clásica, Gold, Black)

Anatomía de un número de tarjeta

Sobre el IIN

La base de datos BINDB proveé información cuando se ingresa un BIN [1] válido. Permite solo 10 consultas gratuitas por computadora.

Bin:	522130
Card Brand:	MASTERCARD
Issuing Bank:	TARJETAS BANAMEX SA DE CV SOFOM E.R.
Card Type:	CREDIT
Card Level:	STANDARD
Iso Country Name:	MEXICO
Iso Country A2:	MX
Iso Country A3:	MEX
Iso Country Number:	484

[1] *Bank Identifier Number*

Anatomía de un número de tarjeta

Sobre el número de cuenta

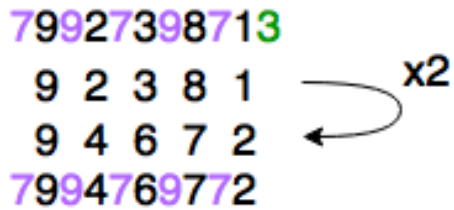
Los dígitos que siguen al IIN, excepto el último, son el número de cuenta. El número de cuenta puede variar, pero máximo comprende 12 dígitos, por lo que cada emisor tiene 10^{12} posibles números de cuenta.

Anatomía de un número de tarjeta

Sobre el dígito verificador

El dígito verificador se obtiene de la siguiente manera:

1. Comenzando desde la derecha, se obtiene el doble de cada segundo dígito. Si el producto es mayor a 9, se suman sus dígitos.



2. Se suman todos los dígitos.
3. Se multiplica la suma por 9 mód 10.

$$7+9+9+2+7+3+9+8+7+1 = 67$$
$$(67 \times 9) \bmod 10 = 3$$

El proceso para obtener el dígito verificador es conocido como el algoritmo de Luhn.

Bibliografía I