Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

Israel Alejandro Herrera Araiza

Nombre del curso:

Controles Criptograficos De Seguridad

Actividad:

Fase 1 Criptografía métodos de cifrado Clasicos.

Fecha:

24/05/2024

Introducción

La criptografía parte de la base de la teoría de la información cuyo principal autor fue Claude Shannon, la teoría de la información introduce un conjunto de métodos y estrategias para determinar la seguridad de un criptosistema, haciendo uso de la entropía(H) las definiciones de redundancia y mecanismos de confusión que son en buena parte el eje central del cual gira toda la criptografía, Shannon definió una prueba para comprobar si un criptosistema es seguro, el cual es que la cantidad de información recopilada de un conjunto de **criptogramas (mensajes inteligibles)** y un conjunto de mensajes sea cero es decir que la incertidumbre sea infinita, o en otras palabras y como lo menciona (LOPEZ, 2011) "que el criptosistema no permita que dado un mensaje cifrado, al variar la distribución de probabilidad sobre M hara que unos mensajes mas probables que otros y que por siguiente unas claves de cifrado sean mas probables que otras esto significa que podemos obtener una clave mucho mas frecuente que otras la cual nos permitirá romper el cifrado"

Shannon también menciona que un criptosistema debe ser seguro si su cardinalidad de espacio de claves es igual al mensaje que se busca asegurar, un ejemplo, es el algoritmo ***one-time-pad***.

Así mismo planteo la definición de **entropía** así mismo como el entropía condicionada, se puede declarar que la definición de entropía es nada más y nada menos que como lo define (LOPEZ, 2011) " el **número medio de bits** que necesitamos para codificar cada uno de los estados de la variable"

Sin embargo, una definición más amplia puede ser la aleatoriedad o el grado de imprevisibilidad de los datos utilizados para crear claves criptográficas, la entropía es importante debido a que la cantidad de información que se aporta por un mensaje es proporcional a su nivel de ocurrencia, es decir, un mensaje bastante común nos puede aportar una cantidad ínfima de información en comparación con un mensaje poco común, el término mensaje es utilizado para simplificar el hecho de que estamos en realidad hablando de lo que serían variables o conjuntos de valores, la entropía pues y según lo pospone López, no es más que la multiplicación del logaritmo con base 2 del inverso de la probabilidad de ocurrencia de un determinado caso por la probabilidad de ocurrencia de este mismo caso.

Una vez definido lo que es la entropía hace falta preguntarnos, ¿Qué es la entropía condicionada?, la entropía condicionada no es más que en este caso dadas dos variables Como por ejemplo Z y e el hecho de conocer el valor de alguno de estas dos variables reducirá el grado de incertidumbre que tenemos sobre la otra variable, otro concepto importante que hace falta mencionar que nos declara López es el hecho de la redundancia, la redundancia como tal es el grado en el que nosotros podemos determinar o inferir una información en base al contexto de un mensaje, es posible utilizar la redundancia para que nosotros podamos de forma automática realizar una estimación de si una cadena de símbolos corresponden o no a un lenguaje determinado, como expone López, Ahora bien el concepto de redundancia puede ser utilizado tanto en el contexto de los algoritmos de compresión de datos como con los códigos de redundancia cíclica, sin embargo, en el contexto de la criptografía, es un mecanismo recurrentemente usado para poder explotar o conocer la información de un mensaje a partir de una determinada clave, esto quiere decir que dependiendo de una clave dada podemos asignarle una probabilidad de que un mensaje sea el que esté protegiendo, esto ocurre por ejemplo con los ataques de **Rainbow tables**.

Técnicas de ocultamiento de información empleadas por los criptosistemas

Según lo menciona Lopez fundamentado en la teoría de Shannon existen 2 técnicas básicas de ocultamiento de información, estas técnicas son un concepto clave de cualquier mecanismo de cifrado incluyendo la criptografía clásica.

1) **Confusión:** Trata de ocultar la relación entre el texto claro y el texto cifrado. Recordemos que esa relación existe y se da a partir de la clave k empleada, puesto que si no existiera jamás podríamos descifrar los mensajes. El mecanismo mas simple de confusión es la sustitución, que consiste en cambiar cada ocurrencia de un símbolo en el texto claro por otro. La sustitución puede ser tan simple o tan compleja como queramos.
2) **Difusión**: Diluye la redundancia del texto claro repartiéndola a lo largo de todo el texto cifrado. El mecanismo mas elemental para llevar a cabo una difusión es la transposición, que consiste en cambiar de sitio elementos individuales del texto claro. (LOPEZ, 2011).

La criptografía clásica no solo consta del uso de este mecanismo de cifrado, sino que también involucra la definición del **cifrado simétrico**, si bien en el campo de la criptografía podemos definir tanto un cifrado simétrico como asimétrico, la criptografía clásica únicamente se considera aquella anterior al estallido de la segunda guerra mundial y el uso de la maquina enigma,

Una definición que podemos llegar en base a lo mencionado por Schneier, B. (1996) es:

Aquel criptosistema donde tanto el remitente como el receptor deben compartir la misma clave para cifrar y descifrar los mensajes. Este tipo de cifrado depende completamente de la clave, ya que el algoritmo puede ser conocido públicamente

Motivación para el uso de Criptografía Clásica

La criptografía clásica nació por la necesidad de mantener la confidencialidad de las comunicaciones, ya sea en tiempos de guerra o en transacciones comerciales privadas. Desde la antigüedad, las civilizaciones buscaban maneras de ocultar sus mensajes para que no fueran entendidos por enemigos o terceros no autorizados. La criptografía era, por tanto, una herramienta clave para la seguridad y la privacidad.

Problemas Principales de la Criptografía Clásica

1. **Seguridad limitada por la longitud de la clave**: Los cifrados clásicos pueden ser vulnerables a ataques de fuerza bruta, donde un atacante prueba todas las combinaciones posibles de claves hasta encontrar la correcta. A medida que el poder de cómputo ha aumentado, las claves cortas pueden ser fácilmente descifradas
2. **Vulnerabilidad a ataques de criptoanálisis**: La criptografía clásica, especialmente los cifrados por sustitución y transposición, es susceptible a técnicas de criptoanálisis, como el análisis de frecuencias, que permite deducir el mensaje original a partir de patrones en el texto cifrado
3. **Distribución y manejo de claves**: Un desafío clave en la criptografía clásica es el manejo de las claves. Para que dos personas se comuniquen de manera segura, deben acordar y compartir una clave de manera segura. En ausencia de medios electrónicos seguros, este proceso es altamente vulnerable a interceptaciones

Para definir el las principales máquinas de cifrado utilizadas en la criptografía clásica debemos profundizar en la definición de lo que es una máquina de cifrado, Según lo define Bruce Schneier, una **máquina de cifrado** es un dispositivo mecánico o electromecánico que realiza el cifrado de mensajes de manera automatizada, implementando métodos criptográficos como sustitución o transposición. Estas máquinas utilizan configuraciones internas, como rotores, para sustituir o transponer caracteres del texto plano y producir el texto cifrado.

Principales máquinas de cifrado utilizadas:

1. **Enigma**: Fue la máquina de cifrado más conocida, utilizada por los alemanes durante la Segunda Guerra Mundial. Consistía en un conjunto de rotores que intercambiaban letras según configuraciones cambiantes. Aunque era avanzada para su tiempo, fue descifrada por los Aliados, con ayuda de criptógrafos polacos y británicos.
2. **Máquinas de rotores**: Estas máquinas, como la Enigma, utilizaban rotores que sustituían letras basándose en permutaciones complejas. Cada rotor tenía 26 posiciones (correspondientes al alfabeto) y se movía de manera secuencial con cada letra cifrada, creando una secuencia de cifrado que cambiaba constantemente.
3. **ADFGVX**: Fue utilizada por el ejército alemán durante la Primera Guerra Mundial. Combinaba cifrado por sustitución y transposición, haciendo uso de un cuadro

polialfabético para generar una secuencia compleja de cifrado. Esta máquina también fue descifrada por criptógrafos aliados.

Mecanismos de Cifrado clásicos:

Como sabemos los mecanismos de cifrado con frecuencia hacen uso de diferentes mecanismos para ocultamiento de información, una de ellas es la técnica de confusión por sustitución

Esto puede ser que se realice de forma independiente de la posición del mensaje, es decir, generar una equivalencia dependiendo un carácter específico (conocido como cifrado **monoalfabetico**)

O bien depender de un desplazamiento para poder generar la confusión (conocido como un cifrado **polialfabetico**) (este último según menciona Schneier también puede ser un tipo de cifrado que emplee otros cifrados de sustitución para su funcionamiento) , según lo describe Schneier la criptografía clásica, en conciso las técnicas de confusión por sustitución más comunes aplicadas además del método **monoalfabetico** y sustitución **polialfabetica**, existen otros mecanismos como:

- **Substitucion homofonica:** este tipo de técnica se caracteriza por utilizar un conjunto de caracteres que pueden corresponder a múltiples caracteres como explica Schneier.
- **Substitucion poligramica:** este tipo de técnica consiste en agrupar o **tokenizar** las palabras y en base a ello cifrarlas

El cifrado cesar, el cual, es muy similar al actualmente conocido como **ROT13** era un tipo de cifrado que consistía en sumar un 3 a la posición de un determinado carácter es decir generar un desplazamiento de este. Como se define en (LOPEZ, 2011) la fórmula utilizada para realizar este tipo de cifrado es:

$$c = (m + 3)\ mod\ 26$$

Esto en código podemos verlo de la siguiente forma considerando el uso de **ASCII**:

```
i = input("caracteres: ").split()
print("texto cifrado:" + "".join([ chr(ord(c) + 3)  for x in i for c in x]))
```

otro cifrado clasico que podemos encontrar es el cifrado vigenere, el cual constitye un tipo de cifrado polialfabetico, que consiste en el uso de un conjunto de símbolos que actúan como clave la cual se repetirá en multiples tiempos dependiendo si el texto a cifrar es más grande que la clave, a esto se le denomina como el periodo de cifrado, dependiendo de si el mensaje era mas largo que la clave utilizada es posible el reutilizar la clave multiples veces como si se tratara de concatenar la clave una n cantidad de tiempos para que iguale el largo del mensaje a cifrar, sin embargo esto ocasiona el inconveniente de que un determinado carácter del mensaje será correspondido con un determinado carácter de la clave multiples veces (dependiendo de si la clave es inferior al largo del mensaje (también conocido en este caso como la cardinalidad del conjunto M)), Schneier menciona que aquellos algoritmos clásicos con un periodo de cifrado más largo con frecuencia eran más difíciles de romper que los cifrados con periodos cortos, sin embargo, con el avance de la tecnología es actualmente relativamente sencillo romper esta clase de cifrados, la siguiente formula presentada por (LOPEZ, 2011) describe el funcionamiento de este tipo de cifrado:

$$E_k(m_i) = (m_i + k_i) * mod\ (n)$$

Desglosemos esta ecuación paso por paso

El conjunto m significa un conjunto de caracteres o en este caso de números codificados según un estándar de codificado, como puede ser **ASCII**, K corresponde a cada carácter del conjunto de la clave, n corresponde a la cardinalidad del conjunto de caracteres existentes en el abecedario, si consideramos el uso de **ASCII** n correspondería a un valor de 255, se realiza la operación modular para cerciorarse que no supere el rango de caracteres mayor de 255, es decir, si la suma da un número mayor a 255, la multiplicación con la operación modular automáticamente "atenuara" ese digito y lo colocara en un rango que sea admisible para el estándar de codificación usado, en realidad esta es una propiedad de la aritmética modular o como lo describe Lopez la también llamada "**aritmética de reloj**", debido a que, podemos realizar operaciones en un conjunto reducido de datos finitos y generalmente pertenecientes a los números reales, de hecho podríamos decir que el cifrado **Vigenère** no es más que una simple aplicación de la propiedad de la adición en la aritmética modular, con un conjunto variable de datos (en este caso el estándar de codificación de caracteres), en python esta ecuación puede ser codificada como:

```
keygen = lambda key,msj: key * (len(msj)//len(key)) +
key[:len(msj)%len(key)]
x = lambda abc,key,msj:"".join([abc[(ord(x)+ ord(y))%len(abc)] for x,y in
zip(msj,keygen(key,msj))])
```

finalmente, uno de los últimos tipos de cifrado clásicos que podemos nombrar es el cifrado **escitalo** utilizado por los espartanos para evitar la captura de información, este cifrado hace uso de la técnica de transposición, es decir, una forma de realizar la difusión de la redundancia de un mensaje que se encuentra íntimamente ligada a todos los lenguajes usados, este cifrado básicamente consistía en utilizar una matriz de permutación la cual no hacía más que solo alterar el orden de los caracteres que conforman un texto dado.

Conclusiones

A lo largo de la historia, la **criptografía clásica** ha sido esencial para proteger la confidencialidad de las comunicaciones en diversos contextos, tanto bélicos como comerciales. Los sistemas criptográficos iniciales, como el cifrado de sustitución y transposición, establecieron los fundamentos de la criptografía moderna.

Uno de los enfoques principales de la criptografía clásica fue el uso de **algoritmos de cifrado simétrico**, donde tanto el remitente como el receptor compartían una misma clave. Aunque este método fue efectivo en su momento, presentaba desafíos significativos en la distribución segura de las claves y era vulnerable a ataques de criptoanálisis, como el análisis de frecuencias.

La introducción de **máquinas de cifrado**, como la Enigma y otras máquinas de rotores, representó un avance notable en la automatización del cifrado de mensajes. Sin embargo, la historia demostró que incluso estas máquinas podían ser vulnerables a los criptoanalistas, como se evidenció durante la Segunda Guerra Mundial.

Los **métodos de cifrado clásicos**, como el cifrado de César, el cifrado Vigenère y el cifrado homofónico, proporcionaron soluciones de seguridad básicas. No obstante, con el tiempo, estos métodos se volvieron vulnerables a técnicas de criptoanálisis avanzadas. Aunque algunos mecanismos, como el One-Time Pad, ofrecían una seguridad teórica perfecta, su implementación práctica presentaba complicaciones debido a la distribución y manejo de claves.

A pesar de los avances en los métodos de cifrado, la **criptografía clásica** enfrentaba limitaciones importantes, como la longitud de las claves y la vulnerabilidad ante ataques de fuerza bruta. Con el incremento del poder computacional, muchos de los algoritmos clásicos se volvieron inseguros.

En resumen, la criptografía clásica sentó las bases para el desarrollo de sistemas más robustos. Sin embargo, las limitaciones inherentes a estos métodos llevaron a la creación de técnicas modernas más complejas y seguras, adaptadas a los desafíos tecnológicos actuales.

Bibliografía

LOPEZ, M. J. (2011). *Criptografia y Seguridad en Computadores.* Andalucía: UNIVERSIDAD DE JAEN.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). John Wiley & Sons.

Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.