

Fundamentos de Criptografía

Seguridad para Arquitectura Empresarial y gestión
de la seguridad

ESCUELA DE INGENIERÍA, CIENCIA Y TECNOLOGÍA

UNIVERSIDAD DEL ROSARIO

[@Carlos Stivert Garavito Cardenas](#)



Criptografía simétrica

1. Explique qué es la difusión.

Transforma (sustitución y permutación) un texto, en otro que tiene una apariencia completamente aleatoria. Oculta la relación entre el texto original y el texto cifrado.

2. Explique qué es la confusión.

El criptoanalista solo conoce el texto cifrado y del conocimiento del cifrado utilizado, intentará encontrar la clave secreta. Busca ocultar la relación entre el texto cifrado y la clave secreta.

3. ¿Qué es Security through obscurity?

Hace referencia al proceso de implementar seguridad a sistema criptográfico, mediante la confidencialidad de la arquitectura interna del sistema. La idea principal es la de asegurar que un sistema es seguro mientras mantenga sus vulnerabilidades ocultas [1].

4. ¿Cómo es el principio de Kerchoff opuesto al concepto de Security Through obscurity?

El principio de Kerchoff asegura que la seguridad del sistema debe recaer en la seguridad de la clave, suponiendo como conocidos el resto de los parámetros del sistema criptográfico. Así, a pesar de que el principio STO promueve que la arquitectura y parámetros del sistema se mantengan ocultos, éstos nunca lo estarán. Esto es debido a que por lo menos un equipo de desarrolladores y diseñadores tendrán conocimiento de la arquitectura del sistema. De esta manera, el principio de Kerchoff no es opuesto a STO; sino antes bien, ambos principios son complementarios.

5. ¿Cómo puede el principio de Shanon ser aplicable en un contexto de negocios donde hay empleados con acceso a información privilegiada?

El principio de Shannon asegura que "El adversario conoce el sistema". En un contexto de negocios, el principio de Shannon es relevante ya que además de considerar ataques por entidades externas a la organización, también se hace necesario considerar la posibilidad de tener atacantes que están al interior de la organización y, por ende, conocen el sistema. De esta manera, en este contexto se justifica la necesidad de aplicar del principio de Kerchoff pues el principio STO por sí solo se vuelve insuficiente.

6. Explique las operaciones principales desarrolladas por una función AES (Advanced Encryption Standard)

El algoritmo AES procesa bloques de texto de 128 bits, con claves estándar de 128, 192 ó 256 bits. Usa una matriz de estado de tamaño 4x4, cuyas celdas cambian de valor en función de la operación del

algoritmo usando técnicas de sustitución y permutación; en algunos casos con operaciones polinómicas dentro de un cuerpo.



Figura 1. Representación del bloque de texto en AES. A la izquierda, bloque de texto y su representación hexadecimal. A la derecha, representación del bloque de texto en la matriz de estado.

El algoritmo ejecuta sus funciones según el esquema presentado en el diagrama de flujo de la figura 2. En cada ronda (vuelta o iteración) se genera una llave de vuelta, generada a partir de la llave maestra o principal. Las funciones que ejecuta se explican a continuación.

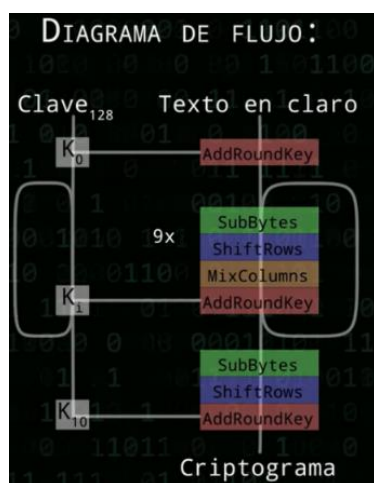


Figura 2. Diagrama de flujo algoritmo AES.

AddRoundKey Suma XOR entre los bytes del mensaje y la llave



Figura 3. Representación esquemática de la función AddRoundKey.

SubBytes Sustitución de cada uno de los 16 bytes de la matriz de estado mediante una tabla

MATRIZ DE ESTADO

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E

Figura 4. Representación esquemática de la función SubBytes

ShiftRows Permutación de filas de la matriz de estado.

- La primera fila no rota
- La segunda fila, rota una vez
- La tercera fila, rota dos veces
- La cuarta fila, rota tres veces

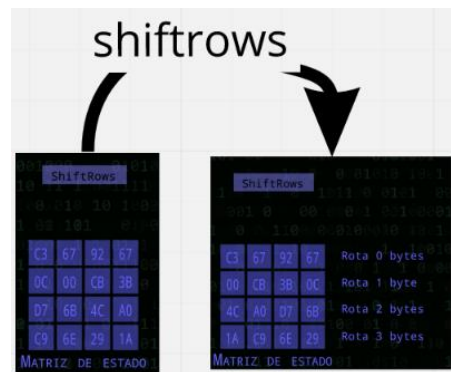


Figura 5. Representación esquemática de la función ShiftRows

MixColumns Multiplica cada una de las columnas de la matriz de estado, por un polinomio fijo

CONSTANTE

MATRIZ DE ESTADO

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

x

C3
00
4C
1A

=

67	92	67
CB	3B	0C
A0	D7	6B
C9	6E	29

Figura 6. Representación esquemática de la función

Para el descifrado, el algoritmo recorre el mismo diagrama de flujo, pero en sentido contrario y aplicando las funciones inversas del algoritmo de cifrado.



Figura 7. Representación esquemática del diagrama de flujo para el descifrado.

7. Si usted desarrolla un algoritmo de cifrado robusto y genera una llave larga, ¿cómo puede usted distribuir la llave a un colega que está ubicado en lejos de usted?

La idea es codificar la llave con un algoritmo convencional como el AES, tal que su llave corresponda a una información que solo el destinatario tiene o pueda generar. En este sentido, la llave del AES puede corresponder a un conjunto de valores adquiridos por un sensor biométrico en la ubicación del destinatario.

Criptografía asimétrica

1. ¿Cómo la criptografía asimétrica puede proteger la confidencialidad de un mensaje?
La criptografía asimétrica

En contraste con la criptografía simétrica, la criptografía asimétrica se ejecuta mediante el uso de dos claves, que están relacionadas entre sí; esto es, una pública y una privada. Como su nombre lo indica, la pública es una clave que está disponible para todos, mientras que la privada solo es conocida por una de las dos entidades del proceso de comunicación. La idea de la criptografía asimétrica se puede explicar desde la analogía de enviar un mensaje al interior de una caja que se asegura con un candado. La llave pública representa la actividad de cerrar el candado abierto, mientras que la llave privada, que solo la tiene quien recibe la caja, es única, y es la que abre el candado. Esto es, la llave pública cifra el mensaje (cerrar el candado) y la llave privada lo descifra (abrir el candado). Así, la criptografía asimétrica protege la confidencialidad de un mensaje en el hecho que la llave privada, que es la clave que descifra el mensaje, nunca se distribuye.

2. ¿Cómo la criptografía asimétrica puede proteger la autenticidad de un mensaje?

La llave privada puede ser usada tanto para descifrar como para cifrar. Lo mismo sucede con la llave pública. De esta manera, cuando se cifra un mensaje con la llave privada, cualquiera que tenga la llave pública estará en capacidad de descifrar el mensaje. Al estar relacionadas entre sí, el proceso de cifrado y descifrado solo tendrá éxito si se usa el par de llaves adecuado. Así, cifrar un mensaje con una clave privada garantiza que solo quienes tengan la llave pública correspondiente estarán en capacidad de descifrarlo y, a su vez, los receptores del mensaje tendrán certeza de su autenticidad bajo el hecho que si el mensaje ha sido descifrado con la clave pública, pone en evidencia que fue cifrado con la clave privada correspondiente, que es única y solo es de conocimiento del emisor.

3. Mencione los beneficios de una firma digital sobre una firma mecánica.

- **Autenticidad** Garantiza la identidad del emisor de un mensaje,
- **Integridad** garantiza que el mensaje no ha sido alterado ni modificado,
- **No repudio** El emisor no puede negar el conocimiento de un mensaje.

4. ¿Cómo los certificados digitales resuelven parcialmente el problema de la criptografía asimétrica relacionado con la distribución de las llaves?

Un certificado digital, se utiliza para vincular una clave pública con la entidad que la posee. La distribución, autenticación y revocación de certificados digitales se implementa mediante la infraestructura de clave pública (PKI). Es usual que la generación de los certificados se haga mediante terceros que administran soluciones PKI. Sin embargo, los certificados digitales no son una solución completa para los ataques del tipo Man-in-the-Middle. Los atacantes pueden capturar certificados de sitios web confiables y engañar a los usuarios para que compartan información confidencial. Un ejemplo de certificados digitales es el cifrado SSL, el cual cifra la comunicación entre el servidor y el cliente, lo que ayuda a que los atacantes no roben los datos del cliente [2].

5. Encuentre las desventajas de la criptografía asimétrica relacionadas con el rendimiento.

El rendimiento se puede evaluar desde dos perspectivas [3]:

- **Velocidad** En contraste con la criptografía simétrica que usa solo una llave, el hecho de que la criptografía asimétrica use dos llaves hace que su proceso de encriptación sea más robusto y lento. En general, los procesos de cifrado y descifrado se consideran lentos e impactan directamente la capacidad de cómputo y el gasto de energía.
- **Seguridad:** La criptografía asimétrica presenta ventajas sobre la criptografía simétrica, ya que en el caso de la criptografía simétrica la necesidad de distribuir la llave que descifra el mensaje aumenta el riesgo de seguridad, en contraste con la criptografía asimétrica en donde la llave que descifra el mensaje no es necesario que se comparta.

6. Use OpenPGP para intercambiar un mensaje encriptado con un compañero de clase. Adjunte capturas de pantalla con una explicación del proceso.

Seleccione una de las opciones disponibles

Opción seleccionada

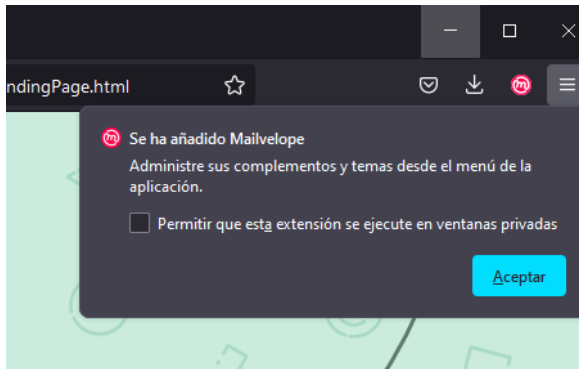
Mailvelope

Mailvelope is a browser extension for Google Chrome and Firefox that allows secure email communication based on the OpenPGP standard. It can be configured to work with arbitrary Webmail provider. The project focuses on easy usage and good integration with nearly every webmail client.

Key Facts

- Developer/Publisher: Thomas Oberndörfer with [Community](#)
- License: Open Source (GNU GPL)
- Price: Free
- Web: <https://www.mailvelope.com/>
- Help: Help is provided by the CEO
 - [Email](#)
 - [FAQ](#)

Instalación del plugin



Cree una llave pública y privada para su cuenta de correo URosario

Generando la llave

[< Administración de llaves](#)

Generar llave

Generar

Nombre

Carlos Garavito

Nombre completo del propietario de la llave

Correo electrónico

carloss.garavito@urosario.edu.co

Avanzado >>

Introduzca contraseña

MKquD9kSygFupKF|

Vuelva a introducir la contraseña

.....

☒ Subir llave pública al Servidor de Claves de Mailvelope (se pueden borrar en cualquier momento). [Conocer más](#)

Sincronización de la cuenta de correo con el servidor de mailvelope

Mailvelope Key Server

Email address carloss.garavito@urosario.edu.co successfully verified

Your public OpenPGP key is now available at the following link: <https://keys.mailvelope.com/pks/lookup?op=get&search=carloss.garavito@urosario.edu.co>

© 2021 Mailvelope GmbH

[Imprint](#) | [Privacy](#)

Verificación de la cuenta en el servidor de mailvelope

[https://keys.mailvelope.com/manage.html](#)

Mailvelope Key Server [Home](#) [Manage Keys](#) [GitHub](#)

OpenPGP key upload

Paste PGP PUBLIC KEY BLOCK here ...

Upload

OpenPGP key lookup

carloss.garavito@urosario.edu.co

Mailvelope Key Server

[Home](#) [Manage Keys](#) [GitHub](#)

Email: carloss.garavito@urosario.edu.co

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBGKE71ABEADUVshU3MuD2vKeCM/Iwk6L+Nbcu6SwdIZ1qyQmOGXDLy5
AMs3x8NouprCjZQk9Vr2V+PudI153F67+hcYtpFA/eo8bGh9X3c+hvjucg8t
Mdj0wdEQ8bDy37B1kYh8bIhp7bB3NVu3nruQ6fwLAZayZ2023KuCbFsmtvF
fyzu9q+7iG2s0p7aphy4Ye4CxM6C9/q1BbDocICfz8a/800dH+FTNF8HKHEH
k4AI0unnvpFtcdUL04cxmOXM1HtGKpByMDkOpz2vnDUM86vStnMZF1UkYFj7
aoCvuRzn3JYnM2tFK68q/qbfcS8faHTOPWdX0K3Cz0q2dCFFLhw1ABmE3fmd
CDAoUj1zvs4F1DVlmb3tkySzD3rjW4krkBPpRgUe0U5bykdScOSWKKGCFf
+35/d8sSLxo0EhuZ38gvhiXwkTX5Bto1ZGXYShEBD6LYb4fu8v4+t3JgDLjs
phICmoGdNUNVUICvgwYMEuGph/GwpY+bOrqRA/qcyuW4jpmTsJN8az/uP/t
eKhpqKKx0DlWAmpEP+1Qs6hzZ7HprSR1bV0ktwYba1h5DH012vG1QaGF578sa
UYwi15uy61j8RmyEuF4du51UI16XdI7z4Y9D2+0GGEizK9gQcotsdCf/Vp/
GA8cn471P9aeDcr7u0IbKVSH6d1p3PK004c1YwARAQABzTJ0YXJ3b3M3MgR2Fy
YXZpdG8gPGNhcmxvc3MuZ2FyYXZpdG9AdXJvc2FyaW8uZWRR1LmNlPvSLBdQQQ
AQgAHwUCYoTuUAYLQCICIAwIEFQgKAgWAgECGQECGwMCHgEACgkQJ5N7Lvrc
Ko37rBAAsm4FUoEtHxst10tDk62rKfcdR412TjsdoqO4WUjHy3/V10KwiTP
joTZZCH+TVa1vuY8z641xHaV+5rXSTQ1zL6UXU9LOqzFqemIn19z01ZwWp8E
IXCujmyIMjc9KglEo18sQ+QVYaqteZjUAAT8tqVXnZwWvH46q+58HEqj5eY4
SwIKdgFVKUUmG20ZQ3jM0xLEjFQkjbsb8xx8dmBohqpsjyITA1ptd2g25x
ZM2T0oFs/E7e4xKHeJU/tZ/IU01sTQ7EW7Fc705aAQYFX5eYFz7sp2CaHyV8
```

Usuario 2 (simula compañero de clase)

[< Administración de llaves](#)

Generar llave

Generar

Nombre

Carlos Garavito UN

Nombre completo del propietario de la llave

Correo electrónico

cgaravitoc@unal.edu.co

Avanzado >>

Introduzca contraseña

HKquD9k5ygFupKrf

Vuelva a introducir la contraseña

☒ Subir llave pública al Servidor de Claves de Mailvelope (se pueden borrar en cualquier momento). [Conocer más](#)

Mailvelope Key Server

Email address cgaravitoc@unal.edu.co successfully verified

Your public OpenPGP key is now available at the following link: <https://keys.mailvelope.com/pks/lookup?op=get&search=cgaravitoc@unal.edu.co>

© 2021 Mailvelope GmbH

Imprint | Privacy

Envíe su llave pública a su compañero de clase

Exporta clave de usuario 1

Exportar llave

×

¿Qué llave desearía exportar?

Público

Privado

Todas

—BEGIN PGP PUBLIC KEY BLOCK—
Version: Mailvelope v4.5.2
Comment: <https://www.mailvelope.com>

xsFNBGKE7lABEADUYshUU3MuD2vKeCM/lwk6L+Nbcu6SwdlZ1qy
QmOGXDLy5
AMs3×8NouprCjZQk9Vr2V+Pudl153F67+hcYtpFA/eo8bGh9X3c+hvj
cug8t
Mdj0wdEQBbDyJ7B1kYh8blhp7bBJNVujnruQ6fwLAZayZ2O2J3KuC
bFSmtvF
fyzu9q+7iG2s0p7aphy4Ye4CxM6C9/q1BbDoclCfz8a
/80DdM+FTNf8HKHEH
k4AIounvnpFtcdUL04cxmOXM1HtGKpByMDWOpz2vnDUMB6vSTn
MZFlUkyFj7
aoCvuRznJlYnM2tFK68q/qbfcSbfaHTOPWDx0KJCzOq2dCFFLhw1A

Cerrar

Copiar al portapapeles

Descargar

Reciba la llave publica de su compañero

Importando clave publica de usuario 2

< Administración de llaves

Añadir claves

Importar claves

Importar

Buscar

Puedes añadir claves tanto como archivo o como texto desde el portapapeles.

Seleccionar archivos

Arrastre el archivo hasta esta ventana o

Añadir archivo

Texto desde el portapapeles

```
21QHwGAS03dDUdJ492mxh1eDsqw4qE6nL8mCqj0ezWlU2dCLX0f+JqHUu2E
5AMbw00CUwnusKg0pS3Oij7O2xHoapKkOULZ4wsuTlfr+C/KGSFX6zgbY4bq
w6C0Qcp+EDb9lhWtN4N03t8vEF0aVgGQwYbZgdkUysiqmCU69YzJFV/FBMvV
RnXEM2hHBL+9dvU7p5+Y3EMyjvQMAx2x8DKLwYfYaBEFgKVC8XfHqIuB
kW7aXN9Dc+92gVHCgX94G0RqzApKGDrtT4iXOt/ig74Jat8hrqV+tdotB
1w1p281vXYOVmHlpkTweUW0woGcNpq3x13Bq3BQSBg0YvLzeBuwmalY56QGu
qyhiPXUGbCJijNa4KLxWVQW6C2F1qwJ7ATGBudxv7txDm08EgaeHkBP9eJH
FkleOfDKRtgg3SVdhbPVJWE=
=dvPk
--END PGP PUBLIC KEY BLOCK--
```

Enví un correo encriptado a su compañero y valide que éste lo recibe y lo descifra

Cifrado del mensaje

Cifrar datos

Cifrar

Destinatario

cgaravitoc@unal.edu.co x

Los datos cifrados están firmados con tu llave (carloss.garavito@urosario.edu.co)

Cambiar

Remover firma

Adjuntos

Arrastre el archivo hasta esta ventana o

Añadir archivo

Mensaje

Hola,
este es un texto cifrado desde carloss.garavito@urosario.edu.co.

< Cifrar datos

Cifrado exitoso

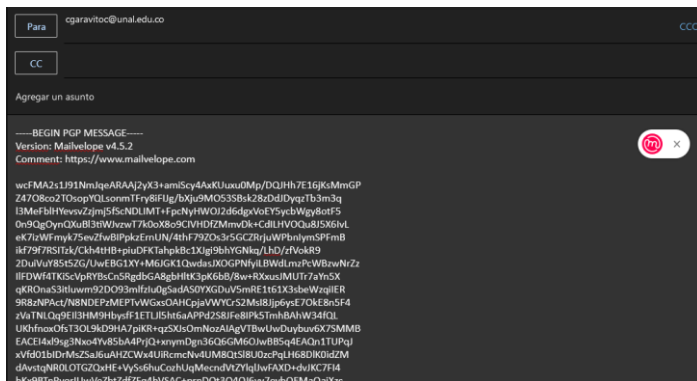
Cifrado para cgaravitoc@unal.edu.co

Firmado por Carlos Garavito (carloss.garavito@urosario.edu.co)

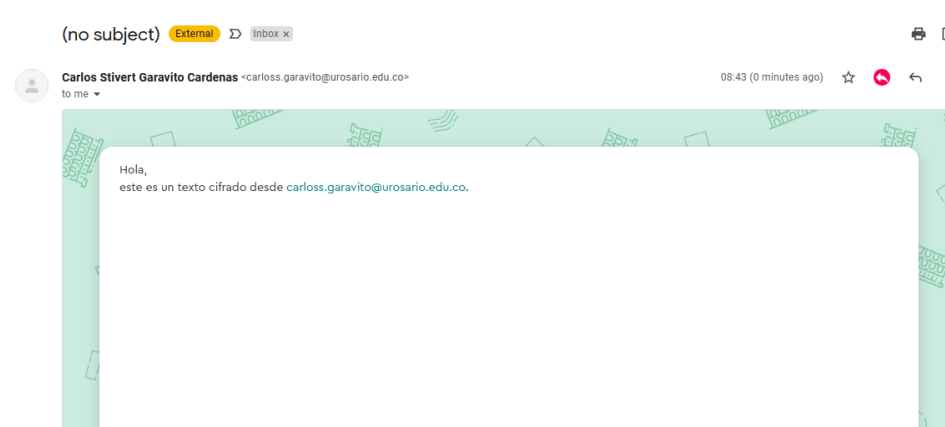
Archivos cifrados

```
text.txt
CMjGBPHC+QJL/8O2GnX9E2K6AaCVUHaBaq30p5j1YfaWnM1Biv3zv/OXXEF
baX0tdLw60NC+6wTECaibYzPC0s9Vzu5SzLEFonRkTRGd13E
ue4UZZn+TnBLaxa56s1X8Q2tE+O9EJ+vcLP40/WvVC4CVU+uadAWBv
0+als5eKdK10V/bjHeAP+Y2ZJHfgvP5n7XfudD9mXaqqhA+40v3DB1N
7oq3YU8+4ueuhjSHQcXhneJ0LtatWZ+AKQZ7X9Dyasochx
==Sun
--END PGP MESSAGE--
```

Envío del mensaje cifrado



Recepción del mensaje por parte de usuario 2



7. Pegue en el informe su llave pública.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: Mailvelope v4.5.2

Comment: https://www.mailvelope.com

xsFNBGKE7IABEADUYshUU3MuD2vKeCM/lwk6L+Nbcu6SwdlZ1qyQmOGXDLY5

AMs3x8NouprCjZQk9Vr2V+Pudl153F67+hcYtpFA/eo8bGh9X3c+hvjcug8t

Mdj0wdEQBbDyJ7B1kYh8blhp7bBJNVujnruQ6fwLAZayZ2O2J3KuCbFSmtvF

fyzu9q+7iG2s0p7aphy4Ye4CxM6C9/q1BbDoclCfz8a/80DdM+FTNf8HKHEH

k4AIounnvpFtdcUL04cxmOXM1HtGKpByMDWOpz2vnDUMB6vSTnMZFIUKYFj7

aoCvuRznJIYnM2tFK68q/qbfcsBfaHTOPWDx0KJCzOq2dCFFLhw1ABmE3fmd
CDAoUj1zvus4FiDVImB3tkySzD3rjW4krkBPMRgUe0U5bykdScOSWNKKGCff
+35/d8sSLxoOEhuZJ8gvWiXwkTX5BtolZGXyShEBD6LYb4fu8v4+tJJgDLjs
phlCmoGdNUNVUICvgwYMEuGpW/GwpY+bOrqRA/qcyuW4jpmtsJN8az/uP//t
eKhpqKKxDIWAMpEP+IQs6hzZ7HprSRibV0KtwYba1h5DHO12vGiQaGFS78sa
UYwil5uy61j8RmyEufX4du5UIl6XdI7z4Y9D2+0GGEizK9gQcotsdCf/Vp/
GA8cn47IP9aeDcr7uOlBKV5H6d1p3PK004c1YwARAQABzTJDYXJsb3MgR2Fy
YXZpdG8gPGNhcmxvc3MuZ2FyYXZpdG9AdXJvc2FyaW8uZWR1LmNvPsLBdQQQ
AQgAHwUCY0TuUAYLCQClAwIEFQgKAgiMwAgECGQECGwMCHgEACgkQJ5N7Lvrc
Ko37rBAAsm4FUoEtMxstlOtDk62rKfcdR412TjsdoqO4WUjHyy3/Vl0KwiTP
joTZZCH+TVaIvuYBz64lxHaV+5rXSTQlzl6UXU9LOqzFqeminl9z0lZwMp8E
IXCujmyIMjc9Kg1Eol8sQ+QVYaqteZjUAAT8TqVXnZwNvH46q+SBHEqjSeY4
SwIKdgFVKuUmgG202QJm0xLEjfQkjbsb8xx8dmBohqpsjyITAiptd2g25x
ZM2T0oFs/E7e4xKHeJU/tZ/IU01sTQ7EW7Fc7OSaAQYFX5eYFz7sp2CaHyV8
iNsoay8brpwHG6SBLc/NwLM4PD8t7wl62yeNBhpli9Y70mtg4NfDxwNL9xqf
dE047OEhs2upe1OrfR3ZE9vtGuRIJ2Q5iUD3wqK8xVPkql0Pa4MywFzX6d+2
fwU78itn24noG119CwedHf0M83d1UN5liuTp+l3S9zVQtZ+Td7ZOayBrHqTn
waucwGs/Kxa79Y8UwLxzQE/PsMt6AgEn9r9sXdLqZt3YE4myACHdxknmc2zm
QG49GEy4pkmYWC9jS7aiPhF7ppU7vquBN1pO/v33FGG9quLuOxLGhV4Ppq8e
fu0QmCvtnRZRDFSvZ7t/BuU8YCiZkt80yc52LWxfQrZE039otOyz+UizWWGc
kfAauENbFUG252YPJk/Aim0MFK3OdQrOwU0EYoTuUAEQAMCsiH9G084sHqg0
sOMzeGARq8uULaWeOfR5PmFGLE6iHfPOHdmNdbQvOqCS5WE2PZkpAyL84dA1
Tzlg/D2V/h0bEJ3s5OKilwnOvZgwo4aH3iUqUYXnt9iM9rIO6h9UiyG9Mg82
LYI86aNIipe4uZhieSkH5OQHsNvnvp4z9LrfR/nwlyEEK51RQtoBd1p/hFOy
Wu3/leyVLW8tYPIMWkC8ZYjFOx0DorZJxqkv6cSq2QtfnHwo4z4mJ9bmOLe
oZ3KHgNH9Rzj5Gg6pWfx55OyVyFq7ScnYNiOMp6m0dRRBtf0dn1zkO0VIDb
m66tRxBr8l+NV3NUmvaF2bsgoLIhMXCoscFEs7fzj3g+RcCQZgFaXp2eC3MX
KBgN+lv34zxvShS8rFrEsbo7X2IBInSIC1QCAVH9hWQsqeZtel68AgF9T1Hr
GBTDsb8CWwTqho3S8mefd0lfhTpHDbmOX629Q4tzvqavV148v8mFu9/BYnmf

JUG4FpIIVfWujcsM2jdU4ldYkPp3Efn+rVxouHjrlRSU+nZP7a3NdjOm0LUB
moUYrpyXYt1k4YMBUyU5A5zhtN3s1z9MebTXGyVDvU+KFjq9jBAgGXM0E9d
PQAW3BJmBtzuwlu5rOEb7feGoXR6t6AsCTcFRTbpKXTx7omN4eUPYz+yZPrS
7RnGG3AfABEBAAHCwV8EGAEIAAKFamKE7IACGwwACgkQJ5N7LvrcKo0vxxw//
WYBtqUL+rC2BqOGxzmG2Tf0qpO1YNYTzg2563cppTI5KFrGjVxVeYkvU2q
ORAswgEPrtMYlqyQTKIUSGYXw4AeCkzHlqiQXPzf+78hZA6VDQZ3Uwcbh2aB
9SZ/0SF0NN1CQigZ9QAc/Tz1N1SE2aNOpKwinU/7uoKJO9TrxHJhtZID4C92
YLWIMfoAW9xCdRDMODSHABHGXP16Sr7e8Pej0zVnVPD3HCEmOX+kaSiDGXFN
2TQHWGAs03dDUdJ492mxh1eDsqw4gE6l1L8mCdj0ezWIU2dCLx0f+JqHUu2E
5AMbww0CUwnusKg0pS3Olj7O2xHoapkKOUlZ4wsuTlft+C/KGSFX6zgbY4bq
w6COqcp+tDb9lhWtN4NO3t8vEF0aVgGQwYbZgdkUysiqmCU69YZJFV/FBMvV
RnXExM2hHBl+v9dvtu7p5+Y3EMyJvQMAx2xBDKLwYtFyaBEFqKVC8XfHqluB
kW7aXN9Dc9zgivHGgX94G0RqzApkGDr1zT4iXOt/igx74JatBhrqV+izloTB
1w1p281vXYOVMhlpkTweUWOwoGcnpq3xl3Bq3BQSbg0YvLzeBuwmalYS6QGGu
qyhIPXUGbCJljNa4KLXsWVQW6C2F1qwJ7ATGBudxv7txDm08EgaehkBp9eJH
FkleOfDKRtgg3SVdhibPVJWE=
=dvPk
-----END PGP PUBLIC KEY BLOCK-----

Referencias

- [1] Security Through Obscurity (STO) <https://www.techopedia.com/definition/21985/security-through-obscurity-sto>. Consultado el 17 de mayo de 2022.
- [2] ¿Qué es un Certificado Digital y para qué se usa? <https://ciberseguridad.com/guias/prevencion-proteccion/certificado-digital/>. Consultado el 18 de mayo de 2022.
- [3] When to Use Symmetric Encryption vs. Asymmetric Encryption. <https://www.keyfactor.com/blog/symmetric-vs-asymmetric-encryption/>. Consultado el 18 de mayo de 2022.