

RSA

(Proyecto 2)

Canek García [kaan.ek@ciencias.unam.mx]



Parte 1


(Código)

Especificación general

Elaborar **un** programa con **tres** métodos principales: uno que **genere llaves** (acorde al criptosistema RSA), uno que **cifre** (obtener un criptograma usando el sistema de RSA) y otro que **descifre** (recuperar el texto en claro obtenido a partir del cifrado) texto en español (**Z/26** o **Z/27**), usando el **criptosistema de RSA**.



Detalles de la implementación

1. La función relacionada con **generar las llaves**, deberá buscar números primos primos **p** y **q** distintos y aleatorios de al menos **100 dígitos**.
 2. La función relacionada con **cifrado**, debe recibir como parámetros **N** y **e** (o hacer variables globales y referenciarlas) y el **texto en claro** que se va a cifrar (**m**).
 3. La función relacionada con **descifrado**, debe recibir como parámetros **N**, **d** y el **texto cifrado** (criptograma) en el punto anterior.
 4. Recuerden incluir un **método main** (método principal del programa) con pruebas a estas funciones.
 5. Pueden agregar todos los métodos auxiliares que requieran.
- 

Parte 2

(Reporte)

Especificación general

Utilizando las herramientas vistas en clase (**whois**, **nslookup**, **traceroute** y **nmap**), elaborar un breve reporte escrito con capturas de pantalla referente al flujo de escaneo de vulnerabilidades.



Detalles del reporte

- Para **whois**, incluir una captura de pantalla que muestre la siguiente información de algún dominio: fecha de creación, fecha de expiración, datos de contacto del administrador y direcciones IP de los DNS.
- Para **nslookup**, una captura de pantalla que muestre toda la información disponible (utilizando la opción type) de algún dominio: Nombre del host, dirección IP de los servidores DNS y demás detalles del servidor.



- Para **traceroute**, una captura de pantalla que muestre el trazado de ruta hacia el un servidor DNS (dominio cualquiera) y obtener información de algún servidor por donde viaja la comunicación con la herramienta **nslookup**.



Utilizar **nmap** para mostrar:

1. Barrido de red.
2. Escaneo de puertos TCP SYN.
3. Escaneo de puertos UDP.
4. Determinar el Sistema Operativo del objetivo.
5. Determinar servicios y versiones de puertos abiertos.
6. Evaluar reglas de firewall y determinar si hay puerto filtrados con TCP ACK
7. Investigar las categorías **NSE**: *auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version* y *vuln*. Describir brevemente cada categoría NSE de nmap, así como mostrar el uso de cada una en equipo objetivo de tu red local.
8. ¿Qué es un exploit?. Con base en el punto 5 y 7 buscar un exploit en la red que comprometa al sistema objetivo con las versiones vulnerables halladas (solo buscar el exploit, no es necesario ejecutarlo).



Notas

Notas adicionales

El código fuente puede ser entregado en: **C/C++** o **Python 3**. El reporte debe ser entregado en formato **PDF**.

Desarrollar el proyecto en equipos de **uno, dos** o **tres** integrantes.

Documentar el código fuente e incluir el nombre completo de los integrantes en el método main del programa, así mismo como en el reporte escrito.

Enviar el código y el reporte el día **8 de noviembre de 2022**.

Enviar el código fuente y reporte por medio de la plataforma **ClassRoom**. (al menos un integrante, pero de preferencia todos los miembros del equipo sin importar que se repita esta entrega).

