Clase 1

11 de marzo 2024

Esquema $\pi(Gen, Enc, Dec)$ priv

- $k \leftarrow Gen()$
- $c \leftarrow Enc_k(m)$
- $m := Dec_k(c)$

$Dec_k(Enc_k(m)) = m$ Correcto

La seguridad debe recaer en que la clave se mantenga en secreto

Es mas simple mantener en secreto algo mas chico (una clave) que algo mas grande (como el algoritmo entero).
No es correcto que la seguridad de un algoritmo resida en que el algoritmo no se conozca, siempre hay que asumir que es conocido.

Ejemplo de un ejercicio para cifrado de ROT

GEN: se elige k entre 0 y 26, con P(k) = 1/27
ENC(k): m(i) + k congruente a c(i) mod 27
DEC(k): c(i) - k congruente a c(i) mod 27

Cifrados clásicos

Reemplazo de un caracter por otro

Sustitución

Sustitución Monoalfabética

Un unico alfabeto para todas las letras (es una permutacion del alfabeto original). La misma letra siempre se reemplaza por el mismo caracter.

Ej: Cifrado César

- Espacio de claves (necesario)
- Frecuencias originales en cifrado

En rotacion (un tipo especial de sustitucion) el espacio de claves es 26. En sustitucion normal el espacio de claves es 26!
Sin embargo, la sustitucion es insegura en todas sus formas, ya que los lenguajes tienen patrones que se repiten (como que la letra 'e' aparece seguido)

Sustitución Polialfabética

En el de viguenere, hay multiples alfabetos con distintas rotaciones, y segun el numero de letra se va usando un alfabeto distinto

Ej: Cifrado Vigenere

- Período de clave: D |período
- Indice de coincidencia

$$\sum_{i=0}^{26} p_i^2 \approx 0{,}0775$$

Para descifrar un vigenere, tenemos que ir encontrando patrones que se repitan en el texto. Contamos la cantidad de caracteres hasta que se repita ese patron (periodo). La longitud de la clave es algun divisor del MCD entre las longitudes hasta que se repite el mismo patron n veces.
Por ende, vigenere es mas seguro si la clave es mas larga (poco practico) y si el texto es mas corto.

El indice de coincidencia tiene que ver con la frecuencia de las letras en cada lenguaje. Para el idioma español, tenemos que la probabilidad media de cada letra es 0.0775.

Trasposición

Cambiar dos caracteres de lugar entre si

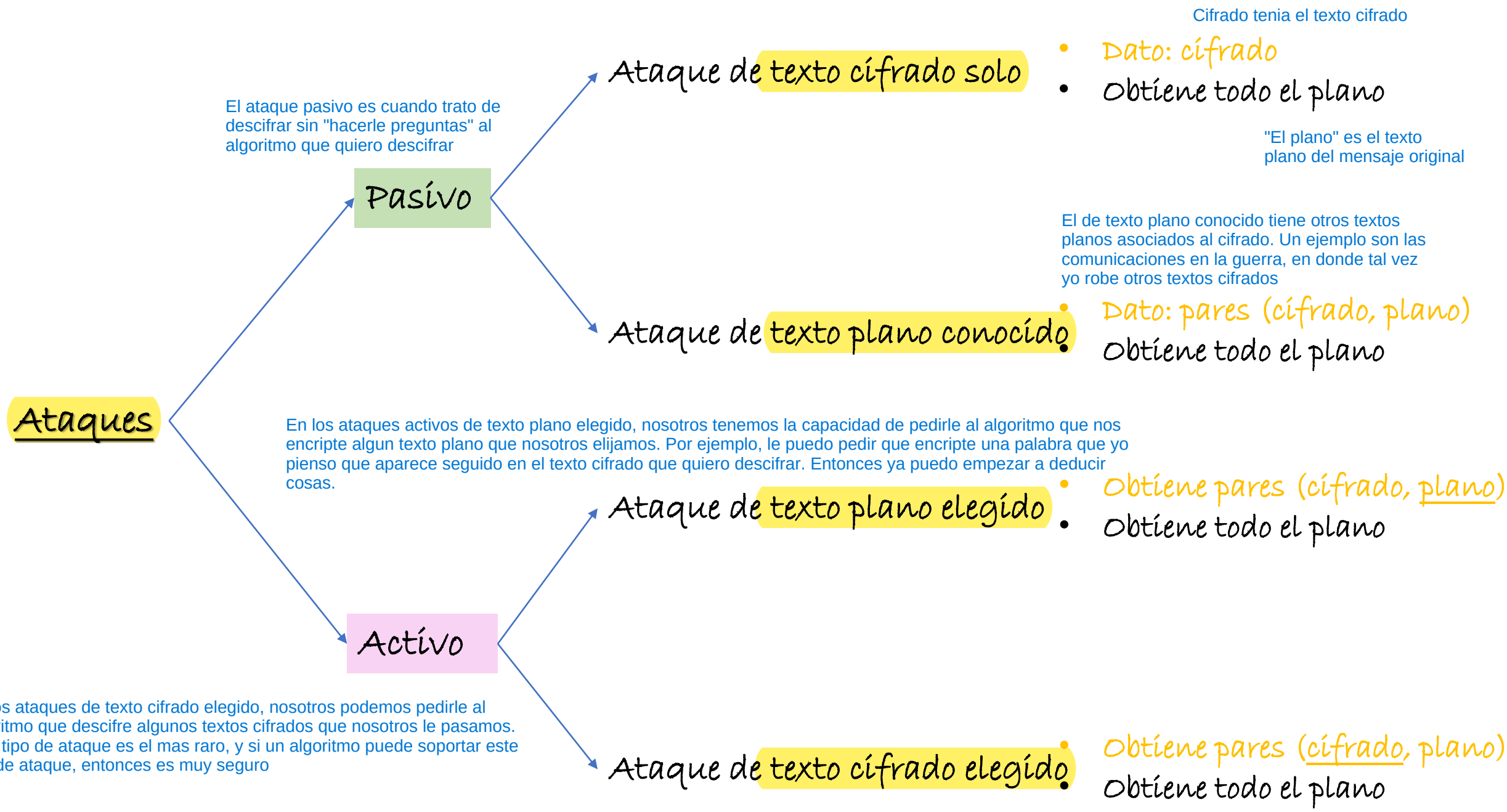
Ej: Trasposición por columnas

- Frecuencias originales

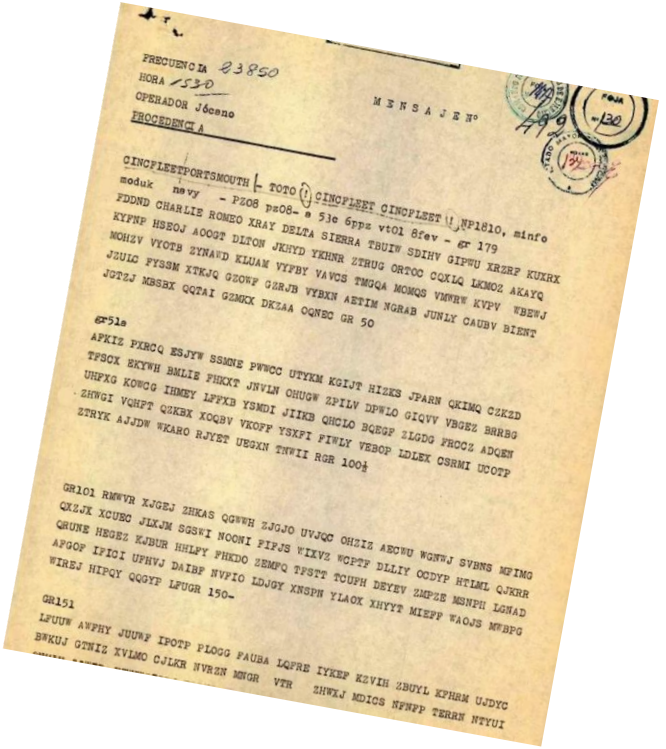
Ejemplo de cifrado de trasposicion de columnas.
Mensaje: EL MENSAJE ES NUEVO
Cantidad: k = 3

ELM
ENS
AJE
ESN
UEV
O$$

El mensaje me queda EEAEUOLNJSE$MSENV$.
El problema con este cifrado es que las apariciones de cada letra permanecen iguales


Cifrado tenia el texto cifrado
Dato: cifrado
Obtiene todo el plano
El ataque pasivo es cuando trato de descifrar sin "hacerle preguntas" al algoritmo que quiero descifrar
Pasivo
Ataque de texto cifrado solo
"El plano" es el texto plano del mensaje original
El de texto plano conocido tiene otros textos planos asociados al cifrado. Un ejemplo son las comunicaciones en la guerra, en donde tal vez yo robe otros textos cifrados
Ataque de texto plano conocido
Dato: pares (cifrado, plano)
Obtiene todo el plano
Ataques
En los ataques activos de texto plano elegido, nosotros tenemos la capacidad de pedirle al algoritmo que nos encripte algun texto plano que nosotros elijamos. Por ejemplo, le puedo pedir que encripte una palabra que yo pienso que aparece seguido en el texto cifrado que quiero descifrar. Entonces ya puedo empezar a deducir cosas.
Ataque de texto plano elegido
Obtiene pares (cifrado, plano)
Obtiene todo el plano
Activo
En los ataques de texto cifrado elegido, nosotros podemos pedirle al algoritmo que descifre algunos textos cifrados que nosotros le pasamos. Este tipo de ataque es el mas raro, y si un algoritmo puede soportar este tipo de ataque, entonces es muy seguro
Ataque de texto cifrado elegido
Obtiene pares (cifrado, plano)
Obtiene todo el plano

Criptografía clásica en la Guerra de Malvinas


FRECUENCIA 23850
HORA 1530
OPERADOR Jócano
PROCEDENCIA
MENSAJE Nº
CINCFLEETPORTSMOUTH ← TOTO ⓘ CINCFLEET CINCFLEET ⓘ NF1810, minfo
moduk navy - PZO8 pz08- ⊕ 53e 6ppz vt01 8fev - gr 179
FDDND CHARLIE ROMEO XRAY DELTA SIERRA TBUIW SDIHV GIPWU XRZRF KUXRX
KYFNP HSEOJ AOOGT DITON JKHYD YKHNR ZTHUG ORTOO CQXLQ LKMOZ AKAYQ
MOHZV YYOTB ZYNAWD KLUAN VYFBY VAVCS TMQQA MOMQS VMWRW KVPV WBEWJ
JSUIC FYS3M XTKJQ GZOWF GZRJB VYBXN AETIM NGRAB JUNLY CAUBV BIENT
JGTZJ MBSBX QQZAI G2MGX DKZAA OQNEC GR 50
6r51s
APKIZ PXRCQ ESJYW SSMNE PWWOC UTYKM KGIJT HI2KS JPARM QKIMQ CZK2D
TPSCX EKYWH BMLIE FHKXT JNVLN OHUGW 2PILV DPWLO GIQVV VBGEZ BHRBG
UHPXG KOWCG IHMEY LFFXB YSMDI JIIKB QHCLO BQEGP 2LGDG FKOCZ ADQEN
ZHWGI VQHPT QZKBX XCQBV VKOFF YSXFI FIWLY VEBOP LDLEX CSRMI UCOTP
ZTRYK AJJDW WKARO RJYET UBGXN TNWII RGR 100↓
GR101 RMWVR XJGEJ ZHKAS QGWWH ZJGJO UVJGC OHZIZ AECWU WGNWJ SVBNS MFIMG
QXZJX XCUBC JLKJM SGSWI NOONI FIPJS WIXVZ WCPTF DLLIY OCDYP HYLML QJKRR
QHUNE HEGEZ KJBUR HHLFY FHKDO ZEMFQ TFSTT TOUFH DEYEV ZMPZE MSNPH LGNAD
APGOP IFIGI UFHVJ DAIBF NVFIO LDJGY XNSPH YLAOX XHYYT MIEPF WAOJS MFBPG
WIREJ HIPQY QQGYP LFUGR 150-
GR151
LFUUW AWFHY JUUWF IPOTP PLOGG FAUBA LQFRE IYKEF KZVIH ZBUYL KPHRM UJDYC
BWKUJ GTNIZ XVLMO CJLKR NVRZN MNGR VTR ZHWXJ MDICS NFWPP TERRN NTYUI

- https://www.tec.gob.ar/el-ultimo-secreto-de-malvinas-como-la-inteligencia-argentina-busco-informacion-sobre-el-enemigo/
- https://hoydia.com.ar/mundo/66689-revelan-complicidad-de-ee-uu-con-gran-bretana-durante-la-guerra-de-malvinas/