

# UN VISTAZO A LA TOKENIZACIÓN

PRESENTAN

DANIEL AYALA ZAMORANO

DAZ23AYALA@GMAIL.COM

LAURA NATALIA BORBOLLA PALACIOS

LN.BORBOLLA.42@GMAIL.COM

RICARDO QUEZADA FIGUEROA

QF7.RICARDO@GMAIL.COM

SANDRA DÍAZ SANTIAGO

SDIAZS@GMAIL.COM

PRIMERA REUNIÓN DE CIBERSEGURIDAD PARA LA INDUSTRIA 4.0  
PUEBLA, 14 DE OCTUBRE DE 2018

ESCUELA SUPERIOR DE CÓMPUTO  
INSTITUTO POLITÉCNICO NACIONAL



# CONTENIDO

El problema de la protección de datos bancarios

¿Qué es la tokenización?

Clasificación del PCI

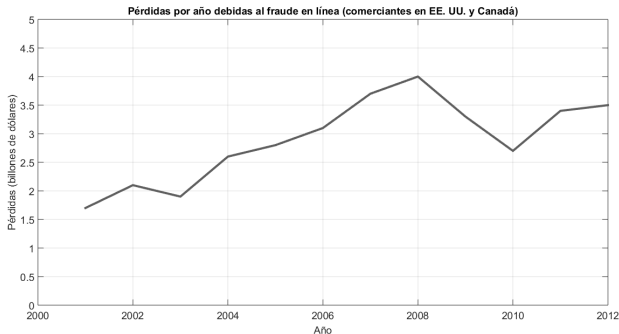
Métodos reversibles: FFX y BPS

Métodos irreversibles: TKR, AHR y DRBG

Resultados y conclusiones

# EL PROBLEMA DE LA PROTECCIÓN DE DATOS BANCARIOS

- El crecimiento del comercio en línea, aunado a sistemas débilmente protegidos propició un incremento en los robos de datos bancarios.



Pérdidas debidas al fraude en línea (2001-2012) [1].

# EL PROBLEMA DE LA PROTECCIÓN DE DATOS BANCARIOS

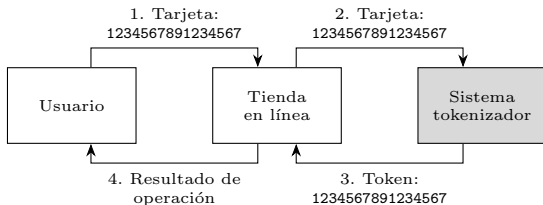
- ▶ En el 2004 se publicó el PCI DSS<sup>1</sup>[2].
- ▶ Hasta este momento el enfoque era proteger la información en donde sea que se encuentre.
- ▶ A pesar de la publicación del estándar, las filtraciones de datos no han cesado.

---

<sup>1</sup>*Payment Card Industry, Data Security Standard*

# ¿QUÉ ES LA TOKENIZACIÓN?

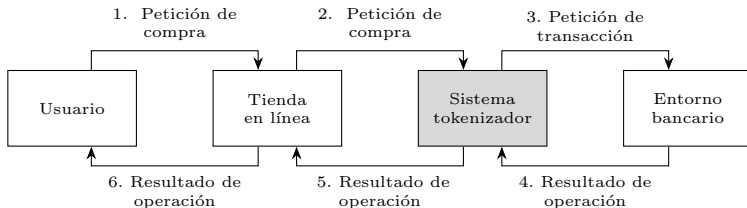
- ▶ Es la sustitución de datos sensibles por valores representativos sin una relación directa.
- ▶ Existen muchas empresas que proveen el servicio de tokenización, pero lo hacen sin detallar la forma en la que se realiza [3]-[5].
- ▶ En 2011, el PCI publicó su guía de tokenización [6].



Arquitectura de sistema tokenizador: operación de tokenización.

# ¿QUÉ ES LA TOKENIZACIÓN?

- ▶ Es la sustitución de datos sensibles por valores representativos sin una relación directa.
- ▶ Existen muchas empresas que proveen el servicio de tokenización, pero lo hacen sin detallar la forma en la que se realiza [3]-[5].
- ▶ En 2011, el PCI publicó su guía de tokenización [6].



Arquitectura de sistema tokenizador: transacción bancaria.

# CLASIFICACIÓN DE LOS ALGORITMOS TOKENIZADORES

## Clasificación del PCI [6]:

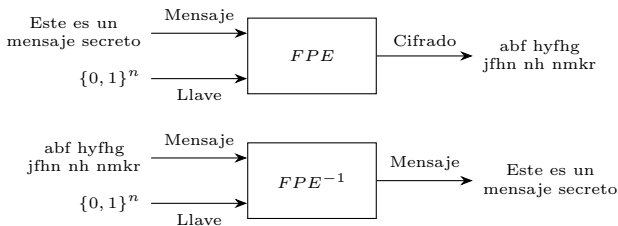
- ▶ Reversibles
  - ▶ Criptográficos
  - ▶ No criptográficos
- ▶ Irreversibles
  - ▶ Autenticables
  - ▶ No autenticables

## Clasificación propuesta:

- ▶ Criptográficos
  - ▶ Reversibles
  - ▶ Irreversibles
- ▶ No criptográficos

# MÉTODOS REVERSIBLES: FFX Y BPS

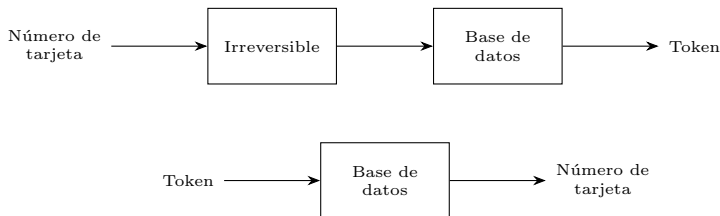
- ▶ Métodos que utilizan cifrados que preservan el formato.
- ▶ Cifran la tarjeta y descifran el token.
- ▶ Se volvieron estándares en 2016 y fueron renombrados por el NIST a FF1 y FF3 respectivamente.
- ▶ Están basados en redes Feistel.





# MÉTODOS IRREVERSIBLES: TKR, AHR Y DRBG

- ▶ Utilizan varias primitivas criptográficas (cifrados por bloque, funciones hash, generadores pseudoaleatorios).
- ▶ Requieren guardar la relación tarjeta-token.
- ▶ Su desempeño está ligado a la base de datos.

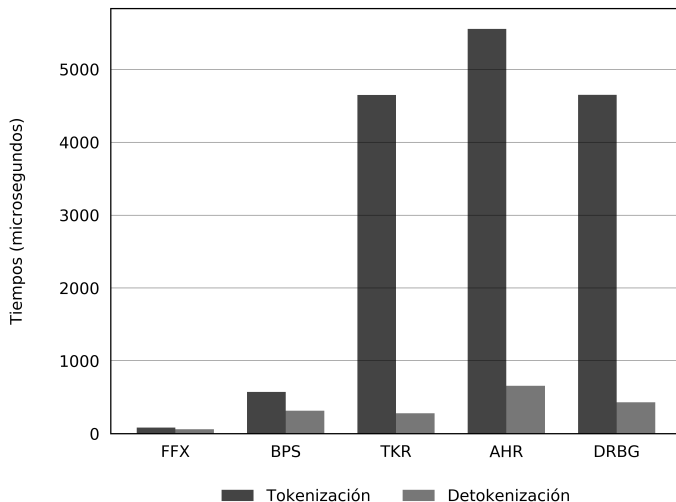


# MÉTODOS IRREVERSIBLES: TKR, AHR Y DRBG

<b>Características</b>	<b>TKR</b>	<b>AHR</b>	<b>DRBG</b>
Primitivas criptográficas	Cifrado por bloque.	Cifrado por bloque y función hash.	Función hash o cifrado por bloque.
Tamaño de llave	16 bytes	32 bytes	-
Función para mantenerse en el dominio	Función RN	Caminata cíclica	-

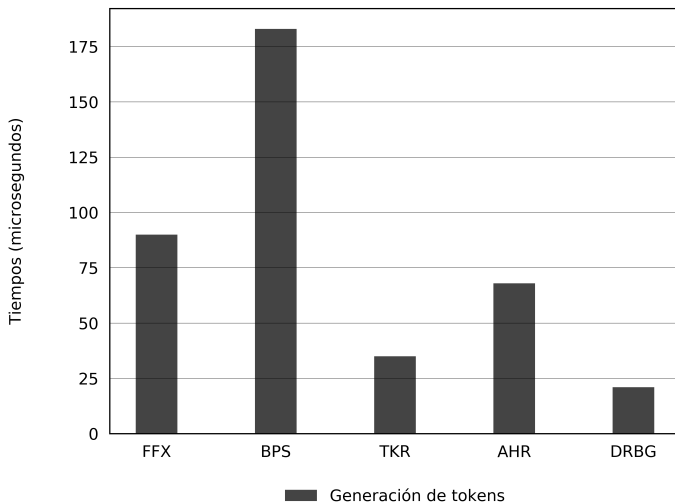
Características de los algoritmos tokenizadores irreversibles.

# RESULTADOS



Tokenización y detokenización.

# RESULTADOS



Generación de tokens.

# CONCLUSIONES

- ▶ La tokenización es una aplicación de la criptografía.
- ▶ La denominación *no criptográfica* del PCI es contradictoria.

# BIBLIOGRAFÍA I

- [1] John S. Kiernan. *Credit Card And Debit Card Fraud Statistics*. <https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/>. Consultado en marzo de 2018 (vid. pág. 3).
- [2] Payment Card Industry Security Standards Council. *Data Security Standard - Version 3.2*. 2016. URL: [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v3-2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v3-2.pdf) (vid. pág. 4).
- [3] Shift4 Payments. *The History of TrueTokenization*. <https://www.shift4.com/dotn/4tify/trueTokenization.cfm>. Consultado en agosto de 2018 (vid. págs. 5, 6).

# BIBLIOGRAFÍA II

- [4] Braintree. *Tokenization Secures CC Data and Meet PCI Compliance Requirements*.  
<https://www.braintreepayments.com/blog/using-tokenization-to-secure-credit-card-data-and-meet-pci-compliance-requirements/>. Consultado en marzo de 2018 (vid. págs. 5, 6).
- [5] Securosis. *Understanding and Selecting a Tokenization Solution*.  
[https://securosis.com/assets/library/reports/Securosis\\_Understanding\\_Tokenization\\_V.1\\_0\\_.pdf](https://securosis.com/assets/library/reports/Securosis_Understanding_Tokenization_V.1_0_.pdf). Consultado en febrero de 2018 (vid. págs. 5, 6).

# BIBLIOGRAFÍA III

- [6] Payment Card Industry Security Standards Council.  
*Tokenization Product Security Guidelines – Irreversible  
and Reversible Tokens*. 2015. URL:  
[https://www.pcisecuritystandards.org/documents/  
Tokenization\\_Product\\_Security\\_Guidelines.pdf](https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)  
(vid. págs. 5-7).



# UN VISTAZO A LA TOKENIZACIÓN

PRESENTAN

DANIEL AYALA ZAMORANO

DAZ23AYALA@GMAIL.COM

LAURA NATALIA BORBOLLA PALACIOS

LN.BORBOLLA.42@GMAIL.COM

RICARDO QUEZADA FIGUEROA

QF7.RICARDO@GMAIL.COM

SANDRA DÍAZ SANTIAGO

SDIAZS@GMAIL.COM

PRIMERA REUNIÓN DE CIBERSEGURIDAD PARA LA INDUSTRIA 4.0  
PUEBLA, 14 DE OCTUBRE DE 2018

ESCUELA SUPERIOR DE CÓMPUTO  
INSTITUTO POLITÉCNICO NACIONAL

