Reglamento de Prácticas
Facultad de Ciencias
Criptografía y Seguridad

José de Jesús Galaviz Casas
galaviz@ciencias.unam.mx

Edgar Omar Arroyo Munguía
omar.am@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

29 de Enero 2020

1. Funcionamiento general de las prácticas.

Durante todo el curso se trabajará con Python3 con la herramienta *pytest*, que debió de haber sido instalado con pip3 y basta con ejecutar el comando *pytest nombre.py* una vez que el script correspondiente haya sido completado.[1]

Siempre que una llave no sea apta para que se realice un cierto cifrado, se deberá de levantar la excepción *CryptographyError*. En todas las prácticas de criptografía clásica, se le da la opción al usuario de escoger una llave, si éste no la especifica, entonces el programa debe de generar automáticamente las llaves correspondientes, obviamente, una llave correcta.

2. Evaluación de prácticas

Las prácticas se podrán entregar a lo más en parejas y se deberá de subir a la plataforma en la actividad correspondiente como:

$$ApPat_1 ApMat_1 ApPat_2 ApMat_2 n.zip$$

Con los apellidos correspondientes y en orden alfabético con respecto al apellido paterno, es decir, en mi caso, si entregara con alguien que se apellide Mota Méndez, debemos de entregar la práctica 1 como *FongBaezaMotaMendez1.zip*.

En caso de que el grupo no sea un número par, se permitirá hacer equipos de 3, pero se preguntará a los 3 individuos sobre el funcionamiento del código, no la explicación del algoritmo y en cuyo caso, todos deberán estar presentes, cosa que no pasará en caso de que alguien decida entregar la práctica de manera individual o en parejas. Si esto llegara a pasar, se deberá fijar un nombre del equipo y entregar las prácticas de la manera:

$$NombreEquipo\_n.zip$$

[1] Se escogió Python3 por su versatilidad de lenguaje y la capacidad para manejar enteros grandes o *BigInts* de manera nativa

Se aceptarán prácticas a destiempo pero cada día que pase, es un punto menos en la evaluación de la misma, hasta llegar a 5, después de 5 días, ya no se aceptará esa práctica.

En caso de detectar copias de prácticas, todos los individuos o equipos involucrados, se anulará con 0 la práctica y para las prácticas siguientes se les hará entrevista respecto a los funcionamientos de los códigos de las prácticas siguientes.

Si a un equipo se le entrevista acerca del código, influirá en su calificación final de esa práctica. Las preguntas se hacen al azar y cualquier miembro del equipo deberá de ser capaz de responder, en caso de que alguien interfiera en la respuesta que se le hace a la persona, esto también afectará el resultado de la evaluación.

Es completamente válido, utilizar código de Internet que ya esté implementado, siempre y cuando, éste no resuelva como tal la práctica, es decir, no se vale copiar los algoritmos de cifrado y descifrado de otro lado, pero se vale que utilicen el código del algoritmo extendido de Euclides, por decir un ejemplo, para que esta regla sea válida, tienen que agregar código personal, decir de dónde sacaron el código (en la documentación o comentado) y para qué lo están utilizando, obviamente, también es completamente válido, usar cualquier biblioteca ya implementada siempre y cuando no infrinja con lo estipulado anteriormente.

No hay necesidad de entregar todo en un solo archivo, se recomienda altamente que modulen el código, ya que esto hará más fácil la implementación de los algoritmos, sin modificar el código base que se les entrega.

El código deberá estar correctamente documentado y entregar junto con el comprimido, un README con los nombres de los integrantes.

3. Prácticas

El curso constará de 8 prácticas en total, implementando los aspectos más importantes de la Criptografía tanto clásica como moderna, así como analizar qué tan eficientes son las heurísticas de criptoanálisis para cada criptosistema.

Las prácticas que se llevarán a cabo en el curso, son:

1. Cifrado de XOR, César y Afín.
2. Cifrado de Vigenere y Hill.
3. Criptoanálisis clásico.
4. Test de primalidad de Miller-Rabin y Wilson.
5. Intercambio de llaves de Diffie-Hellman.
6. El criptoalgoritmo de RSA.
7. ECIES simplificado.
8. Algoritmo de factorización de Lenstra.

4. Proyecto final

Este proyecto final es de manera completamente opcional pero las personas que lo implementen de manera correcta y completa, serán acreedores a 2 puntos extra sobre calificación final en el laboratorio.

El proyecto final, consta de crear un servicio de mensajería, de manera local pero con las comunicaciones cifradas usando cualquier criptosistema[2]. Se considerarán como puntos extras quienes utilicen un criptosistema que no haya sido enseñado en clases de laboratorio, posteriormente se elaborará un PDF con todas las especificaciones del mismo.

5. Sesiones de laboratorio

Durante estas sesiones, se cubrirán aspectos de seguridad del curso, con temas como seguridad en la web, creación de contraseñas seguras bajo criptografía clásica, funcionamiento y uso de protocolos seguros (IPSec, HTTPS, SSH, ...), así como detección de intrusos e introducciones al *firewall* y mecanismos básicos de defensa ante ataques, autenticación en línea y firma digital. Sin embargo también se cubrirán dudas respecto a las prácticas del laboratorio y proyecto, además de aclaraciones respecto a calificaciones y las entrevistas para los equipos de 3 integrantes a los equipos correspondientes, implicando que solo los equipos de 3 integrantes su asistencia al laboratorio sea obligatoria pero libres de abandonar el salón una vez concluida la misma.

6. Notas finales

Todas las dudas respecto a las prácticas o aclaraciones, deberán de ser mandadas por correo al ayudante de laboratorio con el asunto [CyS 2020-2].

Estas reglas pueden verse modificadas a lo largo del semestre por parte del profesor titular.

7. Bibliografía

[1] William Stallings. *Cryptography and network security principles and practice*. Pearson, Fifth Edition, New York, 2011.

[2] Lawrence C. Washington *Elliptic Curves, number theory and cryptography* Chapman & Hall, Second Edition, Maryland, 2008.

[3] Trevor D. Wooley *A Complete Course on Number Theory* Bristol University, First Edition, Bristol, 2019.

[4] Jonathan Katz and Yehuda Lindell *Introduction to Modern Cryptography* CRC Press, First Edition, Washington D.C., 2007.

[2] Aplican restricciones, es decir, criptografía clásica desde César hasta One-Time pad, no cuenta