



INSTITUTO POLITÉCNICO  
NACIONAL



ESCUELA SUPERIOR DE CÓMPUTO

CRYPTOGRAPHY

---

## Primitivas simétricas

---

*Autores:*

González Núñez Daniel Adrián  
Hernández Castellanos César Uriel

*Docente:*

Dra. Sandra Diaz Santiago

**Ingeniería en Sistemas Computacionales**

6 de marzo de 2019

# Índice

<b>1. Librerías criptográficas en python</b>	<b>3</b>
<b>2. PyCrypto</b>	<b>3</b>
2.1. Cifrados de bloque . . . . .	3
2.2. Cifrados de flujo . . . . .	3
2.3. Hash . . . . .	3
2.4. Modos de operación . . . . .	3
2.5. Generador de bits pseudoaleatorios . . . . .	4
<b>3. Cryptography</b>	<b>4</b>
3.1. Cifrados de bloque . . . . .	4
3.2. Cifrados de flujo . . . . .	4
3.3. Modos de operación . . . . .	4
3.4. Generador de bits pseudoaleatorios . . . . .	4
<b>4. Sitio web de Banamex</b>	<b>5</b>
<b>5. Sitio web de MercadoLibre</b>	<b>6</b>
<b>6. Referencias</b>	<b>7</b>

## 1. Librerías criptográficas en python

## 2. PyCrypto

PyCrypto es una colección de módulos criptográficos que implementan diversos algoritmos y protocolos.

### 2.1. Cifrados de bloque

Los cifradores de bloque que implementa PyCrypto son:

- AES
- Blowfish
- DES
- IDEA
- ARC2
- CAST
- DES3
- RC5

### 2.2. Cifrados de flujo

Los cifradores de flujo que implementa PyCrypto son:

- ARC4
- XOR

### 2.3. Hash

- MD2
- MD5
- MD4
- RIPEMD
- SHA1
- SHA256

### 2.4. Modos de operación

- ECB
- CFB
- CTR
- CBC
- OFB
- OpenPGP

## 2.5. Generador de bits pseudoaleatorios

- Fortuna Generator
- OsRng
- UserFriendlyRNG
- Crypto Random

## 3. Cryptography

### 3.1. Cifrados de bloque

Los cifradores de bloque que implementa Cryptography son:

- AES
- Camelia
- Triple DES
- Cast 5
- Seed
- Blowfish
- IDEA

### 3.2. Cifrados de flujo

- ChaCha20
- ARC4

### 3.3. Modos de operación

- ECB
- CBC
- CFB
- OFB
- CTR
- CFB8
- GCM
- XST

### 3.4. Generador de bits pseudoaleatorios

- Genera números pseudoaleatorios<sup>a</sup> a través de un generador del sistema operativo (CryptGenRandom/Windows y /dev/urandom/Linux) os.urandom()
- Módulo secrets

## 4. Sitio web de Banamex

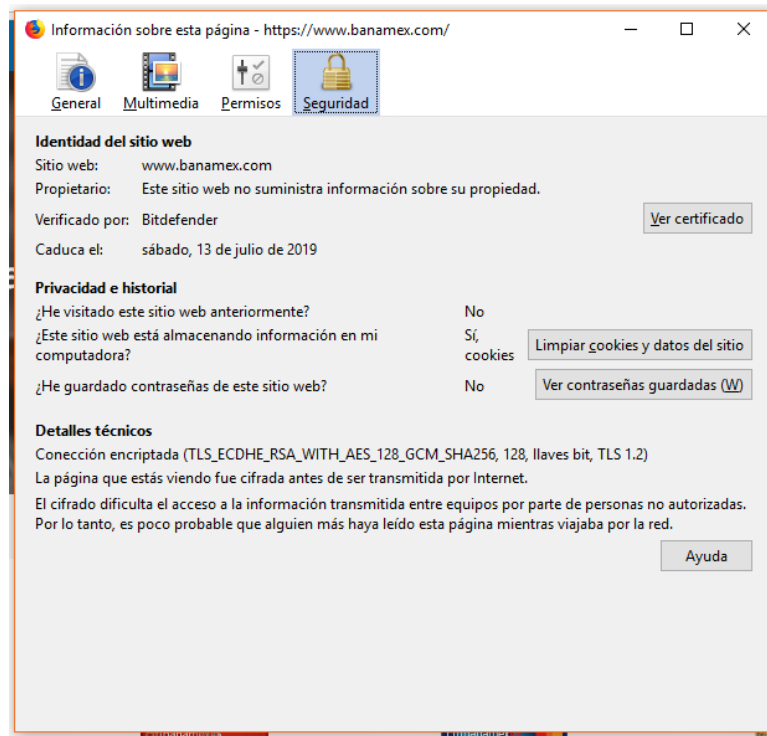


Figura 1: Información sobre la página de Banamex

En la tabla que se muestra a continuación se describen los protocolos y modos de operación usados por el sitio web de Banamex.

Siglas	Descripción
<b>TLS</b>	Seguridad en Capa de Transporte. Algoritmo criptográfico que proporciona seguridad en las comunicaciones en internet. La información es encriptada por 2 protocolos
<b>EDCH</b>	El protocolo ECDH es un protocolo de establecimiento de claves anónimo que permite a dos partes, cada una de las cuales tiene un par de claves pública-privada de curvas elípticas, establecer un secreto compartido en un canal inseguro.
<b>RSA</b>	El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye, y otra privada, la cual es guardada en secreto por su propietario.
<b>AES 256</b>	Algoritmo de cifrado por bloques que se basa en sustituciones, permutaciones y transformaciones lineales que son ejecutadas en bloques de 16 bytes. El valor de 256 representa la longitud de la clave en bits
<b>GCM</b>	Es un modo de operación para cifrados de cifrado de clave simétrica que se ha adoptado ampliamente debido a su eficiencia y rendimiento. Las tasas de rendimiento de GCM para los canales de comunicación de alta velocidad más modernos se pueden lograr con recursos de hardware razonables.

## 5. Sitio web de MercadoLibre

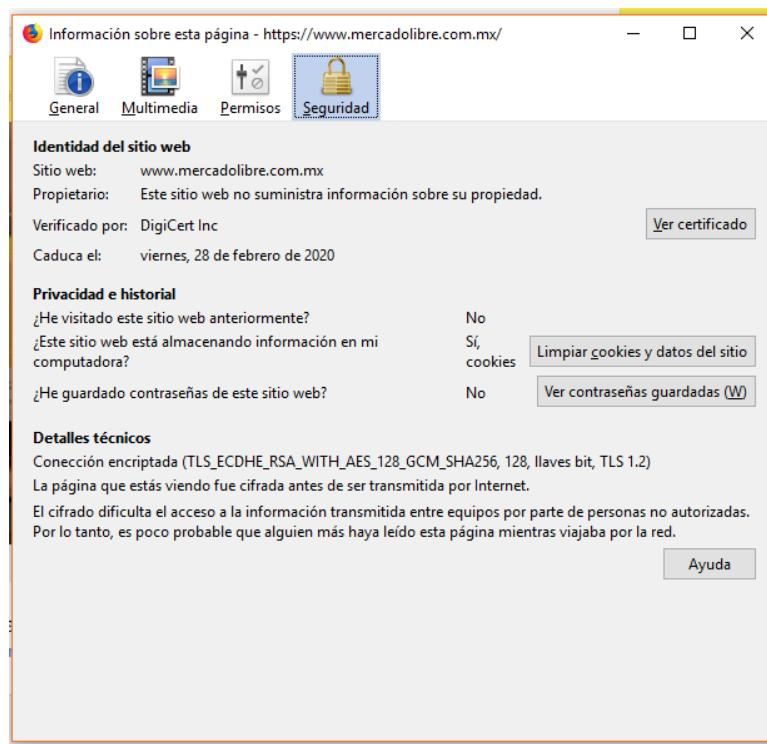


Figura 2: Información sobre la página de Mercado Libre

Es posible observar que Mercado Libre usa los mismos protocolos y modos de operación que Banamex.

Siglas	Descripción
<b>TLS</b>	Seguridad en Capa de Transporte. Algoritmo criptográfico que proporciona seguridad en las comunicaciones en internet. La información es encriptada por 2 protocolos
<b>EDCH</b>	El protocolo ECDH es un protocolo de establecimiento de claves anónimo que permite a dos partes, cada una de las cuales tiene un par de claves pública-privada de curvas elípticas, establecer un secreto compartido en un canal inseguro.
<b>RSA</b>	El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye, y otra privada, la cual es guardada en secreto por su propietario.
<b>AES 256</b>	Algoritmo de cifrado por bloques que se basa en sustituciones, permutaciones y transformaciones lineales que son ejecutadas en bloques de 16 bytes. El valor de 256 representa la longitud de la clave en bits
<b>GCM</b>	Es un modo de operación para cifrados de cifrado de clave simétrica que se ha adoptado ampliamente debido a su eficiencia y rendimiento. Las tasas de rendimiento de GCM para los canales de comunicación de alta velocidad más modernos se pueden lograr con recursos de hardware razonables.

## 6. Referencias

- [1]"pycrypto", *PyPI*, 2019. [Online]. Available:  
<https://pypi.org/project/pycrypto/>.
  
- [2]"cryptography", *PyPI*, 2019. [Online]. Available:  
<https://pypi.org/project/cryptography/>.
  
- [3]"Citibanamex | El Banco Nacional de México |  
Citibanamex.com", *Banamex.com*, 2019. [Online]. Available:  
<https://www.banamex.com/>.
  
- [4]*Mercadolibre.com.mx*, 2019. [Online]. Available:  
<https://www.mercadolibre.com.mx/>.