Universidad Técnica Federico Santa María

Criptografía y Seguridad en la Información (TEL-252)

Laboratorio 1: Introducción a SageMath

Profesor(a): Luis Lizama

Ayudante: Diego Maldonado

Objetivos

El objetivo de esta práctica es que los estudiantes se familiaricen la plataforma CoCalc para implementar y comprender distintos métodos de cifrado clásicos, así como técnicas para descifrarlos, utilizando SageMath.

Introducción

Contexto: Esta práctica se enfoca en la implementación del cifrado César, usando SageMath. Estos conceptos son fundamentales en el estudio de la criptografía, y su comprensión es crucial para analizar y romper sistemas criptográficos simples.

Metodología

1. Implementar funciones de cifrado y descifrado para el cifrado César.
2. Realizar un ataque de fuerza bruta sobre textos cifrados.

Ejercicios Prácticos

Parte 1

El objetivo de esta sección es implementar funciones que pueden ser útiles para los algoritmos de cifrados clásicos.

a) Implementa una función que retorne "True"si y sólo si el caracter 'c' pertenece al alfabeto inglés.

b) Implementa una función que convierta un caracter simple en su valor numérico correspondiente (a=0, b=1, c=2, ... , z=25)

c) Implementa una función que retorne el caracter correspondiente a 'x mod 26'.

Parte 2

El propósito de esta pregunta es implementar funciones de Sage para el cifrado/descifrado con el cifrado César, así como ataques.

a) Implementa funciones de cifrado/descifrado en Sage que tomen una clave (como un entero en 0, 1, 2, ..., 25) y una cadena de texto. La función solo debe operar sobre los caracteres 'a', 'b', ..., 'z' (tanto en mayúsculas como en minúsculas) y debe dejar cualquier otro carácter sin cambios.

b) Implementa una función que realice un ataque de fuerza bruta sobre un texto cifrado; debe imprimir una lista de las claves y los desciframientos asociados. También debe tomar un parámetro opcional que tome una

subcadena y solo imprima posibles textos planos que contengan ese desciframiento.

c) Muestra la salida de tu función de cifrado (parte a) en los siguientes pares (clave, texto plano):

- k = 6, texto plano = "Get me a vanilla ice cream, make it a double."
- k = 15, texto plano = "I don't much care for Leonard Cohen."
- k = 16, texto plano = "I like root beer floats."

d) Muestra la salida de tu función de descifrado (parte a) en los siguientes pares (clave, texto cifrado):

- k = 12, texto cifrado = "nduzs ftq buzq oazqe."
- k = 3, texto cifrado = "fdhvdu qhhgv wr orvh zhljkw."
- k = 20, texto cifrado = "ufgihxm uly numnys."

e) Muestra la salida de tu función de ataque (parte b) en los siguientes textos cifrados; si se especifica una palabra clave opcional, pásala a tu función de ataque:

- texto cifrado = 'gryy gurz gb tb gb nzoebfr puncry.', palabra clave = 'chapel'
- texto cifrado = 'wziv kyv jyfk nyve kyv tpdsrcj tirjy.', palabra clave = 'cymbal'
- texto cifrado = 'baeeq klwosjl osk s esf ozg cfwo lgg emuz.', sin palabra clave

Entrega del Reporte

Fecha de Entrega: 18/08/2024

Formato del Reporte:

1. Introducción
   - Contexto.
   - Objetivos de la práctica.
2. Metodología
   - Descripción de los pasos realizados en el laboratorio.
   - Detalle de los ejercicios ejecutados.
3. Ejercicios prácticos
   - Ejercicios completados del laboratorio.
   - Descripción y resultados de cada ejercicio.
4. Conclusiones
   - Síntesis de los resultados obtenidos.
   - Reflexiones finales sobre el aprendizaje.
5. Referencias
   - Citas bibliográficas en formato IEEE.

Referencias

Bibliografía:

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.