

Preparado por: Lic. Federico Martínez E.

Versión 1.0.0

Octubre 2014

© 2014, PagoExpress

La Información contenida en este documento esta sujeta a cambios sin previo aviso.
El presente documento así como los ejemplos incluidos sin limitación se proveen "como son".

El logotipo y PagoExpress son marcas registradas, cualquier otra marca o producto mencionado pertenece a su respectiva compañía u organización.

AUDICIENCIA A QUIEN VA DIRIGIDO

El presente documento va dirigido a desarrolladores, programadores y cualquier persona relacionada con el ámbito de sistemas computacionales.

ALCANCE

El presente documento no incluye contraseñas o claves de acceso a servidores, solo provee la información necesaria para entender el funcionamiento de la(s) aplicación(es) listadas.

PRERREQUISITOS

El desarrollador deberá estar familiarizado con programación de bibliotecas de clase de java llamados JAR o con el uso de estos.

POLITICAS DE PRIVACIDAD

Todos los materiales y contenidos de este documento, incluyendo, pero no limitado a texto, logotipos de marcas registradas o no, contenido, fotografías, audio y video están protegidos por la Ley de Propiedad Intelectual y demás Leyes, tratados y convenios internacionales suscritos por el gobierno Mexicano y por tanto vigentes y exigibles en la República Mexicana.

Queda prohibido copiar, reproducir, distribuir, publicar, transmitir, difundir, almacenar o acceder a través de medios analógicos, digitales o de cualquier otro sistema o tecnología creada o por crearse o en cualquier modo explotar cualquier parte de este servicio sin la autorización previa por escrito de Datalogic S.A. de C.V.

Todos los Derechos Reservados

Documento Propiedad de Datalogic S.A. de C.V.

Objetivo

El presente documento tiene como objetivo dar a conocer la funcionalidad del componente para la encripción y desencripción de cadenas de texto para el intercambio seguro de información transaccional.

Control de Versiones

Fecha	Autor	Cambios	No. Rev
07/Oct/14	Federico Mtz.	Creación del documento	1.0.0

Contactos:

Para cualquier duda y/o comentario favor de comunicarse con:

Federico Martinez
Líder de Integraciones
(81) 8130 8743
fmartinez@datalogic.com.mx

Encripción de una cadena de Texto

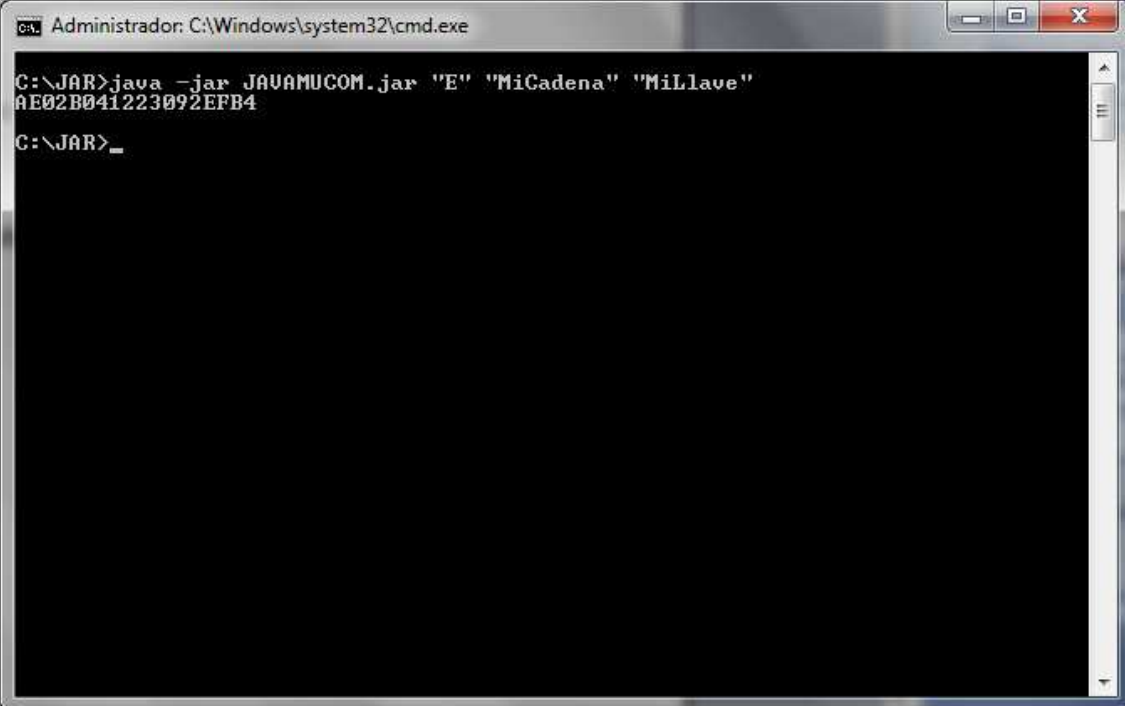
Para encriptar una cadena de texto se requiere como entrada para el JAR 3 parámetros:

1. La cadena a encriptar
2. La llave de encripción
3. Y el parámetro que indica que se hará una encripción.

La sintaxis para la encripción sería la siguiente:

```
path_del_jar/java -jar JAVAMUCOM.jar "E" "Cadena a encriptar" "Llave Secreta"
```

A continuación se ilustra un ejemplo de cómo encriptar una cadena de texto en la siguiente imagen:



```
Administrator: C:\Windows\system32\cmd.exe

C:\JAR>java -jar JAVAMUCOM.jar "E" "MiCadena" "MiLlave"
AE02B041223092EFB4

C:\JAR>_
```

Desencripción de una cadena de Texto

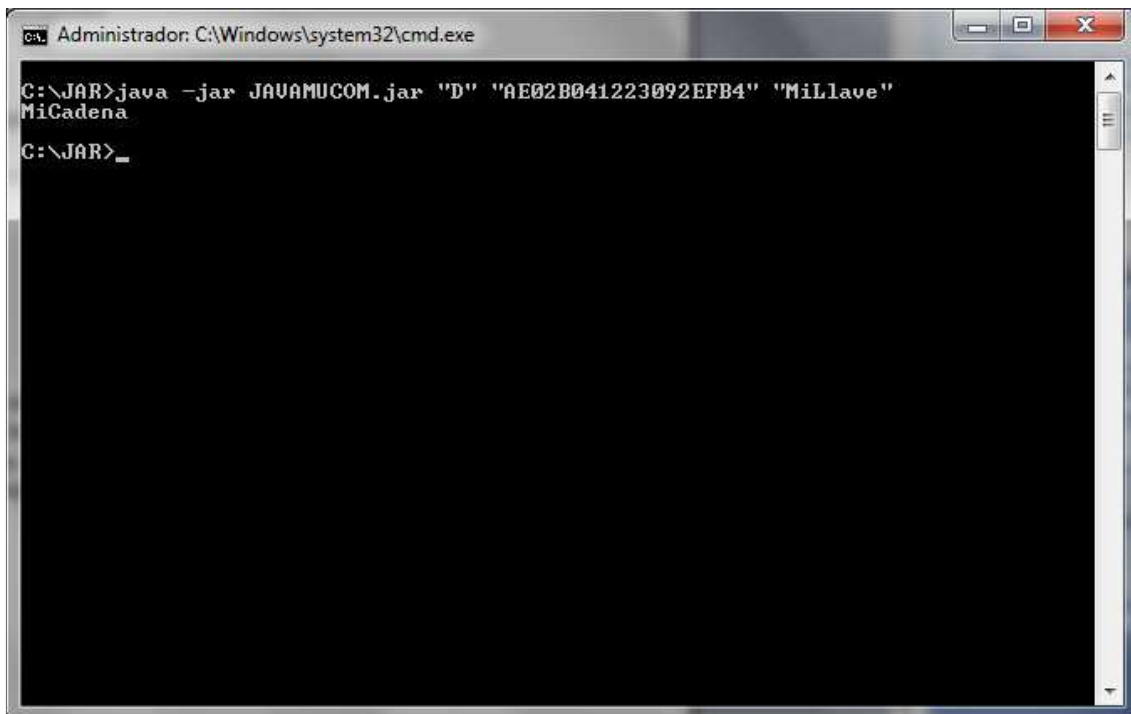
Para desencriptar una cadena de texto se requiere como entrada para el JAR 3 parámetros:

4. La cadena a desencriptar
5. La llave de encripción
6. Y el parámetro que indica que se hará una encripción.

La sintaxis para la encripción seria la siguiente:

```
path_del_jar/java -jar JAVAMUCOM.jar "D" "Cadena a desencriptar" "Llave Secreta"
```

A continuación se ilustra un ejemplo de cómo encriptar una cadena de texto en la siguiente imagen:



Notas Importantes

- a) Si la llave de encripción se introduce como cadena vacía ("") el componente tomara la llave por **default** que contiene internamente la cual es la siguiente: `pxD4t09*09Wm`
- b) La longitud de la cadena de salida encriptada es igual a dos veces la longitud de la cadena de entrada mas 2 caracteres. Si lo expresamos matemáticamente la ecuación resultante seria $L(E(input)) = (L(input) * 2) + 2$.
- c) Si se esta programando con PHP lo que se tiene que hacer es usar una función que emule el shell del sistema operativo y que tome el output de esa función de shell el cual seria la cadena encriptada o desencriptada según sea el caso.
- d) El jar ejecutable no es el que realmente hace la encripción, quien realmente la hace es otro jar llamado "**PXSecurity.jar**" que esta dentro de la carpeta lib.
- e) Existen dos componentes **JAR** ejecutables (en caso de que uno no funcione se usa el otro):
 - a. **JAVAMUCOM.jar** que funciona para cierta versión de JAVA
 - b. Y el **PXDCOM.jar** que funciona para otra versión de java
- f) Finalmente, si se esta programando en JAVA no tiene caso usar el JAR ejecutable, entonces, lo que se hace es agregar a las bibliotecas del proyecto el JAR que hace realmente la encripción: **PXSecurity.jar**