

CTF01 – Resolución

Nombre: Pablo Silva Villalobos

Respuesta:

1. En primer lugar, recordé lo realizado en el LAB01, en donde tuvimos que responder para qué serviría una herramienta de CyberChef que permite cambiar los colores de una imagen. En ese formulario, mi respuesta fue que probablemente existía una técnica para codificar mensajes y esconderlos dentro de una imagen a simple vista, por lo que procedí a buscar cuál era el nombre de esta técnica y llegué a “Steganography”. Luego, supuse que si escribía palabras clave, tales como “Stega...”, CyberChef me recomendaría herramientas relacionadas. Lo cual, así fue. Al principio probé con las herramientas que aparecían primero, pero ocupaban unas recetas un tanto complicadas o que requerían más información de la que yo poseía, por lo que busqué una más simple y llegué a una de las últimas herramientas, la cual se llamaba “Randomize Colour Palette”, la cual solamente necesitaba de una Seed para poder funcionar. Como no sabía qué Seed ocupar, solamente puse “1” y por suerte llegué a la respuesta que se detalla a continuación.

The screenshot displays the CyberChef web application interface. On the left, a sidebar lists various operations under 'Operations', 'Favourites', 'Data format', 'Encryption / Encoding', 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', and 'Code tidy'. The 'Randomize Colour Palette' recipe is highlighted in the 'Favourites' section. The main area shows the 'Recipe' panel with the 'Randomize Colour Palette' recipe selected, with a 'Seed' of '1'. The 'Input' panel shows a base64-encoded PNG image. The 'Output' panel displays the decoded image, which is a noisy, colorful pattern. The 'File details' panel on the right shows the file name 'CTF01.png', size '1,701,474 bytes', type 'image/png', and loaded status '100%'. The 'Output' panel also shows the decoded image with the text 'TICS413CTF01' visible at the bottom.

- Luego, al descubrir la clave para el PDF, pude acceder a la llave privada y pública dentro de este.

A continuación, no sabía muy bien qué hacer o qué herramienta ocupar, pero vi que en <https://linktr.ee/ticsuai> el archivo que poseía el PDF se llamaba “Llaves RSA con contraseña”, por lo que asumí que RSA podía ser un tipo de mecanismo de encriptación y lo busqué en CyberChef, a lo cual, tuve éxito y decidí ocuparlo para decodificar el archivo de las coordenadas iniciales.

The screenshot displays the CyberChef web application interface. On the left is a sidebar with a menu of operations categorized under 'Operations', 'Favourites', 'Data format', 'Encryption / Encoding', 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Operations' list includes 'Bacon Cipher Decode', 'Bacon Cipher Encode', 'Extract LSB', 'Extract RGBA', 'Randomize Colour Palette', and 'View Bit Plane'. The 'Favourites' section has a star icon. The 'Data format' section includes 'Public Key'. The 'Encryption / Encoding' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Public Key' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Arithmetic / Logic' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Networking' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Language' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Utils' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Date / Time' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Extractors' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Compression' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Hashing' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Code tidy' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The 'Forensics' section includes 'Public Key', 'Arithmetic / Logic', 'Networking', 'Language', 'Utils', 'Date / Time', 'Extractors', 'Compression', 'Hashing', 'Code tidy', and 'Forensics'. The main area is divided into three panels: 'Recipe', 'Input', and 'Output'. The 'Recipe' panel shows a list of recipes, with 'RSA Decrypt' selected. The 'Input' panel shows the raw bytes of the file 'CTF01-coordenadas-iniciales.dat'. The 'Output' panel shows the decoded coordinates: '-33.489742, -70.513682'. The 'File details' panel on the right shows the file name, size (128 bytes), type (unknown), and loaded status (100%).

Download CyberChef [Last build: A month ago - Version 10 is here!](#) [Read about the new features here](#) Options About / Support

Operations

- stega
- Bacon Cipher Decode
- Bacon Cipher Encode
- Extract LSB
- Extract RGBA
- Randomize Colour Palette
- View Bit Plane
- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time
- Extractors
- Compression
- Hashing
- Code tidy
- Forensics

Recipe

RSA Decrypt

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA...
-----END RSA PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQYAMIIBCgKCAQEA...
-----END PUBLIC KEY-----

Message Digest Algorithm
SHA-1

Randomize Colour Palette

Seed
1

Input

1505•B4YpF#b?Bx*gb•ÄYauVÄuclcöP ;?(*E+5KSD\$Nz•M"u•y•u•L@Cbcu•09c•OC„07c•504•0z"?6°100„Ü•••••
xciF8b•.Äsz00°•x3q•20x•20xPR••Q„Ëpü••TÄZv••?B8y"8

File details

Name: CTF01-coordenadas-iniciales.dat
Size: 128 bytes
Type: unknown
Loaded: 100%

Output

-33.489742, -70.513682

STEP Auto Bake

- Por último, solo quedaba cambiar las coordenadas y encriptar nuevamente el mensaje, creando un archivo .dat nuevo. Por lo que procedí a buscar algún lugar de interés en Google Maps y realizar el proceso de encriptación, para luego descargar un archivo .dat con el output obtenido.

Download CyberChef [Download](#) Last build: A month ago - Version 10 is here! Read about the new features here Options About / Support

Operations

- rsa
- RSA Sign
- RSA Verify
- RSA Decrypt
- RSA Encrypt
- CipherSaber2 Decrypt
- CipherSaber2 Encrypt
- Generate RSA Key Pair
- Parse User Agent
- Parse IPv6 address
- Parse ASN.1 hex string
- Resize Image
- Remove whitespace
- Compare SDEEP hashes
- From MessagePack
- Parse DateTime
- Parse IP range
- Parse IPv4 header
- Haversine distance
- Parse X.509 certificate
- Parse ObjectID timestamp

Recipe

RSA Decrypt

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAjAX1jomQyphaLvLLqPKChxku8nHR/0hSPBE9LL
oB1McY7
em4ovUoGT7t/7zQtD2QSA+D7T/ZeoJnV5cB1SgAx9w==
-----END RSA PRIVATE KEY-----

Message Digest Algorithm
SHA-1

Randomize Colour Palette

Seed
1

RSA Encrypt

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQYAMIIBCgKCAQEAjAX1jomQyphaLvLLqPKChxku8nHR/0hSPBE9LL
oB1McY7
em4ovUoGT7t/7zQtD2QSA+D7T/ZeoJnV5cB1SgAx9w==
-----END PUBLIC KEY-----

Encrytion Scheme
RSA-OAEP

Message Digest Algorithm
SHA-1

STEP **BAKE!** Auto Bake

Input

-27.112205, -109.353581

Output

*%csÜÜ•arP8hcsÜ•Ü•x06x0\$IEms1"É,ê•Ycs•cê%K•••GS:Ä•••p|Auu7êÄ••Éuu•"XX•••eÉ•"q•••êc•13%••ÜXnyö•r•K•"D%cs+ö•••ÉIt?9••••6(*diefU••
DUms1#•ÜçCcsügDßzQ1