INTRODUCCIÓN A LA CRIPTOGRAFÍA

-Cutipa Mamani Joaquin Esteban
-Blanco Ramirez Aaron Alonso
-Morales Umasi Carlos Gabriel
-Palo Zúñiga José Nicolás
-Ramos Medina Cristian
-Salas Rondon Joan Patricio

La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura.

El primer sistema criptográfico del que se tiene constancia es la Excítala. Este sistema data del siglo V a.m. y era usado en Esparta. El sistema consistía en dos varas del mismo grosor, una en poder del emisor y la otra del receptor. Cuando el emisor quería enviar un mensaje, este, enrollaba una cinta en su vara y escribía el mensaje. De este modo al desenrollar la cinta el mensaje era ilegible. Al recibir el mensaje, el receptor enrollaba la cinta en su vara, y de este modo podía leer el mensaje. Los primeros sistemas de cifrado estuvieron ligados a campañas militares dadas la necesidad de evitar que el enemigo obtuviese los movimientos de las tropas al interceptar mensajes.

1. División de la criptografía

1.1 Encriptación simétrica

Debido a su mayor velocidad, la encriptación simétrica se emplea de forma generalizada para la protección de información en muchos sistemas de computación modernos. El Advanced Encryption Standard (AES), por ejemplo, es empleado por el gobierno de los Estados Unidos para encriptar información clasificada y sensible. El AES reemplazó a su predecesor, el Data Encryption Standard (DES), desarrollado en la década de 1970 como estándar de encriptación simétrica.

1.2 Encriptación asimétrica

La encriptación asimétrica puede aplicarse en sistemas en los que muchos usuarios pueden requerir la encriptación y desencriptación de mensajes o conjuntos de datos, especialmente, cuando la velocidad y la potencia computacional no son preocupaciones primarias. Un ejemplo de este tipo de sistemas es el correo electrónico cifrado, en el que una clave pública puede ser empleada para

encriptar un mensaje, y una clave privada para desencriptarlo.

2. Usos de la criptografía

La criptografía cuenta con 3 usos: Cifrar, autenticar y firmar.

Cifrar:

Como ya hemos dicho, siempre hay cierta información que no queremos que sea conocida más que por las personas que nosotros queramos. En esto nos ayuda el cifrado. Cifrando un mensaje hacemos que este no pueda ser leído por terceras personas consiguiendo así la tan deseada privacidad.

Autenticación:

Otra de las necesidades que surgen con la aparición de internet es la necesidad de demostrar que somos nosotros y que el emisor es quien dice ser. Un método de autenticación puede ser el propio cifrado. Si ciframos un mensaje con una clave solo conocida por nosotros, demostrando que somos quien decimos ser, el receptor podrá constatar nuestra identidad descifrandolo. Esto se puede conseguir mediante clave simétrica (el receptor tiene que estar en posesión de la clave empleada) o usando clave asimétrica en su modo de autenticación

Firmar:

Firmados los trámites que podemos realizar hoy en día a través de internet se hace necesaria la aparición de la firma digital. Igual que firmamos un documento, la firma digital nos ofrece la posibilidad de asociar una identidad a un mensaje. Para la firma digital se utiliza clave asimétrica (dos claves una privada y otra pública).Lo que se cifra con la clave privada (que solo nosotros conocemos) sólo se puede descifrar con la pública. De esta forma al cifrar con nuestra clave privada demostramos que somos nosotros

Criptografía simétrica: DES y AES

La criptografía Simétrica es un método criptográfico mono clave, esto quiere decir que se usa la misma clave para cifrar y descifrar. Esto supone un grave problema a la hora de realizar el intercambio entre el emisor y el receptor, dado que si una tercera persona estuviese escuchando el canal podría hacerse con la clave, siendo inútil el cifrado.

DES:

El algoritmo DES (Data Encryption Standard) es un algoritmo de cifrado desarrollado por la NSA a petición del gobierno de EEUU bajo la presión de las empresas por la necesidad de un método para proteger sus comunicaciones. DES fue escogido como FIPS (Federal Information Processing Standard) en el año 1976 y su uso se extendió por todo el mundo.

AES:

El algoritmo AES (Advanced Encryption Standard) también conocido como Rijndael fue el ganador del concurso convocado en el año 1997 por el NIST (Instituto Nacional de Normas y Tecnología) con objetivo de escoger un nuevo algoritmo de cifrado. En 2001 fue tomado como FIPS y en 2002 se transformó en un estándar efectivo. Desde el año 2006 es el algoritmo más popular empleado en criptografía simétrica.

El algoritmo AES funciona mediante una serie de bucles que se repiten. 10 ciclos para claves de 128 bits, 12 para 192 y 14 para 256.Supongamos que tenemos 2 matrices: matriz ay matriz k

En la matriz a tenemos nuestra información y en la matriz k tenemos una sub clave generada a partir de la principal.

Referencia Bibliográficas

- Fernandez Maíllo Juan Andres, Sistemas seguros de acceso y transmisión de datos (MF0489_3)
- Ed. RAMA ediciones
- Pedro G.(2013). Tipos de criptografía: simétrica , asimétrica e híbrida
- https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida
- Beto G.(2015). Tipos de criptografía
- https://prezi.com/twvtylloadfb/tipos-de-criptografia/
- Héctor C. Carlos C. Alejandro C. .Criptografía y Métodos de Cifrado
- http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

Algoritmos de encriptación

Vamos a dividirlos en dos categorías respecto a su evolución y tiempo práctico, puesto a que cierta cantidad de ellos ya no se utilizan mucho para cifrar como tal, ya que no resulta como la opción más óptima, así que algunos de ellos incluso se encuentran obsoletos en nuestro tiempo actual, y en su lugar se utilizan como métodos de introducción o aprendizaje al cifrado de información.

Algoritmos antiguos:

El Cifrario de César:

La historia del Cifrado de César

Método empleado en la Roma Imperial, llamado así por ser la forma en la que Julio César usaba para comunicarse con sus legiones, y así pasar sus mensajes secretos a sus Centuriones ya experimentados con este sistema de cifrado, manteniendo a salvo así sus estrategias y todo tipo de información de manos enemigas, las cuales desconocían este sistema.

Descripción:

De los algoritmos de criptografía más simples, simplemente reemplazar la letra por una situada tres espacios delante de la misma, creando un mensaje que a simple vista no posee casi ningún sentido o patrón transpuesto, puesto a que solo dispone de un cambio de operación simple por cada una de las letras.

Vigenère

Blaise Vigenère

Blaise de Vigenère, de origen francés, en el siglo XVI, desarrolló la teoría de la criptología polialfabética,y es por esta misma razón por la cual su nombre es parte de uno de los métodos más famosos dentro de este campo, convirtiéndose en una de las mejores formas de asegurar secretos, y por ella también se le conoce y llama,“le chiffre indéchiffrable”.

Descripción:

“tablero de Vigenère” corresponde a su denominación actual consta de una disposición de letras la cual contiene en orden los 26 alfabetos César.

Como parte del proceso se agrega una palabra clave que se repite a lo largo de todo el mensaje a cifrar, tomando la letra de la clave que se corresponda a la letra a cifrar y buscar su correspondiente alfabeto cesar que inicie con dicha letra, y para descifrar consta de lo mismo en una función inversa.

El Código Morse

Consta de un alfabeto alternativo, tratando de ocultar un mensaje de otra manera, en teoría no se está ocultando el mensaje como tal, usado en sus principios con fines militares, va muy bien para transmitir mensajes secretos, es necesario codificarlo antes de poder enviarlo, para un mejor manejo y manipulación.

Algoritmos modernos:

DES:

La historia de DES

DES empezó en los 70, presentado por IMB en una segunda petición de la NBS como algoritmo de cifrado de información confidencial en 1974.

DES como estándar:

DES fue aprobado como estándar federal en noviembre de 1976, y publicado el 15 de enero de 1977 como FIPS PUB 46, autorizado para el uso no clasificado de datos. Fue posteriormente confirmado como estándar en 1983, 1988 , 1993 , y de nuevo en 1998 , este último definiendo "Triple DES" . El 26 de mayo de 2002, DES fue finalmente reemplazado por AES , tras una competición pública . Hasta hoy día , DES continúa siendo ampliamente utilizado.

Descripción:

DES es el algoritmo prototipo del cifrado por bloques — un algoritmo que divide un texto en una cantidad fija de bits y lo cifra transformándolo en otro texto de la misma longitud. En el caso de DES el tamaño del bloque es de 64 bits. DES utiliza también una clave criptográfica para el cifrado, de modo que es necesario conocer la clave utilizada para realizar el descifrado. La clave mide 64 bits, solo se utilizan 56 bits para el cifrado y los ocho restantes son usados para comprobar la paridad y después son descartados.

Al igual que otros cifrados de bloque, DES debe ser utilizado en el modo de operación de cifrado de bloque si se aplica a un mensaje mayor de 64 bits.

RSA:

La historia del RSA

RSA fue desarrollado en 1979 por Ron Rivest, Adi Shamir y Leonard Adleman, del Instituto Tecnológico de Massachusetts ; las letras RSA son las iniciales de sus apellidos. Debido al elevado coste de las computadoras necesarias para implementarlo en la época su idea no trascendió. Su descubrimiento, sin embargo, no fue revelado hasta 1997 ya que era confidencial, por lo que Rivest, Shamir y Adleman desarrollaron RSA de forma independiente.

Patentado por el MIT en 1983. Como el algoritmo fue publicado antes de patentar

la aplicación, esto impidió que se pudiera patentar en otros lugares del mundo.

Descripción:

Con operaciones alrededor de dos números primos aleatorios (para lograr una complejidad superior) se crean un par de llaves representadas como pares ordenados con los que se cifra y descifra independientemente cada letra de nuestro mensaje o información a cifrar, convirtiendo strings a números y operando cada uno de ellos independientemente.

IDEA.

Algoritmo internacional de cifrado de datos, o por sus siglas en inglés “IDEA”, fue diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zúrich y descrito por primera vez a principios de los 90, propuesto como reemplazo hacia el ya conocido DES, IDEA fue una revisión de PES, un algoritmo antecesor, IDEA fue originalmente llamado IPES, IDEA es un algoritmo libre para uso no comercial.

Funcionamiento

IDEA realiza operaciones con bloques de 64 bits utilizando una clave de 128 bits y consiste de ocho transformaciones idénticas y una transformación de salida . El proceso para cifrar y descifrar es similar. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos que son algebraicamente “incompatibles” en cierta forma.

AES.

Historia:

En 1997, el Instituto Nacional de Normas y Tecnología realizó un concurso para escoger un nuevo algoritmo de cifrado capaz de proteger información sensible durante el siglo XXI. Este algoritmo se denominó Advanced Encryption Standard (AES).

Los objetivos para este nuevo algoritmo de cifrado eran los siguientes.

- Ser de dominio público.
- Ser un algoritmo de cifrado simétrico y soportar bloques de, como mínimo, 128 bits.
- Las claves de cifrado podrían ser de 128, 192 y 256 bits.
- Ser implementable tanto en hardware como en software.

Desarrollo:

AES, es un cifrador que trabaja en bloques de bits de una longitud fija. El algoritmo toma un bloque de cierto

tamaño, normalmente de 128 bits, y produce un bloque de salida del mismo tamaño. El cifrado requiere una segunda entrada, la cual es la clave. AES soporta tamaños de bloque de 128 bits y tamaños de clave de 128, 192 y 256 bits. Cada tamaño de clave hace que el algoritmo se comporte ligeramente diferente, por lo que el aumento de tamaño de llave no solo ofrece un mayor número de bits con los que se pueden cifrar los datos, sino que también aumenta la complejidad del algoritmo de cifrado.

Criptografía cuántica :

Corresponde a aquella que utiliza principios mecano cuánticos así asegurando la seguridad casi absoluta de toda la información transmitida, incluyendo muchos otros protocolos anti espionaje o anti intercepción.

Historia:

Propuesta como idea en los 70, y no fue hasta 1984 que se publicó su primer protocolo, desarrollado hasta el dia de hoy, requiriendo a nivel mundial de una capacidad matemática poco accesible a público normal registrado.

Descripción y desarrollo:

Utilizando la física para crear un criptosistema seguro tanto en envio, procesado y remitencia, poseyendo protocolos para la intercepción de la información, como cambiar el cifrado por completo o en distintas partes en caso de que un tercero intenta espiar la creación de la clave y advertir a este tercero antes de enviar la información, como consecuencia del teorema de no clonado.

Las piezas de hardware utilizadas en la criptografía cuántica, es distinta a la tradicional, constando de cosas como láseres para emitir la información, utilizando fibra óptica, emitiendo en el elemento contribuyente de la luz y el fotón.

Protocolo BB84:

Historia de BB84:

Publicado en 1984 por Charles Bennett y Gilles Brassard y con este, el nacimiento de la criptografía cuántica.

Funcionamiento:

Logra su transmisión utilizando fotones polarizados enviando por un canal cuántico de emisor a receptor, con la existencia de un canal público,no necesariamente cuántico, entre los dos

entes emisor y receptor, que se utiliza para enviar información requerida para la construcción de la clave compartida, ninguno de los debe ser necesariamente seguro, puesto a que se asume la intercepción de un tercero cuyo fin es obtener información.

Cada uno de los fotones representa un solo bit de información, corresponde a un sistema binario de unos y ceros, un fotón corresponde únicamente a un uno o un cero, y la información se obtiene mediante la codificación de estados no-ortogonales, y en otros casos también se puede optar por una polarización circular horaria o antihoraria, ambos lados pueden enviar fotones polarizados.

Cifrado Afín:

Cifrado monoalfabético genérico

Cifrado por sustitución, cada símbolo del alfabeto es reemplazado por un símbolo del alfabeto cifrado, el número de caracteres del alfabeto cifrado es el mismo que del alfabeto limpio.

Es un cifrado donde se usa la aritmética modular que cumple que a,n sean PESI(primos entre si) para que pueda ser cifrado y descifrado, de caso no cumplir la condición entonces se podrá cifrar pero imposible descifrar

Para hallar el símbolo del alfabeto cifrado para sustituir a un determinado símbolo, se usa una función matemática. Para poder aplicar la función matemática primero hay que asignar un orden a cada símbolo de los alfabetos y asociar un número de orden.

Ejemplo de cifrado Afín:

```cpp
#include<bits/stdc++.h>
#include<iostream>
#include<string>
using namespace std;
int a = 7;
int b = 6;
string encryption(string m) {
    string c;
    for (int i = 0; i < m.length(); i++)
    {
        if(m[i]!=' ')
        c = c + (char) ((((a * (m[i]-'A') ) + b) % 26) + 'A');
        else
            c += m[i];
    }
    return c;
}
string decryption(string c) {
    string m;
    int inverso = 0;
    int flag = 0;
    for (int i = 0; i < 26; i++) {
        flag = (a * i) % 26;
        if (flag == 1) {
            inverso = i;
        }
    }
    for (int i = 0; i < c.length(); i++) {
        if(c[i] != ' ')
            m = m + (char) (((inverso * ((c[i]+'A' - b)) % 26)) + 'A');
        else
            m += c[i];
    }
    return m;
}
int main() {
    string msg = "Hola Mundo";
    string c = encryption(msg);
    cout << "Encrypted Message is : " << c<<endl;
    cout << "Decrypted Message is: " << decryption(c);
    return 0;
}
```

Atbash:

Atbash es un método muy común de cifrado del alfabeto hebreo. Se le denomina también método de espejo, pues consiste en sustituir la primera letra por la última , la segunda por la penúltima y así sucesivamente.

Este método se ideó para un abyad (sistema de alfabeto que utiliza símbolos para los fonemas creados por las consonantes), y luego estas vocalizadas de una manera arbitraria, por ello casi cualquier palabra del idioma hebreo sería pronunciable y cifrable en Atbash.

Se cifra por su letra de posición opuesta en el alfabeto, considerando el alfabeto como una sola línea con principio y fin y no como un ciclo, es decir que por ejemplo la letra ‘a’ será cifrada por la letra ‘z’, la ‘b’ por la ‘y’ y así sucesivamente hasta codificar o decodificar el mensaje, puesto a que su estructura fue ideada inicialmente para el idioma hebreo el resultado en el caso del español no es muy complejo.

```cpp
#include <iostream>
#include <string>
using namespace std;

class Atbash
{
  public:
  string abc="abcdefghijklmnopqrstuvwxyz";
  string abc2="zyxwvutsrqponmlkjihgfedcba";
  string cifrar(string msj);
  string descifrar(string msj);


};

string Atbash::cifrar(string msj)
{
  int aux,aux2;
  for(int i=0;i<msj.length();i++)
  {
    aux=abc.find(msj[i]);
    msj[i]=abc2[aux];
  }
  return msj;
}

string Atbash::descifrar(string msj)
{
  int aux,aux2;
  for(int i=0;i<msj.length();i++)
  {
    aux=abc.find(msj[i]);
    msj[i]=abc2[aux];
  }
  return msj;
}

int main() {
  Atbash atbash;
  string msj,cmsj,dmsj;
  getline(cin,msj);
  cmsj=atbash.cifrar(msj);
  dmsj=atbash.descifrar(cmsj);
  cout<<cmsj<<endl;
  cout<<dmsj<<endl;
}
```

Ejemplo del cifrado en Atbash:

Bibliografía:

- Criptografía Básica. Santiago Fernández
- https://es.wikipedia.org/wiki/Data_Encryption_Standard
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html
- https://es.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://www.boxcryptor.com/es/encryption/
- https://es.wikipedia.org/wiki/International_Data_Encryption_Algorithm
- https://www.ecured.cu/International_Data_Encryption_Algorithm_(IDEA)
- https://www.gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84/
- https://es.wikipedia.org/wiki/Criptograf%C3%ADa_cu%C3%A1ntica