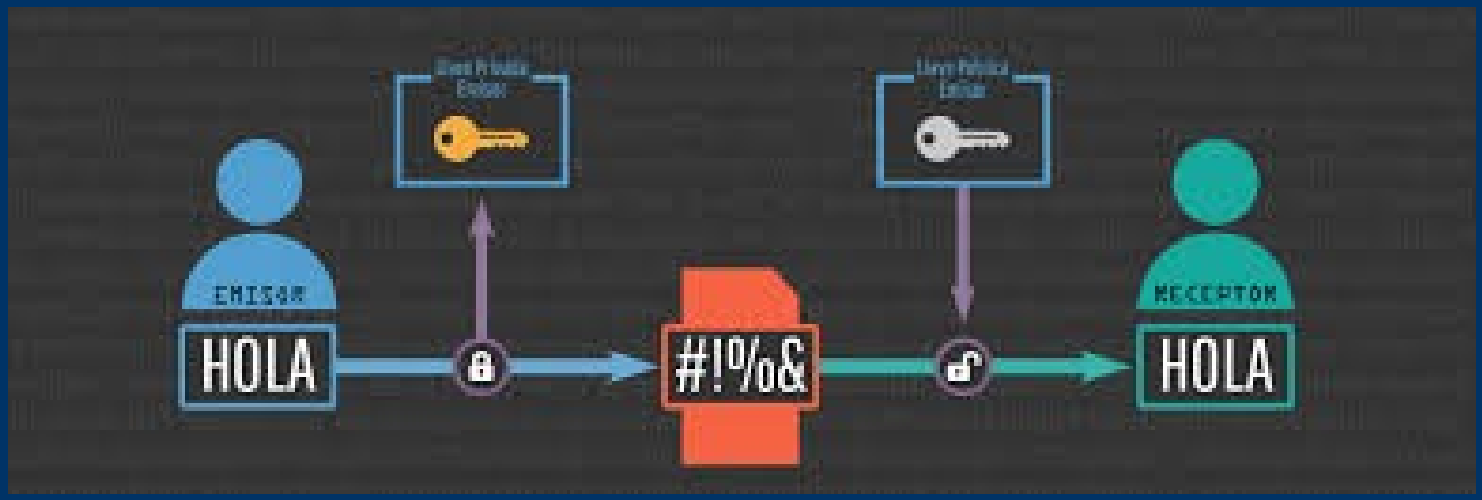
SEGURIDAD INFORMÁTICA
TEMA 1 – INTRO



CRIPTOGRAFÍA CLÁSICA

Métodos

- Transposición
- Sustitución

En ambos métodos el algoritmo de cifrado debe permanecer secreto.

CRIPTOGRAFÍA CLÁSICA

Métodos

- Transposición, funciona reordenando los caracteres del mensaje

  ejemplo:

  en la grecia clásica se utilizó la escítala en el siglo V a.c.

  enrollan un documento en un palo en forma de espiral y escribes el mensaje, de forma que el texto en el papel desenrrollado no tiene sentido.

  Fácil de utilizar pero tiene un nivel muy bajo.

CRIPTOGRAFÍA CLÁSICA

Métodos

- Transposición, funciona reordenando los caracteres del mensaje

  ejemplo:

  tenemos un documento dividido en 6 trozos y los mezclamos de forma 621354 en lugar de 123456

CRIPTOGRAFÍA CLÁSICA

Métodos

- Transposición, funciona reordenando los caracteres del mensaje

  ejemplo:

  tenemos una frase e intercambiamos los caracteres pares por los impares

  - eprd oascneh.z

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución, sustituimos un carácter por otro.

  Es de tipo monoalfabético

  Ejemplo: cifrado César

  sustituimos la A por la D, la B por la E, la C por la F.

  son siempre 3 caracteres más.

  Al final de alfabeto damos la vuelta, la X es la A, la Y la B...

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución, sustituimos un carácter por otro.

  Es de tipo monoalfabético

  Ejemplo: cifrado César I
  pr;sxhgr;ghvfxeulu;dñjxlhp;txh;vhsd;ñr;vxilflhpwh;sdud;ghflu;ghilplwlydohpwh;txh;hv;srvleñh;.;txh;losrvleñh/;khpu.;irug
- Tenemos que desencriptar este mensaje.

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución, sustituimos un carácter por otro.

  Es de tipo monoalfabético

  Ejemplo: cifrado César II
  hñ;iudfdvr;hv;vlosñhohpwh;xpd;pxhyd;rsruwxplgdg;gh;hosh,du;gh;pxhyr/;hvwd;yh,;gh;iruod;odv;lpwhñljhpwh/;khpu.;irug
- Tenemos que desencriptar este mensaje.

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución
- Ejemplo: cifrado de bilateral

  le sumamos un número siempre a la posiciones pares

  le restamos un número siempre a la posiciones impares

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución
- Ejemplo: cifrado de Vigenère (es de tipo polialfabético)

  le sumamos a una letra siempre el mismo número

  Texto: TOBEORNOTTOBETHATISTHEQUESTION

  Clave: RUNRUNRUNRUNRUNRUNRUNRUNRUN

  Cripto: KIOVIEEIGKIOVNURNVJNUVKHVMGZIA
- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Sustitución (es de tipo polialfabético)
- Ejemplo: cifrado de Vigenère

  le sumamos a una letra siempre el mismo número

  Texto: ?

  Clave: abc

  Criptograma=
  'emwnjeoftrptrfclfuarwemfemsufoobrrfodfñotoaechforzhosf'

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  para los cifradores de sustitución clásicos se basa en el análisis de la frecuencia de aparición de las letras en el criptograma y compararla con su distribución en el idioma en el que está escrito el mensaje.

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  3 grupos de frecuencias:

  alta E,A,S,O,U

  media C,L,U,M,P

  baja Y,Q,H,Z,J

- Ver ejercicios en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  diagramas mas usados:

  DE, ES, LA, OS, AR,

  trigramas más usados:

  QUE, EST, ARA, ADO, DEL y CIO

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  Método de Kasiski para descrifrar Vigenère

  Kasiski se dio cuenta de que, para un mensaje es habitual encontrar patrones que se repiten en el criptograma. Cuando la longitud de estos patrones es mayor o igual que 3, es probable que esas palabras sean también iguales en el texto en claro.

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  Método de Kasiski para descrifrar Vigenère

  KIOV se repite cada 9 y NU cada 6 por lo que el divisor común es 3.

  entonces K,V,E,van cifradas con la misma letra y hacemos un análisis monoalfabético.

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS

  Método de Kasiski para descrifrar Vigenère

entonces I,I,I,I,N,N van cifradas con la misma letra y hacemos un análisis monoalfabético.

entonces O,E,G,O,U,V van cifradas con la misma letra y hacemos un análisis monoalfabético.

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS
- Índice de coincidencia

Este concepto fue básico, de hecho, en el posterior criptoanálisis de las máquinas de rotores, como la Enigma, que tan importantes fueron en el desarrollo de la Segunda Guerra Mundial

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS
- Índice de coincidencia

$$IC = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{n(n-1)}$$

fi es el número que se repite cada letra

n es la longitud del texto cifrado

- Ahora con el valor del IC consultamos la tabla

y así obtenemos la d que es el factor de repetición

d	IC
1	0,072
2	0,054
3	0,049
4	0,046
5	0,044
6	0,040
...	
Grande	0,037

CRIPTOGRAFÍA CLÁSICA

Métodos

- CRIPTOANÁLISIS
- Índice de coincidencia

  criptograma=”GUVQAEQORNGVCOGPVGUG IWTQF GSWGGNRTKOGTCNWOPQSWGFGUEKHTGGUVGOGPU CLGANQRWDNKSWGGPGNHQTQFGNCCUKIPCVWTCVG PFTCOCURWPVQUGPUWPQVC”
- Son 121 caracteres y nos falta calcular el sumatorio.
- Ejercicio en python

CRIPTOGRAFÍA CLÁSICA

Métodos

- Cifrado polialfabético
- Máquina Enigma

  Fue diseñada y utlizada por los alemanes en la W.W. II

  Tiene un sistema complejo de varios alfabetos que se escriben en el exterior de unos rotores mecánicos y conectados entre sí para cambiar de posición el rotor con cada pulsación. Y al terminar la z gira una letra el siguiente.

  4 rotores es como tener 456.976 alfabetos.

CRIPTOGRAFÍA CLÁSICA

Métodos

- Cifrado polialfabético
- Máquina Enigma – partes principales

  Rotores

  Reflector

  Caja de enchufes (Plugboard)

  Teclado

  Lámparas

CRIPTOGRAFÍA CLÁSICA

Métodos

- Cifrado polialfabético
- Máquina Enigma

- video descrifrando un mensaje
  https://www.youtube.com/watch?v=g5LZvytKrys
- Video funcionamiento
  https://www.youtube.com/watch?v=ybkkiGtJmkM

CRIPTOGRAFÍA CLÁSICA

Métodos

- Cifrado polialfabético
- Máquina Enigma

Pudieron descifrar mensajes de la Enigma gracias a Alan Turing que trabajó con el ejercito inglés en un máquina que calculara muchas conbinaciones para acertar con el mensaje.

- Está muy interesante la película de Benedict Cumberbatch y Keira Knightley, Descifrando Enigma