UTN.BA UNIVERSIDAD TECNOLÓGICA NACIONAL FACULTAD REGIONAL BUENOS AIRES | Centro de e-Learning Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Módulo 4:

Ethical Hacking

Unidad 3:

Introducción sobre Criptografía

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Presentación

En esta tercera Unidad del módulo, nos introducimos en el mundo de la criptografía, para comprender el porqué de su uso en la protección de activos.

Conocerán varios algoritmos y procesos de cifrados, lo cual es conveniente aprender, dado que toda información de relevancia, debería estar cifrada.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Objetivos

Que los participantes logren…

- Aprender sobre los conceptos expuestos en el mundo del Hacking.

- Conocer las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y test de penetración (Pentesting), con una filosofía enfocada en la ética profesional.

- Comprender la importancia de usar cifrado seguro en aplicaciones, abordar vulnerabilidades y potenciales ataques y amenazas, así como la correcta concientización en los usuarios.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bloques temáticos

1. EL ABC de la Criptografía
2. Conceptos de sistemas criptográficos
3. Implementación de sistemas criptográficos
4. Ejercicios / Labs.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

El ABC de la Criptografía

¿Qué es la criptografía?

Criptografía (del griego κρύπτω *krypto*, «oculto», y γράφως *graphos*, «escribir», literalmente «escritura oculta») tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.

Definición de seguridad informática:

Es el proceso que se encarga de alterar un contenido de un mensaje, evitando que para personas no autorizadas el mismo sea ilegible, mediante técnicas de ocultación, sustitución y permutación, al igual que el uso de algoritmos matemáticos, ofreciendo confidencialidad e integridad.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

A través de la historia, se podrán encontrar distintos escenarios y modelos de criptografía utilizados.

Método Espartano

Se escribía el mensaje en una tira de cuero que se enrollaba en espiral sobre un bastón.

La tira desenrollada mostraba un texto sin ninguna relación con el texto inicial y sólo podía leerse volviendo a enrollar la tira en el bastón.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

En el ejemplo se puede notar cómo se va formando un nombre de una persona, lo cual sería imposible deducir si no se envolviera la tela en ese pedazo de madera.

Método Alemán

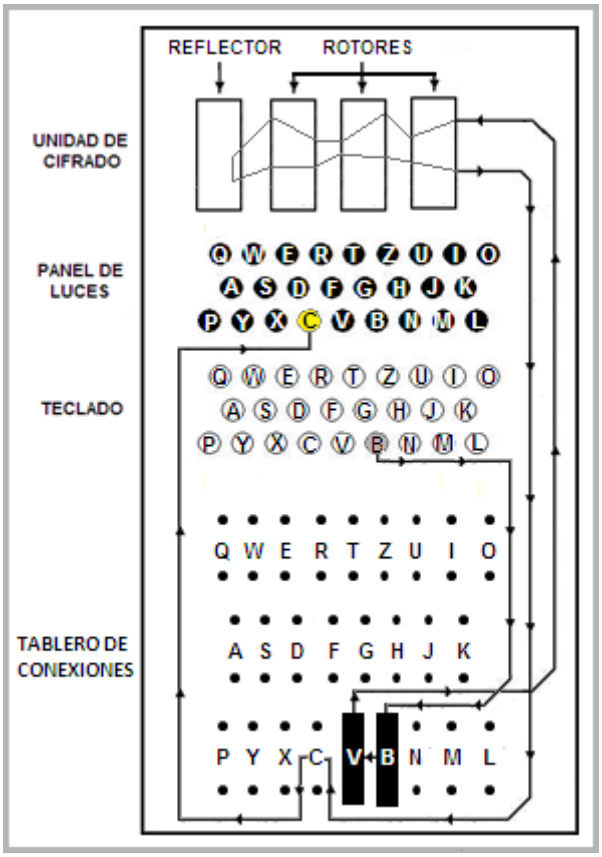
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Máquina alemana de cifrado ENIGMA, usada en la Segunda Guerra Mundial para el cifrado de los mensajes

La máquina contaba con un rotor, un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto.

Cada contacto de una cara está conectado o cableado a un contacto diferente de la cara contraria.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

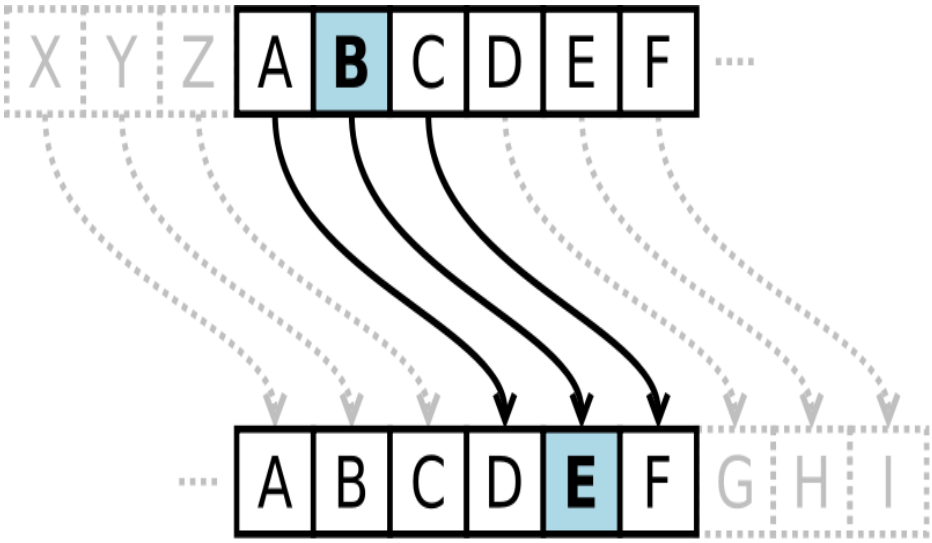


Por ejemplo, en un rotor en particular, el contacto número 1 de una cara puede estar conectado con el contacto número 14 en la otra cara y el contacto número 5 de una cara con el número 22 de la otra.

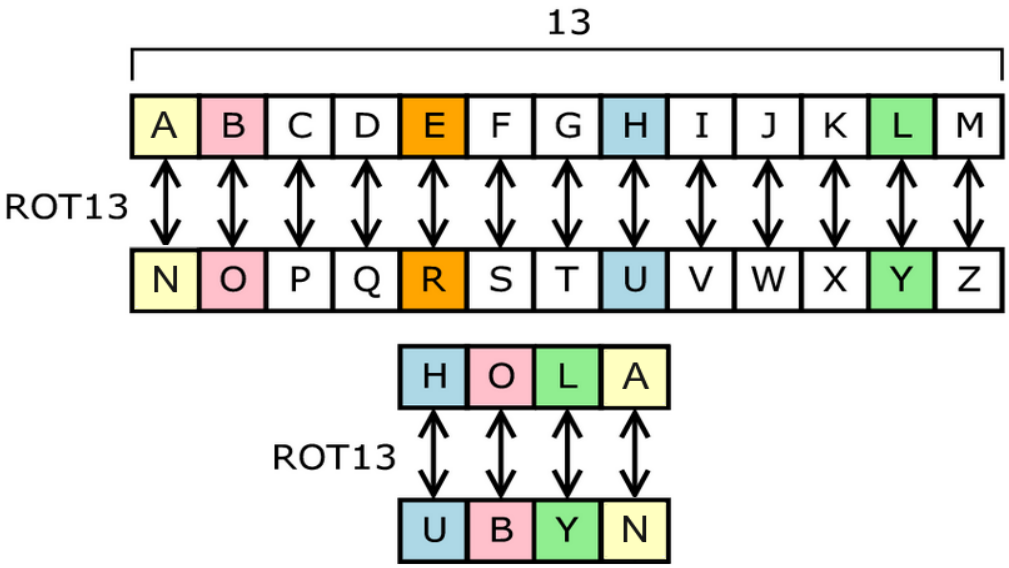
Recomendamos ver la película: **El Código Enigma o The Imitation Game**, donde se habla de esta máquina y se muestra en detalle su funcionamiento.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Método César



En este ejemplo se usa un desplazamiento (rotación) de tres espacios, así que una B en el texto original se convierte en una E en el texto codificado.

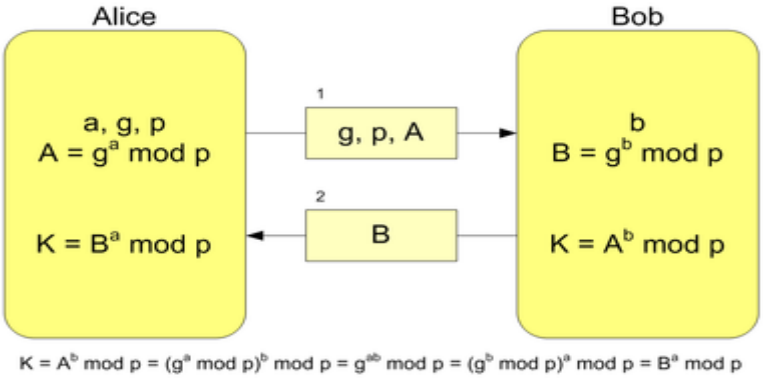


El cifrado César mueve cada letra un determinado número de espacios en el alfabeto, por ejemplo, en el dibujo anterior, vemos un ROT13 (13 desplazamientos de caracteres).

La letra A sería la N, la letra B sería la O, y así sucesivamente.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Conceptos de sistemas criptográficos



¿Y hoy con qué nos encontramos?

Términos como:

HASH – SSL – IPSEC - SSH – VPN – PGP

WEP / WPA / WPA2 / WPA3

Esteganografía y muchos más!!!!

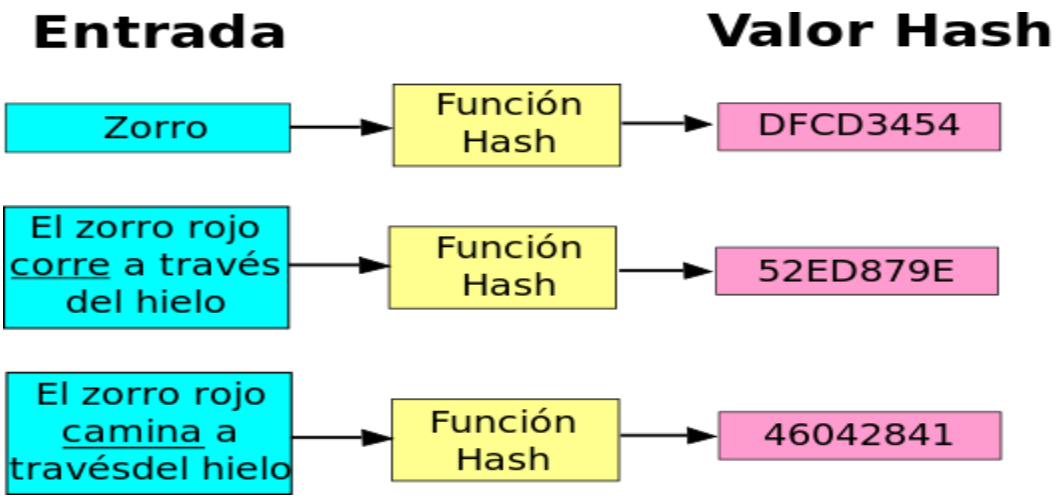
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

```
Standard commands
asn1parse         ca                ciphers           cms
crl               crl2pkcs7         dgst              dhparam
dsa               dsaparam          ec                ecparam
enc               engine            errstr            exit
gendsa            genpkey           genrsa            help
list              nseq              ocsp              passwd
pkcs12            pkcs7             pkcs8             pkey
pkeyparam         pkeyutl           prime             rand
rehash            req               rsa               rsautl
s_client          s_server          s_time            sess_id
smime             speed             spkac             srp
ts                verify            version           x509

Message Digest commands (see the `dgst' command for more details)
blake2b512        blake2s256        gost              md4
md5               rmd160            sha1              sha224
sha256            sha384            sha512

Cipher commands (see the `enc' command for more details)
aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       base64            bf
bf-cbc            bf-cfb            bf-ecb            bf-ofb
camellia-128-cbc  camellia-128-ecb  camellia-192-cbc  camellia-192-ecb
camellia-256-cbc  camellia-256-ecb  cast              cast-cbc
cast5-cbc         cast5-cfb         cast5-ecb         cast5-ofb
des               des-cbc           des-cfb           des-ecb
des-ede           des-ede-cbc       des-ede-cfb       des-ede-ofb
des-ede3          des-ede3-cbc      des-ede3-cfb      des-ede3-ofb
des-ofb           des3              desx              rc2
rc2-40-cbc        rc2-64-cbc        rc2-cbc           rc2-cfb
rc2-ecb           rc2-ofb           rc4               rc4-40
seed              seed-cbc          seed-cfb          seed-ecb
seed-ofb
```

HASH

Una función hash (H) es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M.



Es un conjunto de procesos que se aplican en un texto o archivo, generando un código verificador único, asegurando su integridad y originalidad

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Propiedades a tener en cuenta

ONE-WAY : deberá ser imposible obtener el texto original desde el resumen obtenido

LOW-COST: procesos rápidos y de escasos recursos

OUTPUT: de un texto con longitud variable se conseguirá uno de longitud fija

DETERMINISTIC: el texto original arrojará siempre el mismo resultado

NOT CONTINUOUS: modificando al menos 1 BIT, el HASH tendrá que cambiar al menos un 50%.

A continuación algunos de los algoritmos más conocidos

MD5*: es un algoritmo de* reducción criptográfico diseñado por el profesor Ronald Rivest del MIT, en el año 1992, mejorando sus antiguas versiones (MD2/MD4), utilizando una salida de resumen de 128 bits

SHA -1*: creado por la NSA en el año 1995, utilizando una salida de resumen de 160 bits*

SHA-2*:* es un conjunto de funciones criptográficas de hash (SHA-224, SHA-256, SHA-384, SHA-512) diseñado por la Agencia de Seguridad Nacional (NSA) y publicado en 2001 por el NIST

Ejemplo de uso:

Palabra utilizada para cifrar: "**SEGURIDAD**"

MD5: 9277c39ddaa8b2b2aa0c09597b9950f6

SHA-1: db7d633346ca9f454ac1e8d765c9a0eb93905f70

SHA-256:
EC37BDEDF2540E7899FB502CA50C0B9225396869B8BF3E06A4150F07828D33E4

SHA-512:
ED8FAA2DBED53E091D8428B5E82209545B31F70E594DCA7B6D20C79D6D987B1B7C2
2FDD55C665FB3792C594EEF4D8279D1BD51CE63AE56AF070AAF28CABB3D0D

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Cuanto mayor sea el grado de cifrado, el tamaño del HASH, podría aumentar notoriamente.

"El único sistema realmente seguro es el que está apagado, en una caja fuerte de titanio, enterrado en una bóveda de hormigón en el fondo del mar y rodeado por guardias de seguridad muy bien remunerados…. y aun así tampoco podríamos garantizarlo"

(de Eugene H. Spafford)

La fortaleza de estos algoritmos está en el tamaño de su clave

Cuanto mayor sea su clave, menor cantidad de repeticiones existirán, observe estos ejemplos:

4+4= 8

3+5=8

2+6=8

100*4/50=8

Ahora con algoritmos:

MD5 da una fortaleza de 2^128=3.4*10^38

SHA-1 da una fortaleza de 2^160=1.43*10^38

SHA-2 da una fortaleza de 2^512=1.34*10^154

Ejercicio Número 1 Unidad 1

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Seleccionar un solo ejercicio para exponer en el foro:

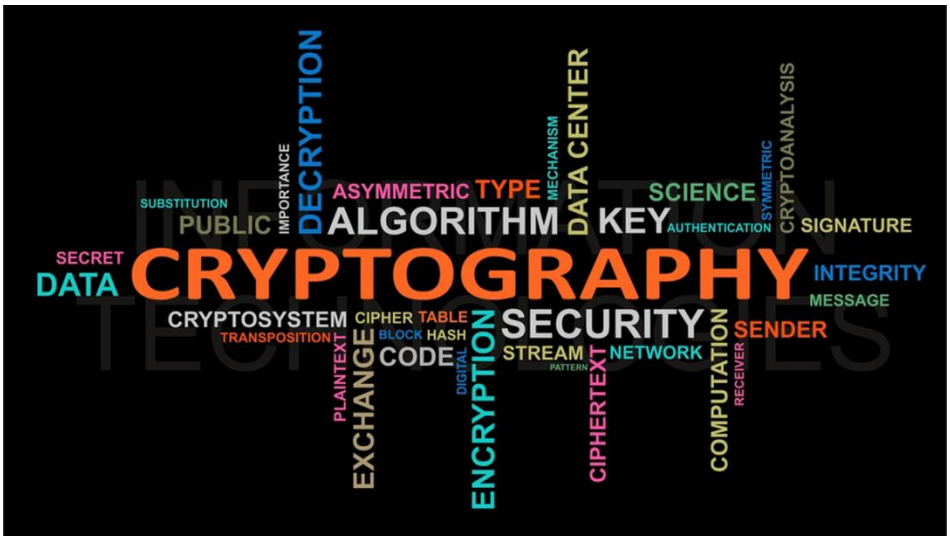
1- Buscar en Internet información sobre el "birthday problem" y exponer que piensan del mismo, aplicándolo en otros ejemplos.

2- Escribir 3 frases de no más de 10 palabras y pasarlas por los mecanismos de algoritmos, postearlo en el foro (al final de la unidad, links de ayuda)

3- ¿Te animas a inventar un tipo de cifrado? (en caso de afirmativo, exponer con ejemplos, pero siempre recordar que es importante demostrar el reverso para saber que descifrar correctamente.

Implementación de sistemas criptográficos

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Se escucha o se lee, “romper un algoritmo”, la pregunta es ¿se pueden romper o realmente se busca una vulnerabilidad?

Hay factores que un atacante tiene en cuenta, y es el procesamiento y uso de recursos a través de la potencia de los equipos, donde pueden jugar una mala pasada, por ejemplo en **MD5**.

Dispositivo: Pentium 4 (10000 interacciones por segundo)

5.9 días

Dispositivo: Intel CORE i7 (6.000.000 interacciones por segundo)

14.1 minutos

Dispositivo: Hardware utilizando GPU (70.000.000 interacciones por segundo)

73 segundos

Hay 2 tipos de categorías en los sistemas criptográficos.

SIMETRICO y ASIMETRICO

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

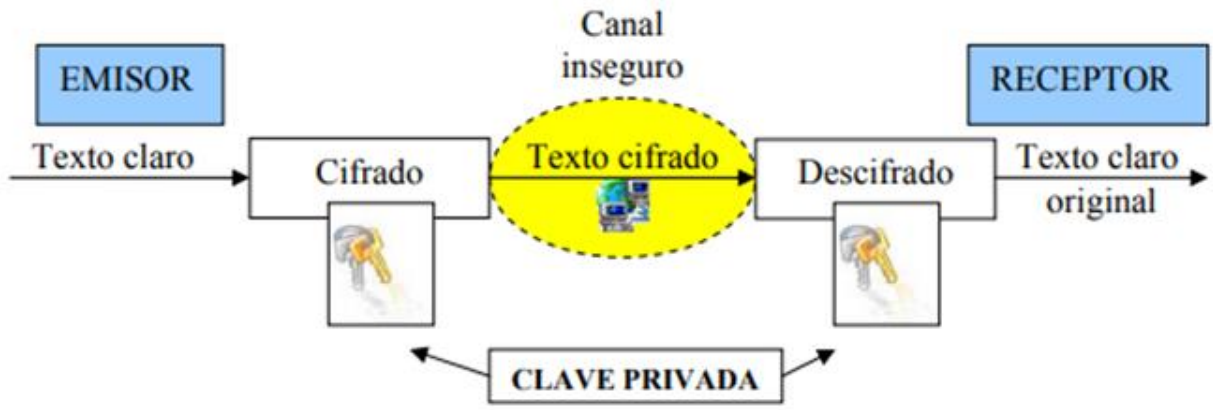
SIMETRICO: utiliza la misma clave para encriptar y desencriptar.

"SEGURIDAD" -> CLAVE -> TEXTO CIFRADO -> CLAVE -> "SEGURIDAD"

ASIMETRICO: utiliza una clave para encriptar y otra para desencriptar.

"SEGURIDAD" -> CLAVE 1 -> TEXTO CIFRADO -> CLAVE 2 -> "SEGURIDAD"

Implementación SIMETRICA



La clave es la misma para cifrar que para descifrar un mensaje, por lo que sólo el emisor y el receptor deben conocerla.

Se basan en operaciones matemáticas sencillas, por ello son fácilmente implementados en hardware.

Debido a su simplicidad matemática son capaces de cifrar grandes cantidades de datos en poco tiempo.

Existe una única clave compartida (SHARED KEY o SECRET KEY) para el proceso.

Sus cualidades son:

Se puede permitir un alto nivel de seguridad utilizando pequeñas claves.

La velocidad de procesamiento es muy alta.

El texto cifrado es compacto.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Las debilidades son:

Si aumentan la cantidad de usuarios, aumentara la cantidad de claves.

El sistema no permite una forma segura de transmitir la clave.

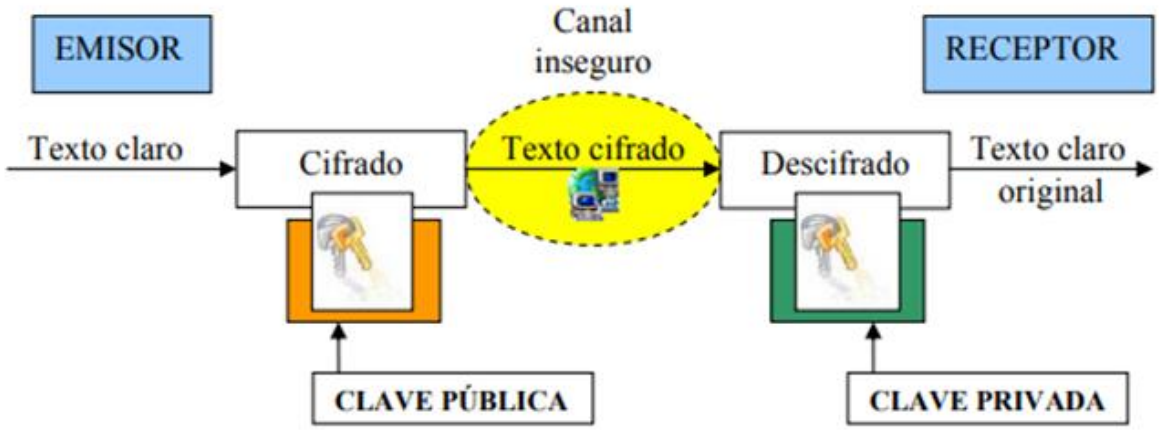
Y por último al ser una clave compartida, no es posible identificar al usuario del otro extremo.

Ejercicio Número 2 Unidad 1

¿Te animas a completar el siguiente ejemplo y subirlo al foro?

Implementación ASIMÉTRICA

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



En este caso hay 2 tipos de claves una pública y una privada, donde se encripta con una y se desencripta con la otra.

El emisor emplea la clave pública del receptor para cifrar el mensaje, este último lo descifra con su clave privada.

Se basan en operaciones matemáticas complejas.

Se ejecutan de 100 a 1000 veces más lento que los algoritmos simétricos.

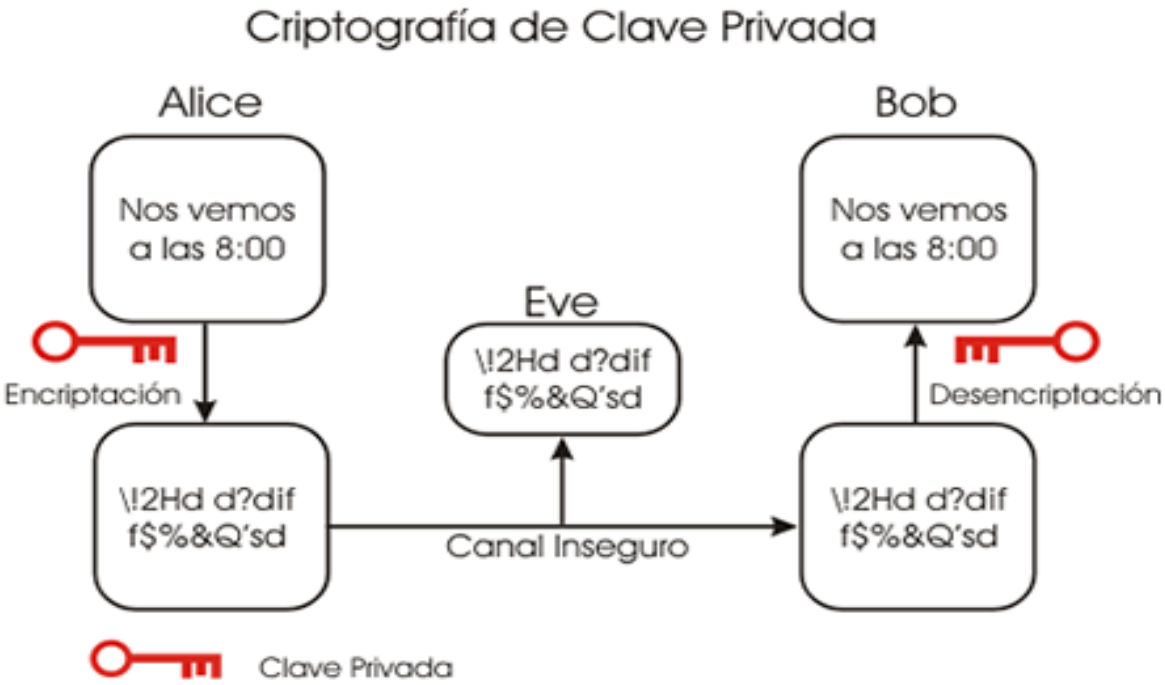
Debilidades: es muy lenta y consume muchos recursos.

Cualidades: Gestión y manejo de claves.

Seguridad en el intercambio de claves para abrir la sesión.

Incorpora concepto de firma digital y no repudio.

A continuación vemos un esquema de una técnica de Clave privada.



Aquí tienen algunos de los diferentes algoritmos que se implementan en sistemas, archivos, etc.

Sistema Simétrico	Sistema Asimétrico
DES	**SSH**
3DES	**SSL/TLS**
AES	**PGP/GPG**
WPA-WP2	**RSA**
BLOWFISH	**DIFFIE-HELLMAN**

Ejercicio Tools - LABS

VERACRYPT: https://veracrypt.codeplex.com/

VeraCrypt es una aplicación para cifrar y ocultar datos en el ordenador que el usuario considere reservados, empleando para ello diferentes algoritmos de cifrado como ***AES*** ***Serpent*** y ***Twofish*** o una combinación de los mismos.

También permite crear volúmenes virtuales cifrados en un archivo de forma rápida y transparente, se usa en reemplazo de TrueCrypt

GPG4WIN: **www.**gpg4win**.org**

Gpg4win (GNU Privacy Guard for Windows) es un software para cifrar ficheros y correos electrónicos

Mediante una máquina virtual, hacer uso de estas 2 herramientas, cifrando un directorio personal y realizando un cifrado de un archivo (ambos resultados, subirlos al foro exponiendo la captura imagen)

ATENCIÓN: **el uso de estas herramientas requiere mucho cuidado al trabajar fuera de una máquina virtual, por ende se recomienda tomar los recaudos necesarios.**

Aquel que requiera manuales de estas herramientas, puede solicitarlo por mensajería.

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy IMPORTANTE que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.

Bibliografía utilizada y sugerida

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU.

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México.

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España.

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU.

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learni the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

Link complementarios:

https://testssl.sh/

https://emn178.github.io/online-tools/base64_decode.html

http://www.counton.org/explorer/codebreaking/frequency-analysis.php

https://crackstation.net/

https://hashcat.net/hashcat/

http://www.tools4noobs.com/online_tools/decrypt/

http://lastbit.com/pswcalc.asp

https://www.onlinehashcrack.com

http://www.viruslist.com/sp/news

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)