Criptografía y Seguridad en Redes

v.2015

Seminario #1

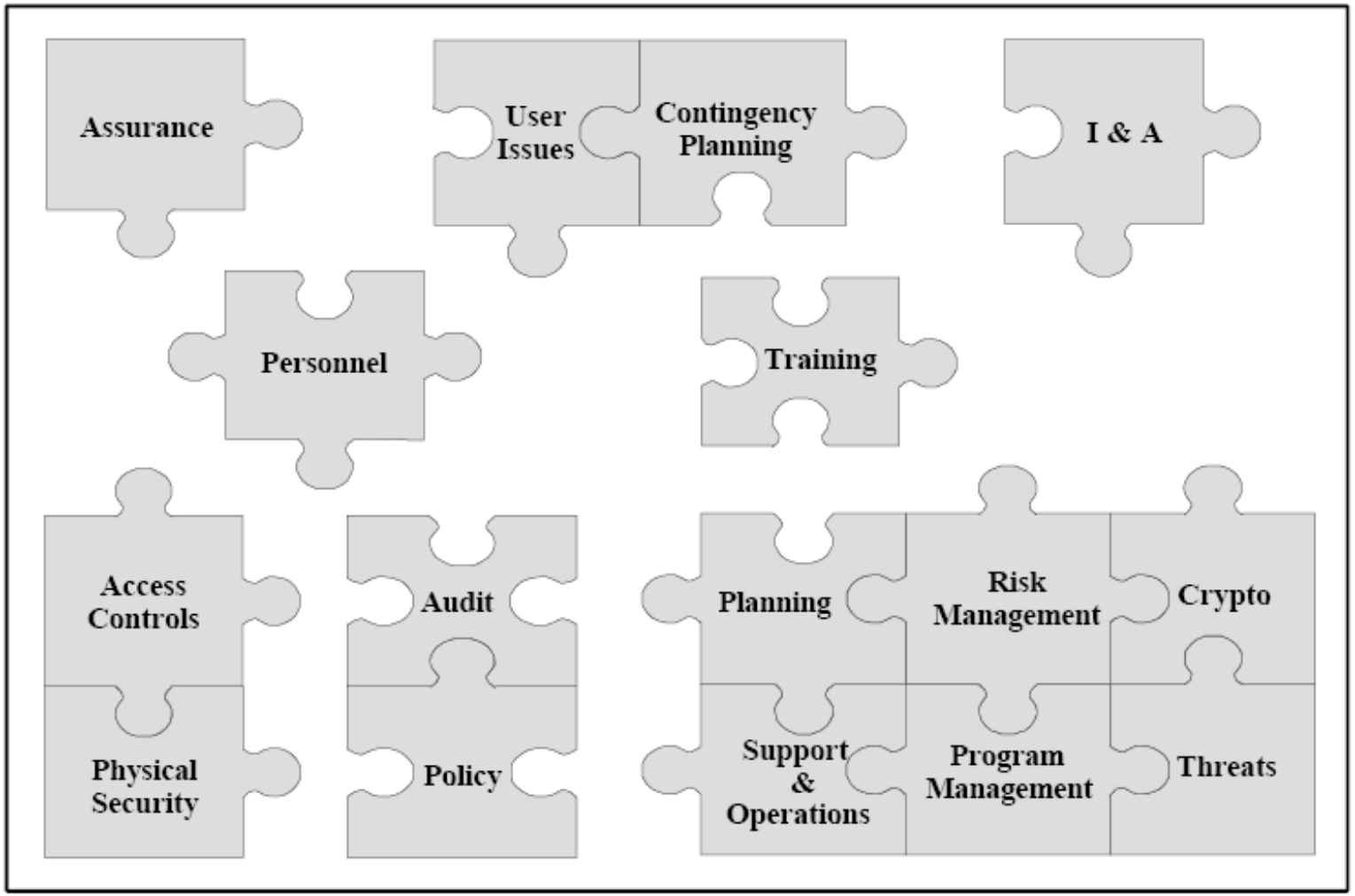
Prof.Ing.Miguel SOLINAS

mksolinas@gmail.com

Agenda

- *Introducción*
- *Criptografía histórica*

Algunas razones para estudiar SI



Propiedades de la Información

Confidencialidad

Garantiza que está accesible exclusivamente para el personal autorizado.

Integridad

Garantiza que no ha sido modificada sin autorización.

Disponibilidad

Garantiza que está disponible.

Servicios de Seguridad

Confidencialidad

Garantizar que la información está disponible para aquellos que están autorizados a verla. Para los demás está oculta.

Integridad

Garantizar precisión en el contenidos.

Autenticación

Garantizar identidad.

Firma Digital

Autenticación + Integridad + No Repudio

El proceso de la comunicación

El proceso de la comunicación segura

(Tercera parte confiable)

(Atacante)

Tipos de ataque: PASIVO

(Tercera parte confiable)

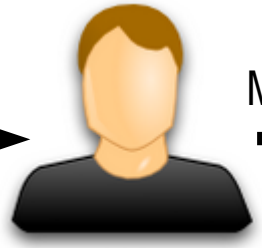
(Identidad)

Mensaje

Alice

CANAL INSEGURO

(Identidad)



Bob

Mensaje

Transformación Segura + Información Secreta

Transformación Segura + Información Secreta

(Atacante)

Tipos de ataque: ACTIVO

(Tercera parte confiable)

(Identidad)

Mensaje

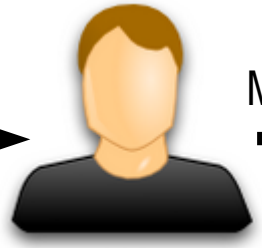
Alice

Transformación Segura

Información Secreta

CANAL INSEGURO

(Identidad)



Bob

Mensaje

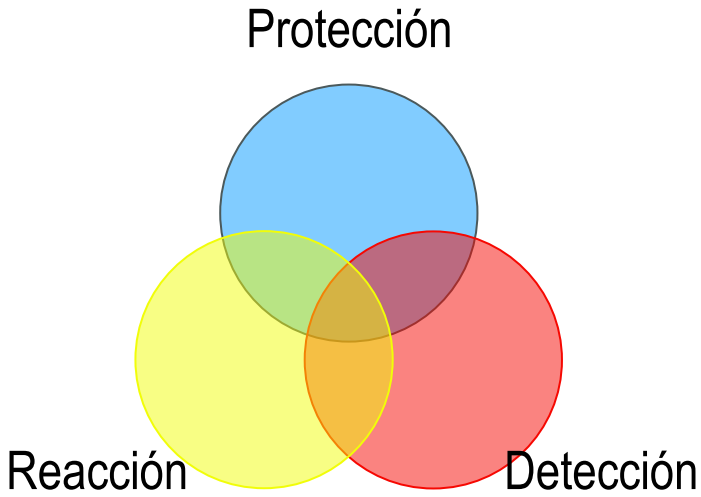
Transformación Segura

Información Secreta

(Atacante)

¿Cómo responder a los ataques ?

a. Identificar bienes claves
b. Evaluar diferentes ataques a esos bienes
c. Implementar las medidas mas convenientes
d. Instrumentar una administración
e. Elaborar planes de contingencia



La criptografía es una herramienta clave

¿Qué es la criptografía ?

CRIPTOGRAFIA

Del griego κρύπτω krypto, «oculto», y γράφως graphos, «escribir», literalmente «escritura oculta».

Estudio de la **escritura secreta**.

Es la ciencia que hace posible que el costo de obtener o alterar información sea mayor que la ganancia potencial por obtenerla o alterarla..!!

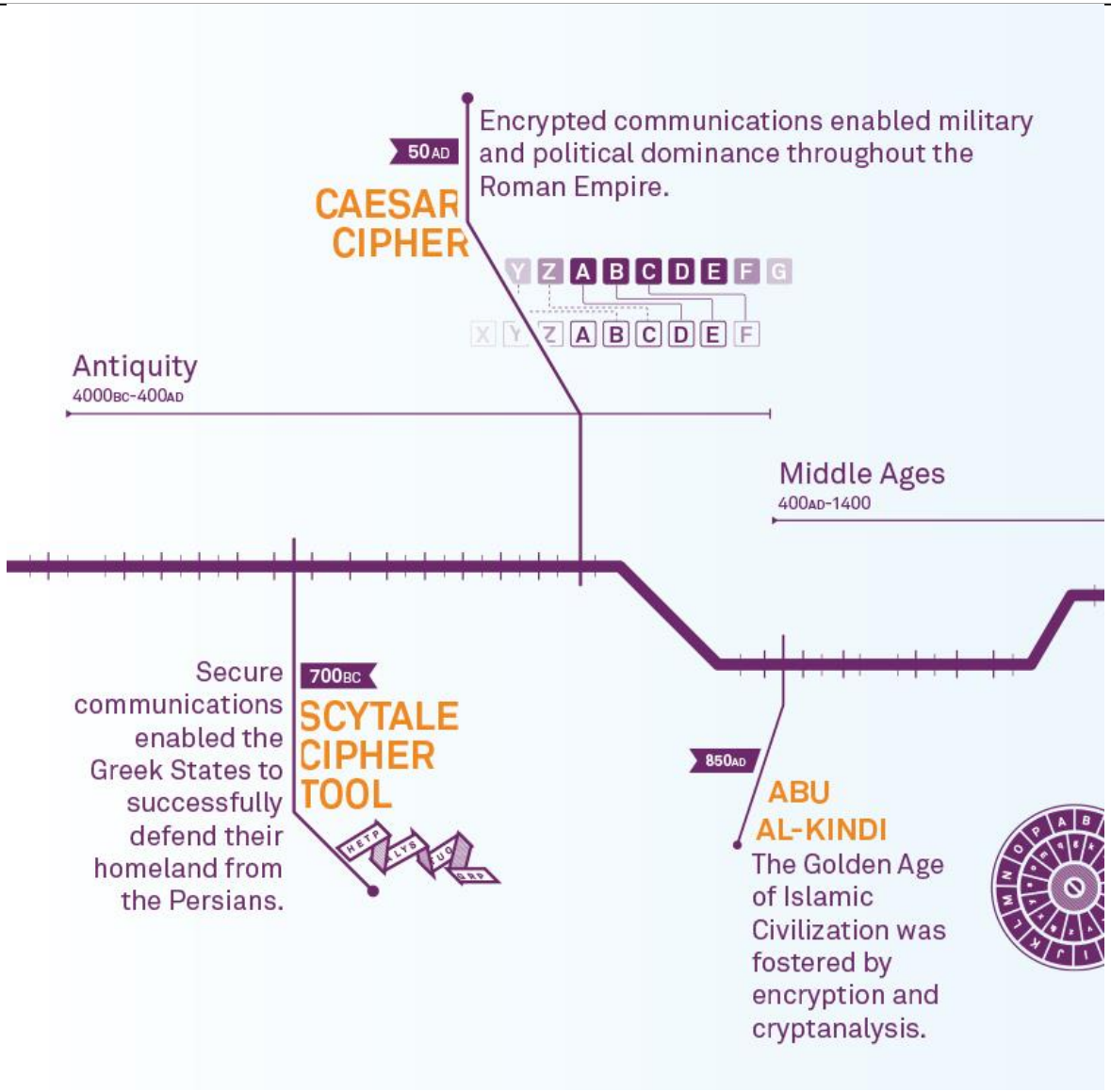
¿Qué es la criptografía ?

Está relacionada con el desarrollo de algoritmos que puedan ser usados para:

- Ocultar el contenido de un mensaje para todos, excepto para emisor y receptor del mensaje; y/o
- Verificar la integridad del mensaje en el receptor.

Es la base de muchos de los desarrollos tecnológicos que brindan soluciones a problemas de seguridad en las comunicaciones.

Criptografía histórica



Criptografía histórica

Escitalo (vara de madera) griego

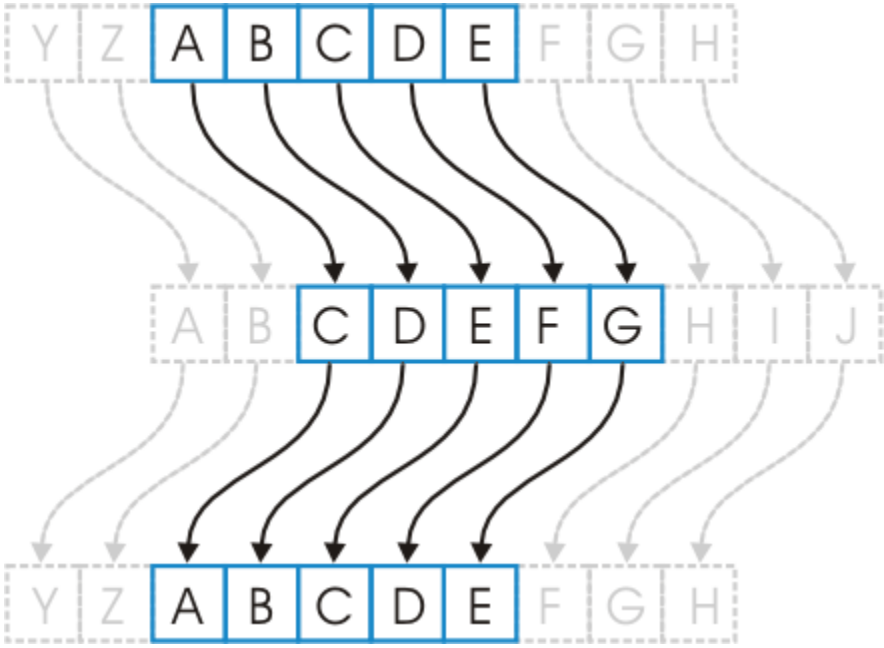
Criptografía histórica

Cifra del Cesar

- Hace mas de 2000 años, Julio Cesar usó una cifra de sustitución simple, que luego se conoció como cifra del Cesar.
- Primeros testimonios de uso son de la guerra de las Galias.
- Reemplaza cada letra con la tercera siguiente, Ej.:
  - `L FDPH L VDZ L FRQTXHUHG`
  - **`-> I CAME I SAW I CONQUERED`**
- Se puede definir esta transformación alfabética como:
  - **`Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ`**
  - `Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC`
- Desencriptar:

`"RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV"`

Veamos algo de cifra de sustitución



Criptografía histórica

Los Hermanos Musulmanes convocaron hoy a "día de ira" con nuevas manifestaciones en El Cairo después de que casi 600 personas murieran en la represión de los últimos días ante la cual la ONU pidió un "máximo de contención" a todos los bandos.

Esta nueva convocatoria hace temer otra jornada de violencia en el país, donde el balance de muertos por el violento desalojo el miércoles de los dos campamentos de simpatizantes del presidente islamista Mohamed Mursi, derrocado por el ejército el 3 de julio, y los posteriores enfrentamientos dejaron 578 muertos, según cifras del ministerio de Salud.

Los Hermanos Musulmanes hablan por su parte de 2.200 muertos y más de 10.000 heridos, en la jornada más sangrienta en Egipto desde la caída de Hosni Mubarak en febrero de 2011.

Este "viernes de la cólera" suscita inquietud en Europa, donde el presidente francés, François Hollande, se entrevistará esta tarde por teléfono con la canciller aleman, Angela Merkel, y posteriormente con el primer ministro británico, David Cameron.

Las autoridades egipcias, designadas por el ejército, han autorizado a la policía a disparar balas reales contra los manifestantes que ataquen bienes públicos o a las fuerzas de seguridad.

"Las manifestaciones contra el golpe de Estado mañana (viernes) saldrán de todas las mezquitas de El Cairo y se dirigirán hacia la plaza Ramses tras la oración por un "viernes de la cólera"", precisó el portavoz de la cofradía islamista, Gehad El Haddad, en su cuenta Twitter el jueves.

Laila Musa, portavoz de la Coalición pro-Mursi contra el "golpe de Estado", informó de que se prevén protestas similares en todo el país.

Criptografía histórica

Nqu Jgtocpqu Owuwnocpgu eqpxqectqp jqa c "fíc fg ktc" eqp pwgxcu ocpkhguvcekqpgu gp Gn Ecktq fgurwéu fg swg ecuk 600 rgtuqpcu owtkgtcp gp nc tgrtgukóp fg nqu únvkoqu fícu cpvg nc ewcn nc QPW rkfkó wp "oázkoq fg eqpvgpekóp" c vqfqu nqu dcpfqu.

Guvc pwgxc eqpxqecvqtkc jceg vgogt qvtc lqtpcfc fg xkqngpekc gp gn rcíu, fqpfg gn dcncpeg fg owgtvqu rqt gn xkqngpvq fgucnqlq gn okéteqngu fg nqu fqu ecorcogpvqu fg ukorcvkbcpvgu fgn rtgukfgpvg kuncokuvc Oqjcogf Owtuk, fgttqecfq rqt gn glétekvq gn 3 fg lwnkq, a nqu rquvgtkqtgu gphtgpvcokgpvqu fglctqp 578 owgtvqu, ugiúp ekhtcu fgn okpkuvgtkq fg Ucnwf.

Nqu Jgtocpqu Owuwnocpgu jcdncp rqt uw rctvg fg 2.200 owgtvqu a oáu fg 10.000 jgtkfqu, gp nc lqtpcfc oáu ucpitkgpvc gp Gikrvq fgufg nc ecífc fg Jqupk Owdctcm gp hgdtgtq fg 2011.

Guvg "xkgtpgu fg nc eóngtc" uwuekvc kpswkgvwf gp Gwtqrc, fqpfg gn rtgukfgpvg htcpeéu, Htcpçqku Jqnncpfg, ug gpvtgxkuvctá guvc vctfg rqt vgnéhqpq eqp nc ecpeknngt cngocp, Cpignc Ogtmgn, a rquvgtkqtogpvg eqp gn rtkogt okpkuvtq dtkvápkeq, Fcxkf Ecogtqp.

Ncu cwvqtkfcfgu gikrekcu, fgukipcfcu rqt gn glétekvq, jcp cwvqtkbcfq c nc rqnkeíc c fkurctct dcncu tgcngu eqpvtc nqu ocpkhguvcpvgu swg cvcswgp dkgpgu rúdnkequ q c ncu hwgtbcu fg ugiwtkfcf.

"Ncu ocpkhguvcekqpgu eqpvtc gn iqnrg fg Guvcfq ocñcpc (xkgtpgu) ucnftáp fg vqfcu ncu ogbswkvcu fg Gn Ecktq a ug fktkiktáp jcekc nc rncbc Tcougu vtcu nc qtcekóp rqt wp "xkgtpgu fg nc eóngtc"", rtgekuó gn rqtvcxqb fg nc eqhtcfíc kuncokuvc, lgjcf Gn Jcffcf, gp uw ewgpvc Vykvvgt gn lwgxgu.

Nckncc Owuc, rqtvcxqb fg nc Eqcnkekóp rtq-Owtuk eqpvtc gn "iqnrg fg Guvcfq", kphqtoó fg swg ug rtgxép rtqvguvcu ukoknctgu gp vqfq gn rcíu.

Criptografía histórica

NQUJG TOCPQ UOWUW NOCPG UEQPX QECTQ PJQAC FCFGK TCEQP PWGXC UOCPK HGUVC EKQPG
UGPGN ECKTQ FGURW UFGSW GECUK RGTUQ PCUOW TKGTC PGPNC TGRTG UKPFG NQUNV KOQUF
CUCPV GNCEW CNNCQ PWRKF KWPOZ KOQFG EQPVG PEKPC VQFQU NQUDC PFQUG UVCPW GXCEQ
PXQEC VQTKC JCEGV GOGTQ VTCLQ TPCFC FGXKQ NGPEK CGPGN RCUFQ PFGGN DCNCP EGFGO WGTVQ
URQTG NXKQN GPVQF GUCNQ LQGNO KTEQN GUFGN QUFQU ECORC OGPVQ UFGUK ORCVK BCPVG UFGNR
TGUKF GPVGK UNCOK UVCOQ JCOGF OWTUK FGTTQ ECFQR QTGNG LTEKV QGNFG LWNKQ ANQUR QUVGT
KQTGU GPHTG PVCOK GPVQU FGLCT QPOWG TVQUU GIPEK HTCUF GNOKP KUVGT KQFGU CNWFN QUJGT
OCPQU OWUWN OCPGU JCDNC PRQTU WRCTV GFGOW GTVQU AOUFG JGTKF QUGPN CLQTP CFCOU UCPIT
KGPVC GPGIK RVQFG UFGNC ECFCF GJQUP KOWDC TCMGP HGDTG TQFGG UVGXK GTPGU FGNCE NGTCU
WUEKV CKPSW KGVWF GPGWT QRCFQ PFGGN RTGUK FGPVG HTCPE UHTCP QKUJQ NNCPF GUGGP VTGXK
UVCTG UVCVC TFGRQ TVGNH QPQEQ PNCEC PEKNN GTCNG OCPCP IGNCO GTMGN ARQUV GTKQT OGPVG
EQPGN RTKOG TOKPK UVTQD TKVPK EQFCX KFECO GTQPN CUCWV QTKFC FGUGI KREKC UFGUK IPCFC
URQTG NGLTE KVQJC PCWVQ TKBCF QCNCR QNKEC CFKUR CTCTD CNCUT GCNGU EQPVT CNQUO CPKHG
UVCPV GUSWG CVCSW GPDKG PGURD NKEQU QCNCU HWGTB CUFGU GIWTK FCFNC UOCPK HGUVC
EKQPG UEQPV TCGNI QNRGF GGUVC FQOCC PCXKG TPGUU CNFTP FGVQF CUNCU OGBSW KVCUF GGNEC
KTQAU GFKTK IKTPJ CEKCN CRNCB CTCOU GUVTC UNCQT CEKPR QTWPX KGTPG UFGNC ENGTC RTGEK
UGNRQ TVCXQ BFGNC EQHTC FCKUN COKUV CIGJC FGNJC FFCFG PUWEW GPVCV YKVVG TGNLW GXGUN
CKNCO WUCRQ TVCXQ BFGNC EQCNK EKPRT QOWTU KEQPV TCGNI QNRGF GGUVC FQKPH QTOFG SWGUG
RTGXP RTQVG UVCUU KOKNC TGUGP VQFQG NRCU

Criptografía histórica

Transformación de encripción / desencripción

$$C = E_K(M)$$

$$M = D_K(C) = D_K[E_K(M)]$$

$M = m_1, m_2, ..., m_i, ...$; donde $m_i \in \boldsymbol{M}$

$K = k_1, k_2, ..., k_i, ...$; donde $k_i \in \boldsymbol{K}$

$C = c_1, c_2, ..., c_i, ...$; donde $c_i \in \boldsymbol{C}$

Para el caso de una cifra de sustitución mono alfabética se tiene:

$\boldsymbol{M} \equiv \{a_1, ..., a_n\}$ donde “n” es el tamaño del alfabeto utilizado.

Criptografía histórica

Transformación de encripción / desencripción

M $\equiv \{a_1, ..., a_n\}$

La transformación de encripción $\mathbf{E_K(M)}$ se puede ver como una simple función de transformación ***f( )*** que mapea ***M*** en ***C***

C $\equiv \{f(a_1), ..., f(a_n)\}$

Si el mensaje es:

$$M = m_1, m_2, ..., m_i, ...$$

Entonces:

$$C = E_K(M) = f(m_1), f(m_2), ..., f(m_i), ...$$

Criptografía histórica

Algoritmo de encripción

$$f(i) = (i+k) \bmod n$$

Para el caso de cifra del cesar, k = 3 y n = 26, y si desea encriptar el mensaje

M = *brutus* ≡ 1, 17, 20, 19, 20, 18

$C = E_K(M) \equiv f(b), f(r), f(u), f(t), f(u), f(s)$

f(1) = (1+3) mod 26 = 4 *f(17) = (17+3) mod 26 = 20*

f(20) = (20+3) mod 26 = 23 *f(19) = (19+3) mod 26 = 22*

f(20) = (20+3) mod 26 = 23 *f(18) = (18+3) mod 26 = 21*

C ≡ 4, 20, 23, 22, 23, 21

C = EUXWXV

Algoritmo de desencripción

$$f^{-1}(i) = (i - k) \bmod n$$

$D_3(C) = D_3(E_3(\text{“brutus”}))$

$= D_3(\text{“}EUXWXV\text{“})$

$=$ “brutus”

Cifra de Sustitución Mono alfabética Genérica

Es una extensión, con un modo mas “operativo” de especificar la clave:

- Escribir la clave eliminando las letras repetidas.
- Escribir el resto de las letras del alfabeto encolumnadas bajo la clave.
- Escriba el alfabeto cifrado, bajo el alfabeto plano, leyendo por columna

Criptografía histórica

Ej: Palabra clave: "STARWARS".

STARW
BCDEF
GHIJK
LMNOP
QUVXY
Z

Leo columnas para obtener el alfabeto cifrado:

Alfabeto Plano: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Alfabeto Cifrado: **SBGLQZTCHMUADINVREJOXWFKPY**

Plaintext: I KNOW ONLY THAT I KNOW NOTHING
Ciphertext: H UINF NIAP OCSO H UINF INOCHIT

Criptografía histórica

Cifra Cesar con alfabeto mixto

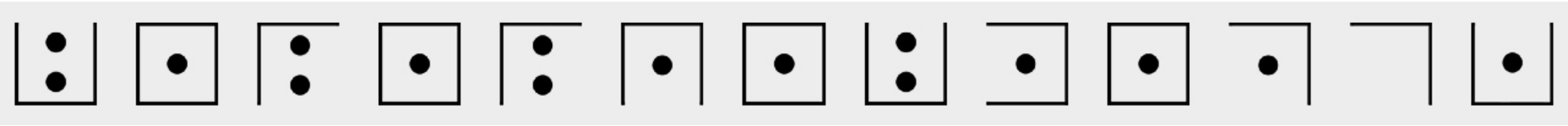
M_i:	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Ci:	[	!	”	{	$	%	&	/	(	)	=	?	¿	¡	]	1	2	3	4	5	6	7	8	9	0	}

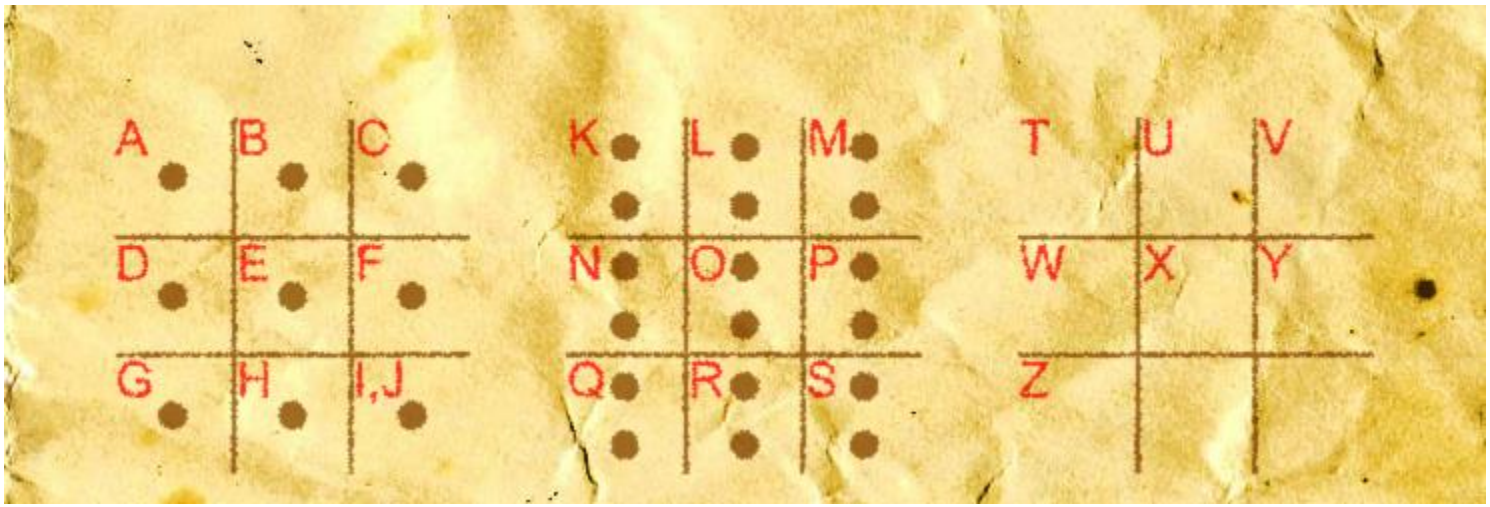
Criptografía histórica

Una tumba con enigma en Trinity Church

Criptografía histórica

Una tumba con enigma en Trinity Church





Criptografía histórica

Algunas consideraciones sobre su seguridad

- Tiene una total de 26! ~ $4x10^{26}$ posibles claves
- Con este número de claves, podría considerarse muy segura..!!
- Se usaron variaciones de esta cifra en muchos conflictos oficiales y militares por muchos siglos hasta entrada la edad media

Criptografía histórica

- Se estima que existen más de cien mil millones (100 000 000 000) de galaxias en el universo.
- **Total número de estrellas** = 300 mil trillones = **3×10^{23}**
- **Total número de granos de arena** en la tierra = **56×10^{20}**
- Total de posibles claves = 26! ~ 4×10^{26}

Parece muy convincente..!!

¿ Por qué se dejo de utilizar ?

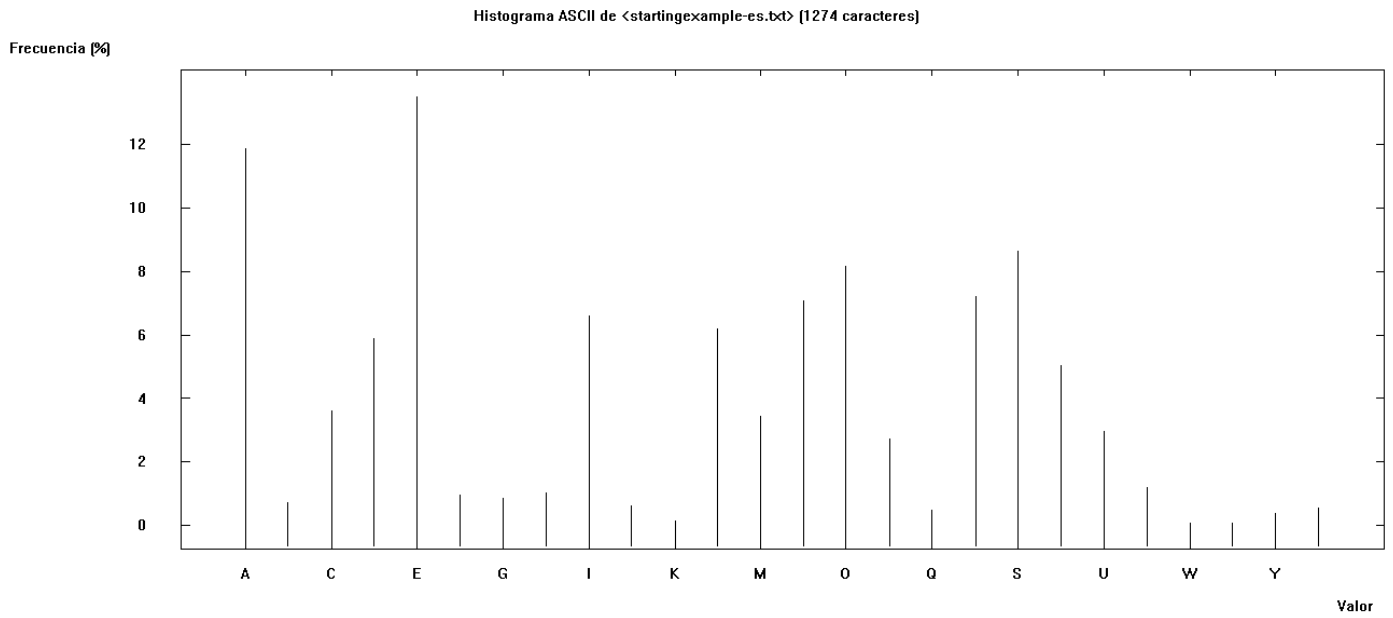
Criptografía histórica

Matemáticas, Estadísticas, Lingüística, Teología..!!

Criptografía histórica

Los Hermanos Musulmanes convocaron hoy a "día de ira" con nuevas manifestaciones en El Cairo después de que casi 600 personas murieran en la represión de los últimos días ante la cual la ONU pidió un "máximo de contención" a todos los bandos.

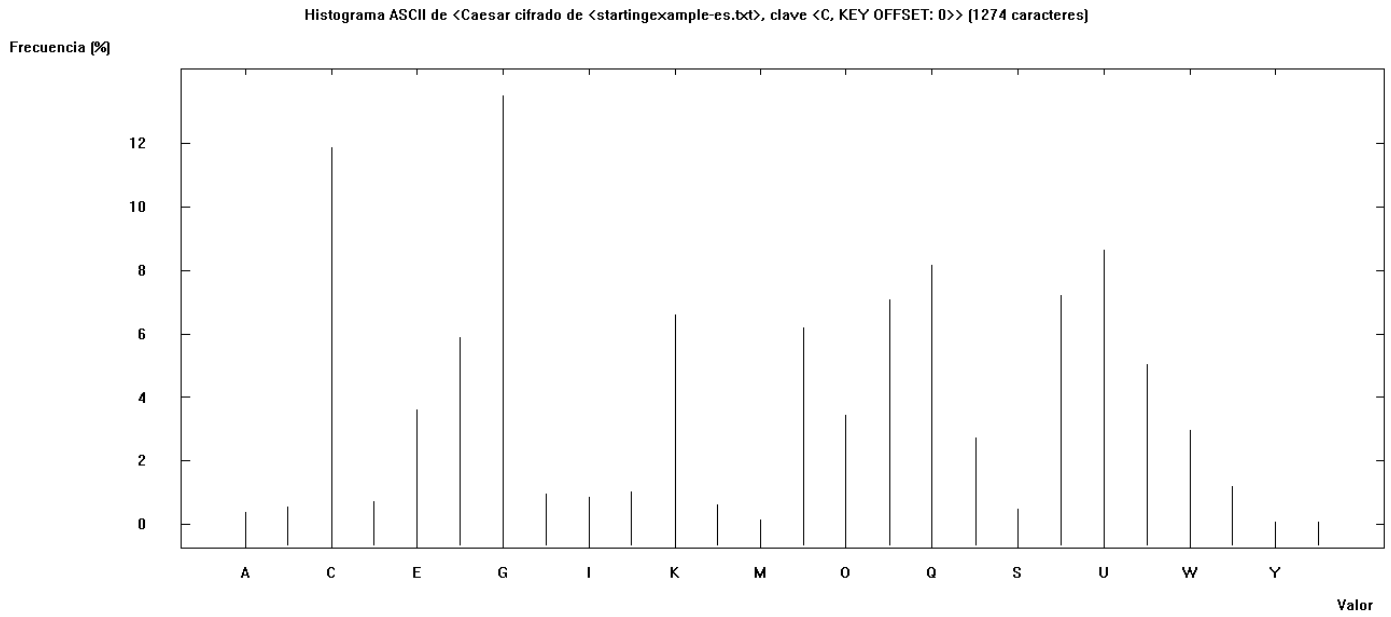
Esta nueva convocatoria hace temer otra jornada de violencia en el país, donde el balance de muertos por el violento nte islamista Mohamed dejaron 578 muertos, s Los Herma en la jornada más sangr Este "viern Hollande, se entrevistar con el primer ministro br Las autori balas reales contra los "Las manif zquitas de El Cairo y se ó el portavoz de la cofradía islamista, Gehad El Haddad, en su cuenta Twitter el jueves.



Laila Musa, portavoz de la Coalición pro-Mursi contra el "golpe de Estado", informó de que se prevén protestas similares en todo el país.

Criptografía histórica

Nqu Jgtocpqu Owuwnocpgu eqpxqectqp jqa c "fíc fg ktc" eqp pwgxcu ocpkhguvcekqpgu gp Gn Ecktq fgurwéu fg swg ecuk 600 rgtuqpcu owtkgtcp gp nc tgrtgukóp fg nqu únvkoqu fícu cpvg nc ewcn nc QPW rkfkó wp "qázkog fg eqpvgpekóp" c vgfgu nqu dcpfgu.



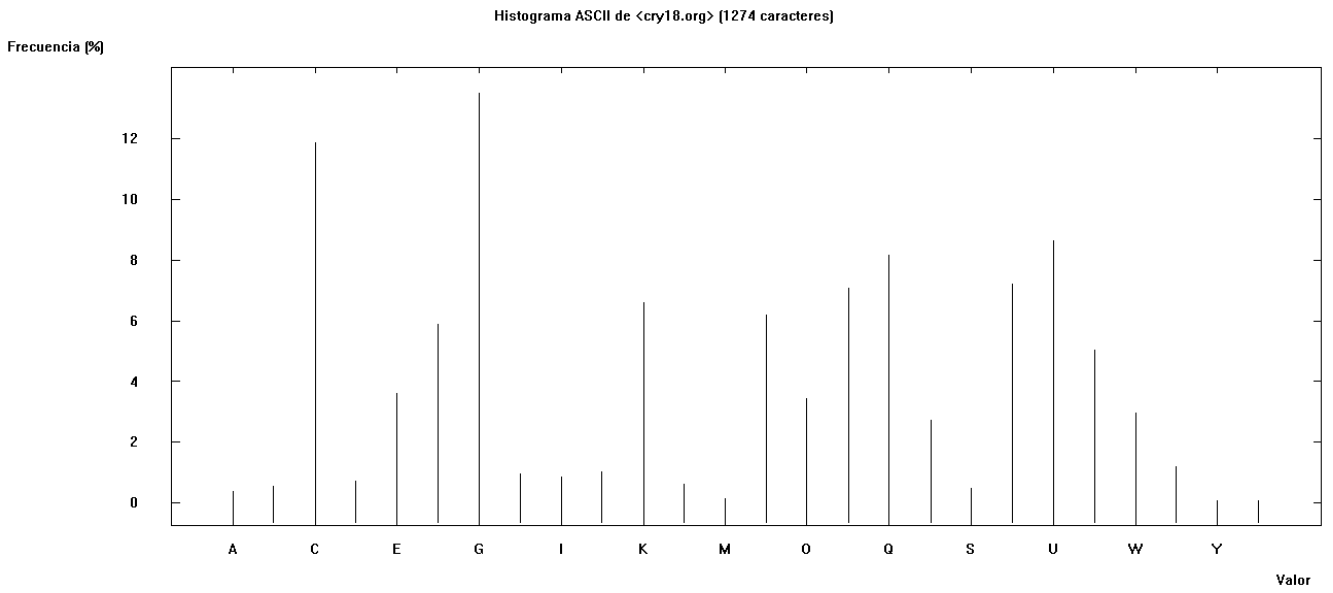
Guvc pwgx g owgtvqu rqt
gn xkqngp g kuncokuvc
Oqjcogf O u fglctqp 578
owgtvqu, u
Nqu Jgtocp ıc lqtpcfc oáu
ucpitkgpvc
Guvg "xkg éu, Htcpçqku
Jqnncpfg, ; Ogtmgn, a
rquvgtkqto
Ncu cwvqt dcncu tgcngu
eqpvtc nqu

"Ncu ocpkl iguvcekqpgu eqpvtc gn iqnrg fg Guvcfq ochcpc (xkgtpgu) dcnntap fg vqfcu ncu ogbswkvcu fg Gn Ecktq a ug fktkiktáp jcekc nc rncbc Tcougu vtcu nc qtcekóp rqt wp "xkgtpgu fg nc eóngtc'", rtgekuó gn rqtvcxqb fg nc eqhtcfíc kuncokuvc, lgjcf Gn Jcffcf, gp uw ewgpvc Vykvvgt gn lwgxgu.

Nckncc Owuc, rqtvcxqb fg nc Eqcnkekóp rtq-Owtuk eqpvtc gn "iqnrg fg Guvcfq", kphqtoó fg swg ug rtgxép rtqvguvcu ukoknctgu gp vqfq gn rcíu.

Criptografía histórica

NQUJG TOCPQ UOWUW NOCPG UEQPX QECTQ PJQAC FCFGK TCEQP PWGXC UOCPK HGUVC EKQPG
UGPGN ECKTQ FGURW UFGSW GECUK RGTUQ PCUOW TKGTC PGPNC TGRTG UKPFG NQUNV KOQUF
CUCPV GNCEW CNNCQ PWRKF KWPOZ KOQFG EQPVG PEKPC VQFQU NQUDC PFQUG UVCPW GXCEQ
PXQEC VQTKC JC ¡O WGTVQ
URQTG NXKQN GI /G UFGNR
TGUKF GPVGK UI JR QUVGT
KQTGU GPHTG PV FN QUJGT
OCPQU OWUWN (¡OU UCPIT
KGPVC GPGIK RV ¡E NGTCU
WUEKV CKPSW K(GP VTGXK
UVCTG UVCVC TF ¿T OGPVG
EQPGN RTKOG T(¡UK IPCFC
URQTG NGLTE KV JO CPKHG
UVCPV GUSWG (¿K HGUVC
EKQPG UEQPV TC JF GGNEC
KTQAU GFKTK IK TC RTGEK
UGNRQ TVCXQ BFGNC EQHTC FCKUN COKUV CIGJC FGNJC FFCFG PUWEW GPVCV YKVVG TGNLW GXGUN
CKNCO WUCRQ TVCXQ BFGNC EQCNK EKPRT QOWTU KEQPV TCGNI QNRGF GGUVC FQKPH QTOFG SWGUG
RTGXP RTQVG UVCUU KOKNC TGUGP VQFQG NRCU



Criptografía histórica

Uso del Análisis de Frecuencia en Criptoanálisis

- Disponer de frecuencia de letras del lenguaje
- Calcular frecuencia de letras de texto cifrado a analizar
- Comparar el gráfico obtenido con el del lenguaje
- Observar picos y valles mas comunes
- Picos en: A-E-I triple espacio, el par NO, la terna RST con la forma de la U; valles en: JK, X-Z

Concepto clave

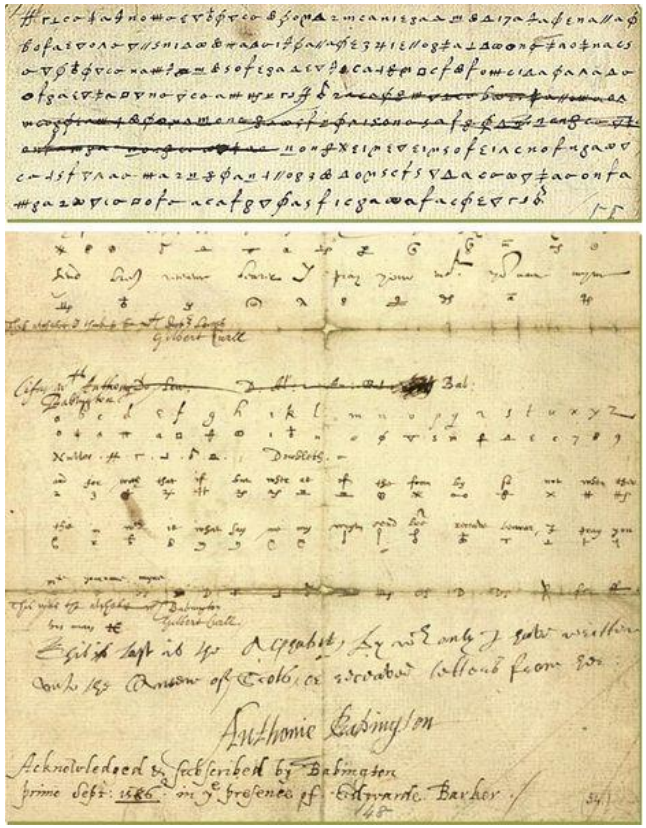
La sustitución mono alfabética no cambia la frecuencia de las letras..!!

Pero me sigue gustando…

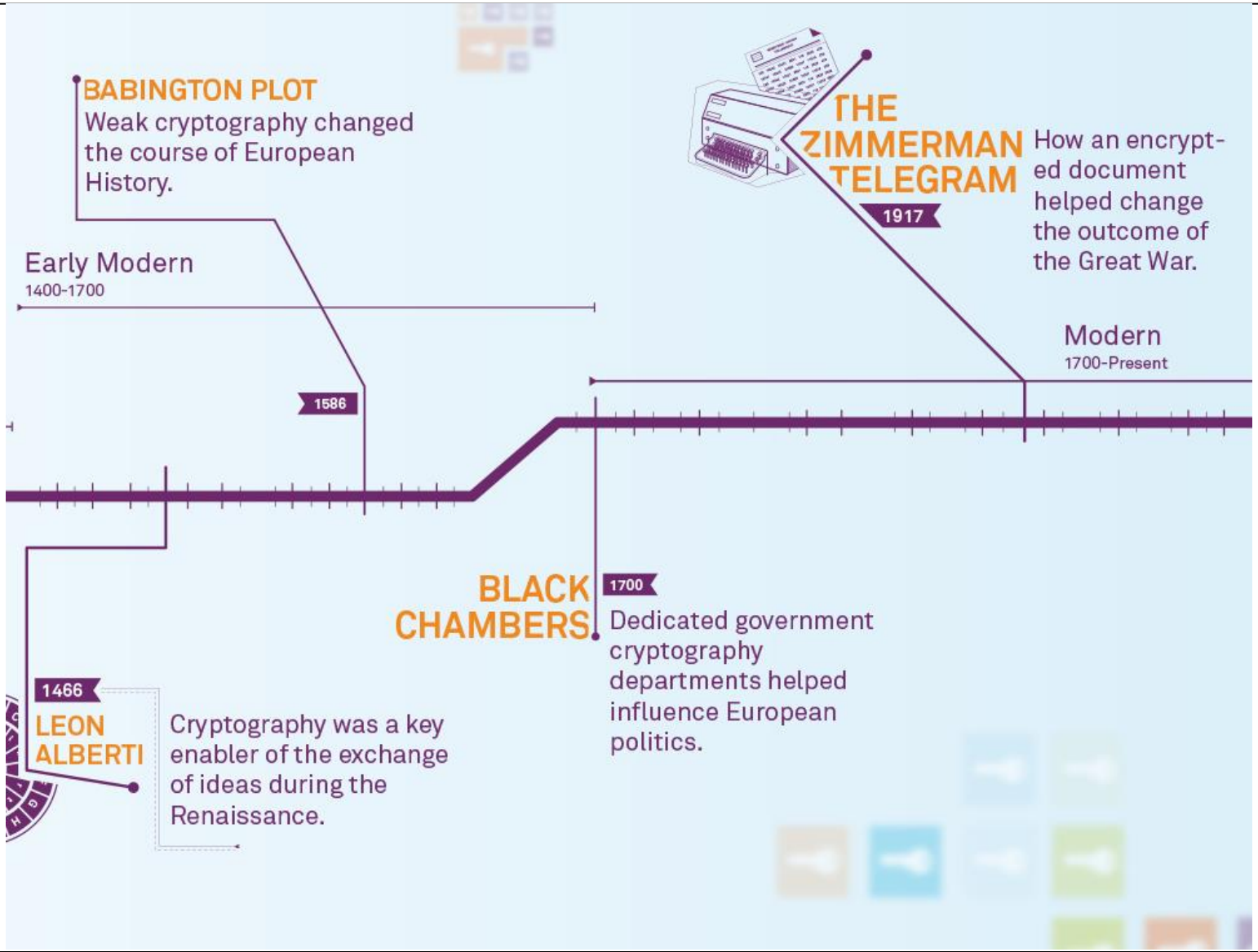
¿ Por qué se dejo de utilizar ?

Criptografía histórica

Quedó fuera de uso a partir de la ejecución de **María Estuardo**, Reina de Escocia (1586), por conspiración..!!



Criptografía histórica



Criptografía histórica

Desarrollos en la Edad Media

- **Roger Bacon (1214-1294)** describe varios métodos para asegurar la escritura.
- **Geoffrey Chaucer (1340-1400)** incluyó varios trabajos sobre cifra.
- En el 1412 se describieron en enciclopedias los conocimientos Árabes sobre cifra.
- Creció su uso y ataque en ámbitos diplomáticas en el sur de Europa (actual Italia).
- **León Alberti (1404-1472)** da un gran avance al plantear el concepto de alfabetos alternados para la codificación

Criptografía histórica

Desarrollos en la Edad Media

- **Blaise de Vigenère** publicó *"Traicté des Chiffres"* en 1585..!!
- Se le acredita ser el inventor de la **cifra de sustitución poli alfabética**
- Para mejorar la seguridad usa **varios** alfabetos de sustitución mono alfabética

Criptografía histórica

Ejemplo de cifra Vigenère

- Escribir el texto plano o mensaje
- Debajo escriba la palabra clave repetidas veces
- Use c/letra de la clave como si fuese la clave de una cifra del Cesar

```
Plaintext  THISPROCESSCANALSOBEEXPRESSED
Keyword    CIPHERCIPHERCIPHERCIPHERCIPHE
Ciphertext VPXZTIQKTZWTCVPSWFDMTETIGAHLH
```

Criptografía histórica

Ejemplo de cifra Vigenère

Palabra clave = CIPHER

Produce la siguiente transformación alfabética:

```
      ABCDEFGHIJKLMNOPQRSTUVWXYZ
C ->  CDEFGHIJKLMNOPQRSTUVWXYZAB
I ->  IJKLMNOPQRSTUVWXYZABCDEFGH
P ->  PQRSTUVWXYZABCDEFGHIJKLMNO
H ->  HIJKLMNOPQRSTUVWXYZABCDEFG
E ->  EFGHIJKLMNOPQRSTUVWXYZABCD
R ->  RSTUVWXYZABCDEFGHIJKLMNOPQ
```

Criptografía histórica

La cifra Vigenère

- Mas segura. Difícil de usar. Por mucho tiempo se uso la cifra de sustitución mono alfabética.
- La mayoría de las naciones crearon **Black Chambers** para romper cifras.
- Esto impulsó el uso gradual y general de cifra vigenère.
- El nuevo “comercio electrónico” del telégrafo la favoreció.
- Se conoció por algún tiempo como *le chiffre indéchiffrable.*
- **Charles Babbage** la quebró (1854 - lo mantuvo en secreto).
- **Friedrich Kasiski** desarrolló y publicó el ataque en 1863.
- Se continuó usando hasta entrado el siglo XX.

Criptografía histórica

Cifras de sustitución polialfabética

- Cifra de sustitución periódica
- Cifra de clave deslizante
- Cifra de cuaderno de uso único

Criptografía histórica

Transformación de encripción / desencripción

$$C = E_K(M)$$

$$M = D_K(C) = D_K[E_K(M)]$$

$M = m_1, m_2, ..., m_i, ... ;$ donde $m_i \in \mathcal{M}$

$K = k_1, k_2, ..., k_i, ... ;$ donde $k_i \in \mathcal{K}$

$C = c_1, c_2, ..., c_i, ... ;$ donde $c_i \in \mathcal{C}$

Criptografía histórica

Cifra de sustitución periódica

La clave se repite luego de un período "***d***" de texto plano.

La transformación de encripción se expresa como un conjunto de "***d***" funciones de mapeo correspondientes a los "***d***" diferentes elementos de la clave.

$$K = k_1, ..., k_d$$

$$f_i : \mathcal{M} \Rightarrow C_i, \text{ para } 1 \leq i \leq d$$

$\mathcal{M} = \{a, b, c, ..., x, y, z\}$ (texto plano)

$C_1 = \{V, G, D, ..., C, X, E\}$ (alfabeto cifrado #1)

$C_i = \{E, Q, S, ..., H, V, T\}$ (alfabeto cifrado #i)

$C_d = \{T, B, N, ..., P, G, W\}$ (alfabeto cifrado #d)

Criptografía histórica

Cifra de sustitución periódica

Para la secuencia que representa un mensaje:

$$M = m_1, m_2, ..., m_{d-1}, m_d, m_{d+1}, m_{d+2}, ..., m_{2d-1}, m_{2d}, m_{2d+1}, m_{2d+2}, ...$$

$$\mathbf{C = E_K(M)}$$

$$C = f(m_1),..., f(m_{d-1}), f(m_d), f(m_{d+1}), f(m_{d+2}),..., f(m_{2d-1}), f(m_{2d}), f(m_{2d+1}), f(m_{2d+2}), ...$$

La cifra ***Vigenère*** es una cifra de sustitución de desplazamiento alfabético periódico. Se inspiró en la cifra de desplazamiento del Cesar. Hay ***d*** funciones de mapeo:

$$f_i(m) = (m + k_i) \bmod n \quad \text{para } \boldsymbol{i = 1} \text{ hasta } \boldsymbol{d}$$

$$f_i^{-1}(c) = (c - k_i) \bmod n \quad \text{para } \boldsymbol{i = 1} \text{ hasta } \boldsymbol{d}$$

Criptografía histórica

Cifra de sustitución periódica: *Vigenère*

M = p e r i o d i c s h i f t e d a l p h a b e t i c s u b s

K = v i g e n e r e v i g e n e r e v i g e n e r e v i g e n

C = K M X M B H Z G N P O J G I U A D X N A O I K M X A A F F

M = t i t u t i o n c i p h e r

K = e r e v i g e n e r e v i g

C = X Z X P B O S A G Z T C M X

Criptografía histórica

Esto me gusta mas que el anterior..!!

¿ Por qué se dejo de utilizar ?

Criptografía histórica

Cifra de sustitución periódica, método Kasiski de criptoanálisis

Este método fue desarrollado por Babbage y Kasiski

Usa las repeticiones de texto en el texto cifrado para determinar un período de repetición que estará relacionado con la longitud de la clave

Podría deberse a un flujo randómico, pero es menos probable..!

Ej.:	Plaintext:	**TOBE**ORNOT**TOBE**
	Key:	**NOWN**OWNOW**NOWN**
	Ciphertext:	**GCXR**CNACP**GCXR**

Criptografía histórica

Cifra de sustitución periódica, método Kasiski de criptoanálisis

- Observar la repetición "GCXR" en el texto cifrado
- Dado que la repetición se da después de 9 letras, es período es 3 o 9
- En general busca secuencias duplicadas
- Registra todas las “distancias” y busca los factores comunes
- Recordar que algunas repeticiones se deberán a la naturaleza randómica y deberán ser descartadas

Criptografía histórica

Cifra de sustitución periódica, método Kasiski de criptoanálisis

- Determinar del periodo ***d*** de la cifra poli alfabética
- Formar las siguientes ***d*** sub secuencias de texto cifrado:

$s_1 = c_1, c_{d+1}, c_{2d+1}, \cdots$
$s_2 = c_2, c_{d+2}, c_{2d+2}, \cdots$
$\vdots$
$s_d = c_d, c_{2d}, c_{3d}, \cdots$

- Aplicar el AF sobre c/u de las sub secuencias y tratar de determinar los ***d*** mapeos de sustitución simple

$\mathcal{M} \Rightarrow C_1$
$\mathcal{M} \Rightarrow C_2$
$\vdots$
$\mathcal{M} \Rightarrow C_d$

Para luego recuperar el texto plano

∃ alguna otra forma de criptoanalizar esto ..?

Si se dispone de una cantidad apreciable de texto cifrado, se pueden evaluar una serie de parámetros que nos permita determinar el valor del período ***d*** de la cifra polialfabética.

Criptografía histórica

Cifra de sustitución periódica, método de Indice de coincidencia

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVXUOAKXAOSXXWEA
HBWGJMMQMNKGRFVGXWTRZXWIAKLXFPSKAUTEMNDCMGTSXMXBTUIADNGMGP
SRELXNJELXVRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLL**CHR**ZBWELE
KMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLXRRIMGNS
NRW**CHR**QHAEYEVTAQEBBIPEEWEVKAKOEWADREMXMTBHH**CHR**TKDNVRZ**CHR**CL
QOHPWQAIIWXNRMGWOIIFKEE

Para n=2,	IC(CREOH...) = 0.046
	IC(HEVAM...) = 0.041
Para n=3	IC = 0.043; 0.050; 0.047
Para n=4	IC = 0.042; 0.039; 0.046; 0.040
Para n=5	IC = 0.063; 0.068; 0.069; 0.061; 0.072 ...

Criptografía histórica

Cifras de sustitución polialfabética

- ~~Cifra de sustitución periódica~~
- Cifra de clave deslizante
- Cifra de cuaderno de uso único

Criptografía histórica

Cifra de sustitución de clave deslizante

Cifra de sustitución poli alfabética no periódica o con un valor ***d*** de la clave tan grande como el texto plano a cifrar. Cómo se uso esta cifra ..?

Se toma la clave de libros, páginas, párrafos, frases, específicos.

La seguridad depende del secreto del texto..!

Ej.:

```
M = t h e t r e a s u r e i s b u r i e d...
K = t h e s e c o n d c i p h e r i s a n...
C = M O I L V G O F X T M X Z F L Z A E Q...
```

Es una cifra donde la clave tiene tantos elementos como el texto plano..!

Criptografía histórica

Cifra de sustitución de clave deslizante

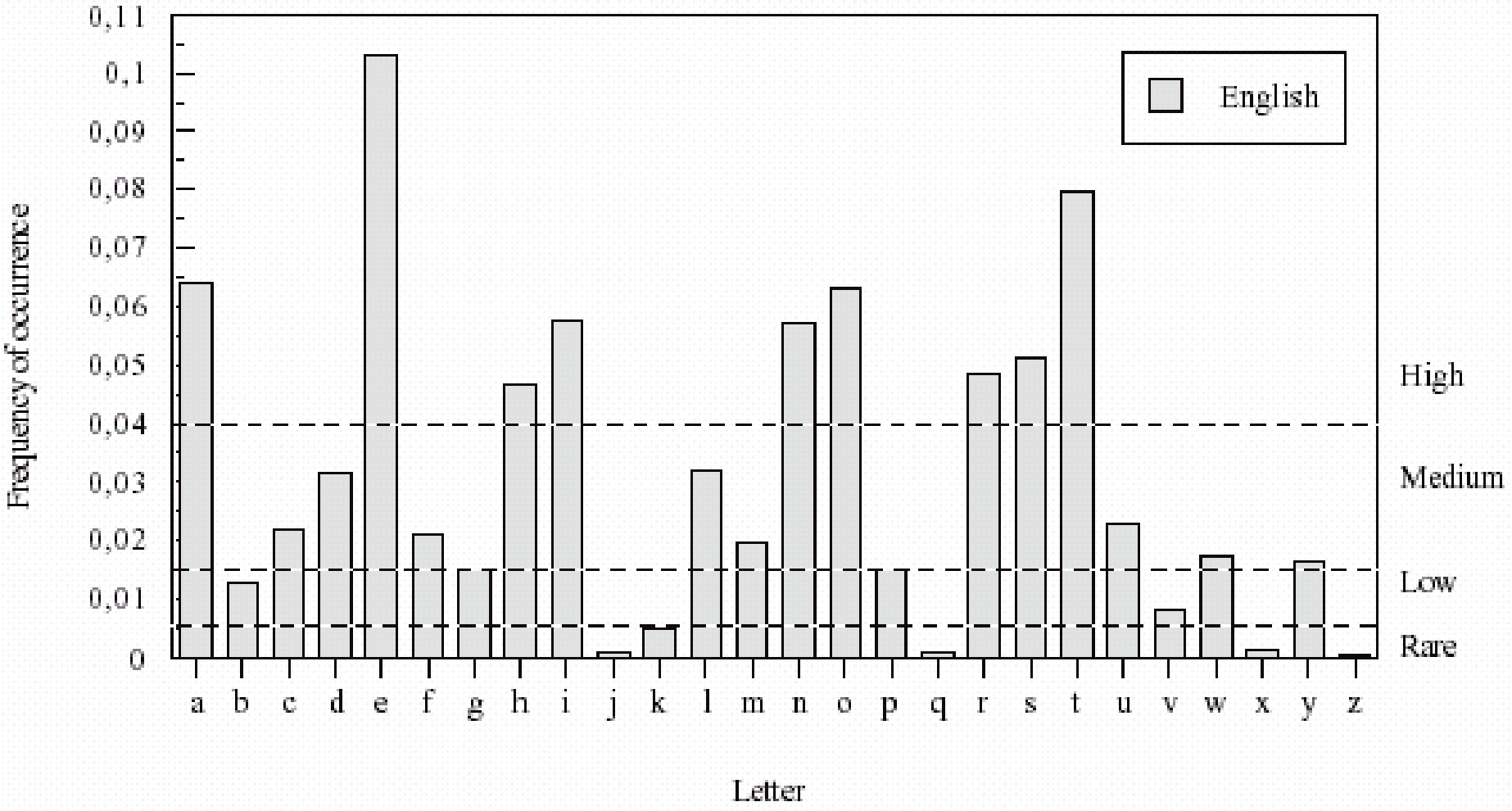
```
M = t h e t r e a s u r e i s b u r i e d...
K = t h e s e c o n d c i p h e r i s a n...
C = M O I L V G O F X T M X Z F L Z A E Q...
```

Dado que la fuente de la clave no es equiprobable, algunos símbolos del texto cifrado tenderán a aparecer mas frecuentemente que otros. Friedman propone un criptoanálisis basado en las frecuencias relativas.

Muchos símbolos del texto cifrado $\{c_i\}$ son el resultado de cifrar letras de texto plano de alta frecuencia $\{m_i\}$ con letras de la clave también de alta frecuencia $\{k_i\}$.

Criptografía histórica

Cifra de sustitución de clave deslizante



Criptografía histórica

Cifras de sustitución polialfabética

- ~~Cifra de sustitución periódica~~
- ~~Cifra de clave deslizante~~
- Cifra de cuaderno de uso único

Criptografía histórica

Cifra de cuaderno de uso único

La cifra **Vernam** o cifra de cuaderno de uso único es también una cifra de clave deslizante incondicionalmente segura.

La clave ***K*** es totalmente randómica y nunca se repite o usa mas de una vez, de allí el nombre.

$M = m_1 \quad m_2 \quad \ldots \quad m_n \quad \ldots$

$\mathbf{C} = \mathbf{k}_1 \quad k_2 \quad \ldots \quad k_n \quad \ldots$

$C = f_{k1}(m_1) \quad f_{k2}(m_2) \quad \ldots \quad f_{kn}(m_n) \quad \ldots$

Donde la secuencia clave es una secuencia randómica no repetitiva.

Criptografía histórica

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

M = RETIRARSE A LAS COLINAS

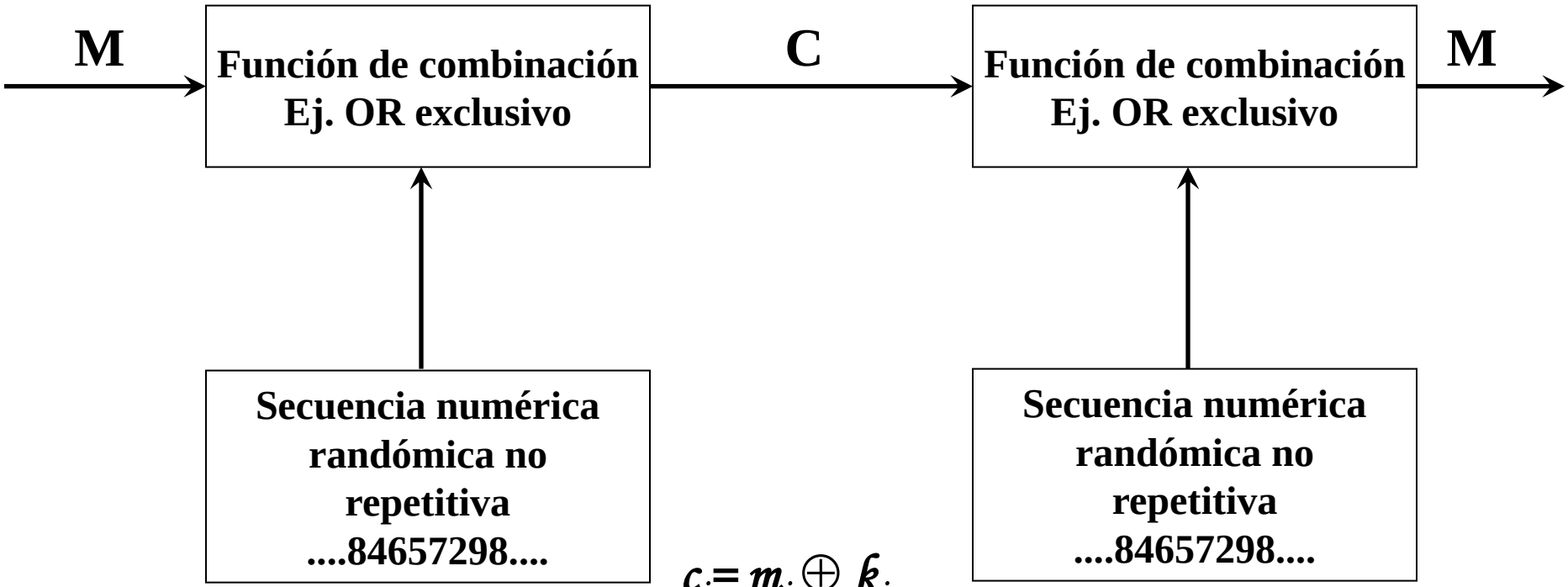
M = RETIRARSEALASCOLINAS

K = HEIBFDGOXTMXZFLZAEQI

C = YIBJWDXGBTXXRHZKIRQA

Criptografía histórica

Cifra de cuaderno de uso único: Ejemplo de cifra Vernan



$$c_i = m_i \oplus k_i$$

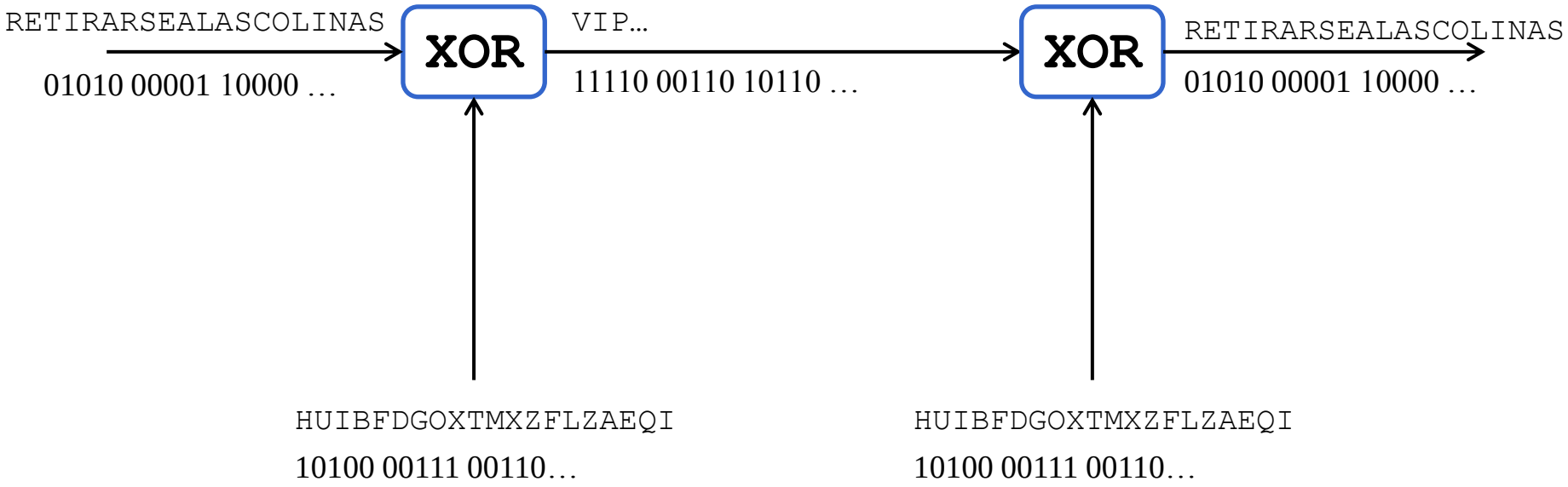
$$m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$$

$$m_i = m_i$$

Criptografía histórica

OTP con código Baudot de 5 bits

M = RETIRARSE A LAS COLINAS



Criptografía histórica

Cifras de sustitución polialfabética

- ~~Cifra de sustitución periódica~~
- ~~Cifra de clave deslizante~~
- ~~Cifra de cuaderno de uso único~~

Criptografía histórica

Cifras de sustitución poligrámica monoalfabética

- Cifra Playfair

  Cifra digrámica popularizada por Lyon Playfair (1818-1898) inventada por Charles Wheatstone (1802-1875), uno de los pioneros del telégrafo. Trabaja con una matriz de 5x5 ó 6x6 y se aplican las siguientes reglas:

- Cifra Hill

  Fue Inventado por Lester S. Hill (1891-1961) en 1929 y se basa en el álgebra lineal. Fue el primer sistema criptográfico polialfabético que era práctico para trabajar con mas de tres símbolos simultaneamente.

Cifra Playfair

1. Si $\mathbf{m_1}$ y $\mathbf{m_2}$ están en la misma fila, entonces $\mathbf{c_1}$ y $\mathbf{c_2}$ son los dos caracteres a la derecha de $\mathbf{m_1}$ y $\mathbf{m_2}$, considerando la primera columna a la derecha de la última.
2. Si $\mathbf{m_1}$ y $\mathbf{m_2}$ están en la misma columna, entonces $\mathbf{c_1}$ y $\mathbf{c_2}$ son los dos caracteres debajo de $\mathbf{m_1}$ y $\mathbf{m_2}$, considerando la primera fila debajo de la última.
3. Si $\mathbf{m_1}$ y $\mathbf{m_2}$ están en diferentes filas y columnas, entonces $\mathbf{c_1}$ y $\mathbf{c_2}$ son las otras dos esquinas del rectángulo que forman $\mathbf{m_1}$ y $\mathbf{m_2}$, donde $\mathbf{c_1}$ está en la misma fila de $\mathbf{m_1}$ y $\mathbf{c_2}$ está en la misma fila de $\mathbf{m_2}$.
4. Si $\mathbf{m_1} = \mathbf{m_2}$ se agrega una letra nula (Ej.: X) en el texto plano, entre $\mathbf{m_1}$ y $\mathbf{m_2}$ para eliminar el par.
5. Si el texto plano tiene un número impar de letras, se agrega una letra nula al final.

Criptografía histórica

Ejemplo de Cifra Playfair

Clave : CHARLES

C	H	A	R	L
E	S	B	D	F
G	I	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

Mensaje: NOS VEMOS EN LA CUMBRE

Reordenado: NO SV EM OS EN LA CU MB RE

Cifra : GU EW DG PE FG CR LO KD

Cifra Hill

Realiza una transformación lineal de "d" caracteres del texto plano sobre "d" caracteres del texto cifrado. Suponiendo d = 2 y M = $\mathbf{m_1 m_2}$, entonces M es cifrado como C = E_K (M) = $\mathbf{c_1 c_2}$, donde:

$$c_1 = (k_{11} m_1 + k_{12} m_2) \bmod n$$
$$c_2 = (k_{21} m_1 + k_{22} m_2) \bmod n$$

Lo cual se puede expresar como C = E_K (M) = K M mod n donde C y M son vectores columnas y K la matriz de coeficientes. Esto es:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} \bmod n$$

Luego, bajo determinadas condiciones existe una matriz K^{-1}, que hace $KK^{-1} = I$ que permite descifrar el mensaje.

Criptografía histórica

Veamos algo de cifra de transposición

Criptografía histórica

Cifra de transposición o permutación.

Los sistemas de transposición son diferentes a los sistemas de sustitución.

En los sistemas de sustitución los valores de texto plano son reemplazados por otros valores.

En los sistemas de transposición los valores del texto plano son reordenados sin cambiarlos.

Todos los caracteres del texto plano presentes antes de cifrar, están también en el texto cifrado, pero en un orden diferente.

Si realizamos un análisis de frecuencia de esta cifra, para un texto lo suficientemente largo, no diferirá del lenguaje original.

Criptografía histórica

Cifra de transposición o permutación.

La mayoría de los sistemas reordenan el texto teniendo en cuenta una letra pero es posible reordenar palabras completas o grupos de letras.

Esta aproximación no es muy segura y tiene poco valor práctico.

Existen sistema de transposición simple y doble.

La mayoría de los sistemas de transposición usan procesos geométricos:

El texto plano se escribe dentro de una figura geométrica (rectángulo o cuadrado) y se extrae de la figura por diferentes caminos al usado para entrarla.

Son fáciles de identificar ya que un conteo de frecuencia luce como texto plano.

Criptografía histórica

Cifra reversa (espejo)

Escribir el mensaje de atrás hacia delante

Texto plano: `I CAME I SAW I CONQUERED`

Texto cifrado: `DEREU QNOCI WASIE MACI`

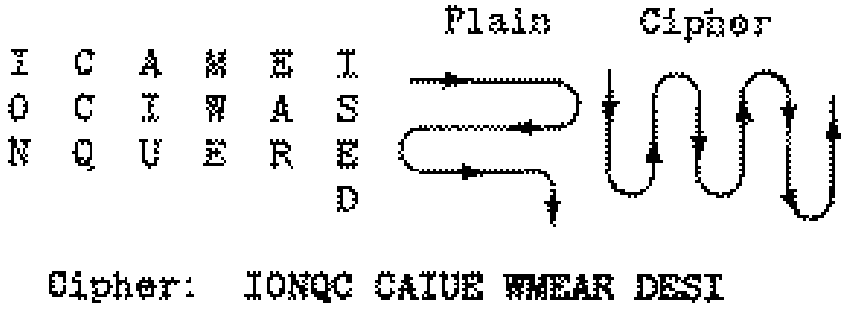
Cifra de doble carril

Escribir el mensaje alternando las letras en dos carriles/filas y luego leer cifra fila a fila

Texto plano:
```
I A E S W C N U R
 D C M I A I O Q E E
```

Texto cifrado: `IAESW CNURD CMIAI OQEE`

Figura geométrica



Criptografía histórica

Concepto de clave en una cifra de transposición

En esta cifra la idea de clave es que Ud.:

- Escribe el mensaje en columnas, siguiendo alguna regla
- Lee el mensaje resultante de alguna otra manera para formar el texto cifrado
- La clave es el orden para: Leer la cifra y escribir el mensaje luego, o ambos a la vez

Criptografía histórica

Un poco de formalidad

La secuencia que representa un mensaje y su cifra serán:

$M = m_1, m_2, ..., m_d, m_{d+1}, m_{d+2}, ..., m_{2d}, m_{2d+1}, m_{2d+2}, ...$

$C = E_K(M)$

$C = m_{f(1)}, m_{f(2)},..., m_{f(d)}, m_{f(d+1)}, m_{f(d+2)},..., m_{f(2d)}, m_{f(2d+1)}, m_{f(2d+2)}, ...$

$C = m_{f(1)}, m_{f(2)},..., m_{f(d)}, m_{d+f(1)}, m_{d+f(2)},..., m_{d+f(d)}, m_{2d+f(1)}, m_{2d+f(2)}, ...$

Donde la función f(i) es la permutación del i-ésimo símbolo del mensaje.

Criptografía histórica

Ej.: Sea la función de permutación f(i)

i = 1, 2, 3, 4, 5, 6

$f(i)$ = 3, 1, 6, 5, 2, 4

Si el mensaje original M es " ...mobile channel is ..."

M = m, o, b, i, l, e, c, h, a, n, n, e, l, ...

M = $m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}, m_{12}, m_{13}, \ldots$

C = $m_{f(1)}, m_{f(2)}, m_{f(3)}, m_{f(4)}, m_{f(5)}, m_{f(6)}, m_{f(7)}, m_{f(8)}, m_{f(9)}, m_{f(10)}, m_{f(11)}, \ldots$

C = $m_{f(1)}, m_{f(2)}, m_{f(3)}, m_{f(4)}, m_{f(5)}, m_{f(6)}, m_{6+f(1)}, m_{6+f(2)}, m_{6+f(3)}, \ldots$

C = $m_3, m_1, m_6, m_5, m_2, m_4, m_{6+3}, m_{6+1}, m_{6+6}, m_{6+5}, m_{6+2}, m_{6+4}, \ldots$

C = $m_3, m_1, m_6, m_5, m_2, m_4, m_9, m_7, m_{12}, m_{11}, m_8, m_{10}, \ldots$

C = B, M, E, L, O, I, A, C, E, N, H, N,

C = "...**BMELOIACENHN**..."

Criptografía histórica

Transposición de ruta

Ejemplos:

			N						M						R						G			
		I		F				E		E				A		R				N		N		
	E				O		C				N		S				I		I				O	
R						R						T						V						W

Ciphertext: NMRGI FEEAR NNEOC NSIIO RRTVW

				R				
			E	I	N			
		F	O	R	C	E		
	M	E	N	T	S	A	R	
R	I	V	I	N	G	N	O	W

Ciphertext:

RMIFE VEONI RIRTN NCSGE ANROW

Criptografía histórica

Criptoanálisis de la cifra de transposición de columnas

- Tiene mucho de prueba y error..!
- Asegurarse de que es una cifra de transposición.
- Use diferentes tamaños de matriz considerando los factores de la longitud del mensaje.
- Pruebe c/uno de ellos a la vez escribiendo la cifra en columnas.
- Busque una forma de reordenar pares de columnas para obtener una terna legible.
- Si tiene herramientas, pruebe con todas las permutaciones.
- Puede probar mostrando sólo aquellas permutaciones que muestren un patrón
- El patrón puede ser una palabra supuesta en el texto.
- O podría asumir que tiene suficiente texto para encontrar palabras comunes como “the” y “and” (preferentemente repetidas).

Criptografía histórica

Todo esto parece ser mas seguro que lo anterior..!!

Criptografía histórica

Mapa de México según su Constitución

1824

Criptografía histórica

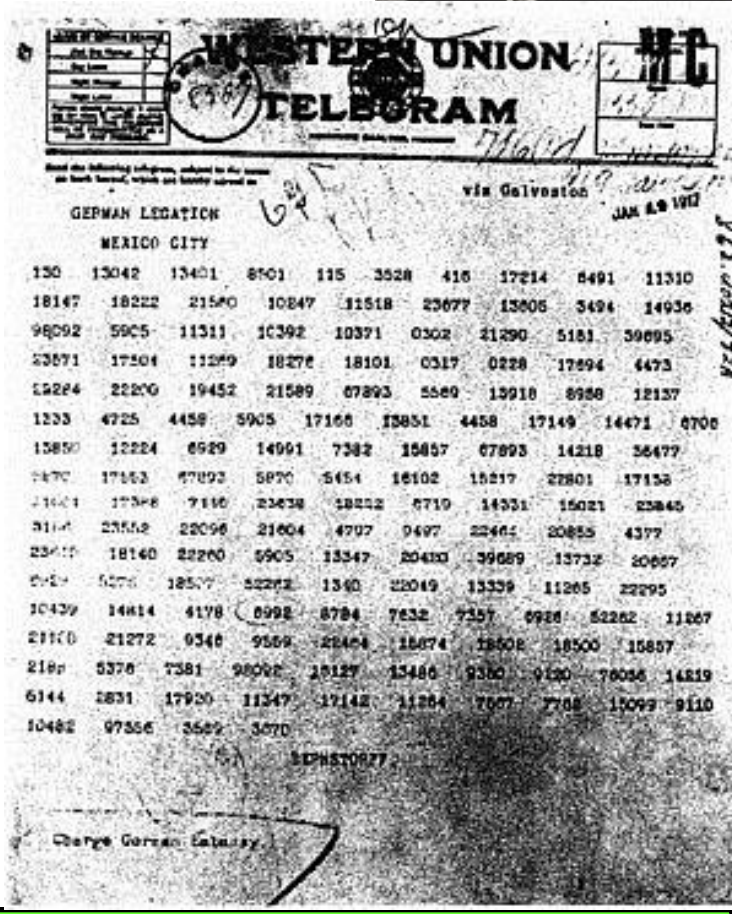
Tratado de Paz, Amistad, Límites y Arreglo Definitivo entre los Estados Unidos Mexicanos y los Estados Unidos de América

1848

Criptografía histórica

En verde claro lo prometido a México!!

1917



WESTERN UNION
TELEGRAM

via Galveston

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10847 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5181 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
13224 22200 19452 21589 67893 5569 13918 8958 12137
1233 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
17163 67893 5870 5454 16102 15217 22801 17138
7186 23638 18232 6719 14331 15021 23845
22096 21604 4797 9497 22464 20855 4377
18140 22260 5905 13347 20439 39689 13732 20667
18577 52262 1340 22049 13339 11265 22295
14814 6178 8998 8784 7632 7357 6928 52262 11267
21272 9348 9559 18474 18502 18500 15857
5378 7381 98092 18127 13486 9360 9130 76036 14819
2831 17920 11347 17142 11264 7607 7708 15099 9110
97556 3582 3070

SEPH5707?

Charge German Legation

Aumentando la seguridad de la cifra

La cifra basada sólo en una sustitución o en una transposición es poco segura y hemos visto cómo atacarla ya que no oscurece suficientemente la estructura del lenguaje.

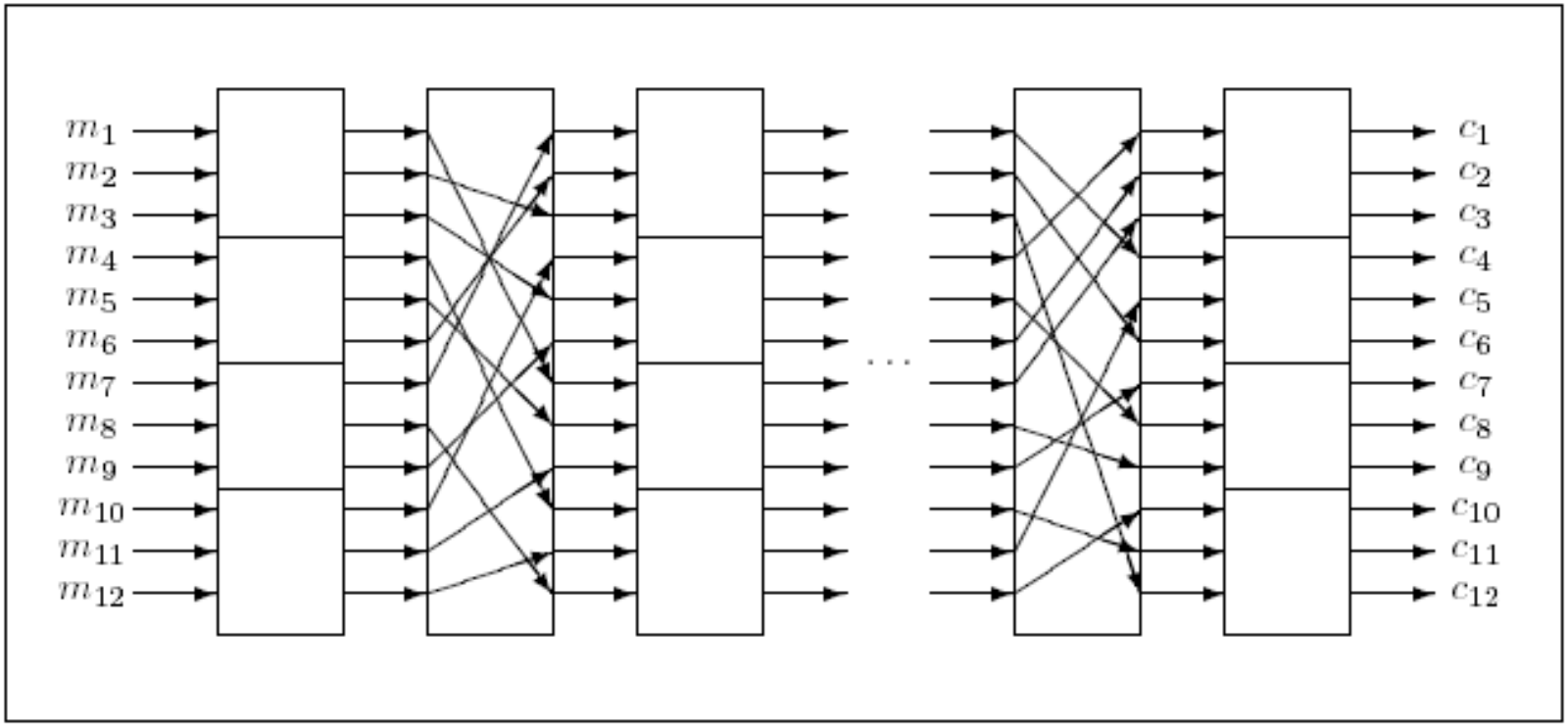
Podemos usar varias cifras en secuencia para hacerla mas fuerte, pero dos sustituciones en realidad es una sustitución mas compleja. Idem para dos transposiciones..!

Pero con una sustitución seguida por una transposición tenemos una nueva cifra mucho mas fuerte...

Criptografía histórica

Cifra de producto

Es una combinación de sustitución-transposición concatenadas y en general es muy complejo realizarlo a mano..!



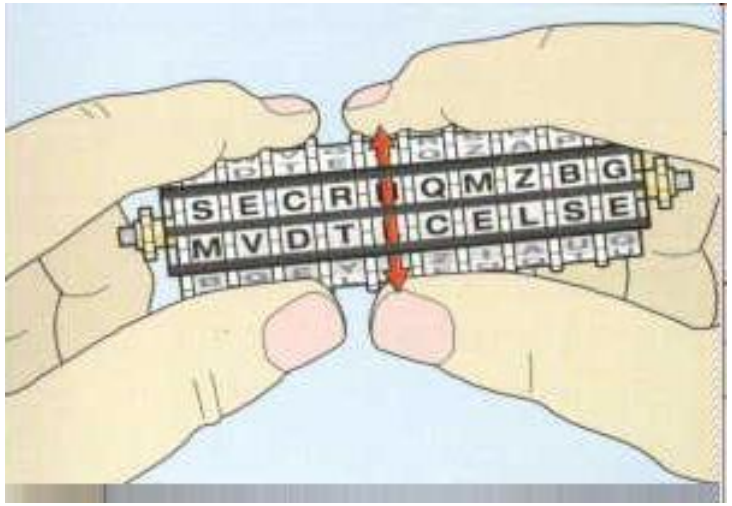
$$C = E_K(M) = S_t \circ P_{t-1} \circ \ldots \circ P_2 \circ S_2 \circ P_1 \circ S_1(M)$$

$$\tilde{M} = D_K(C) = S_1^{-1} \circ P_1^{-1} \circ \ldots \circ P_{t-2}^{-1} \circ S_{t-1}^{-1} \circ P_{t-1}^{-1} \circ S_t^{-1}(C)$$

Criptografía histórica

Máquinas de cifra (1ra generación)

- Se desarrollaron dispositivos mecánicos que facilitaran los procesos de en/desencripción
- El cilindro de **Jefferson***, desarrollado en 1790 estaba compuesto de 36 discos cada uno con un alfabeto randómico

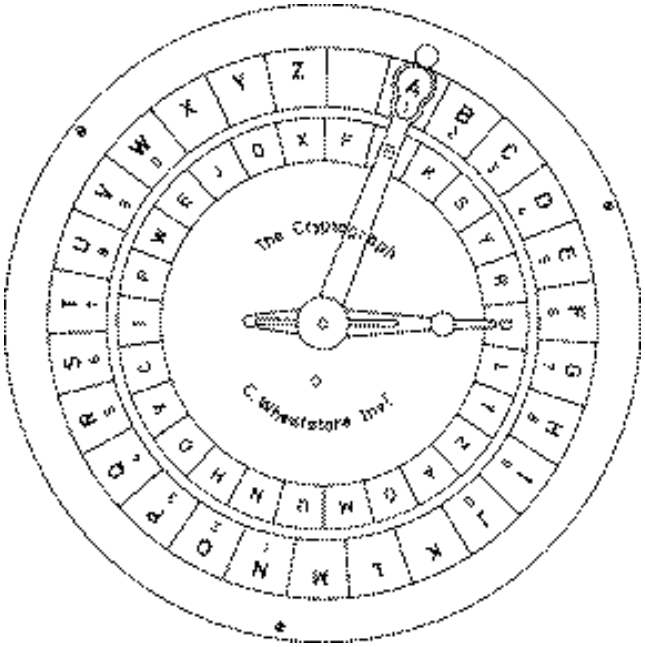


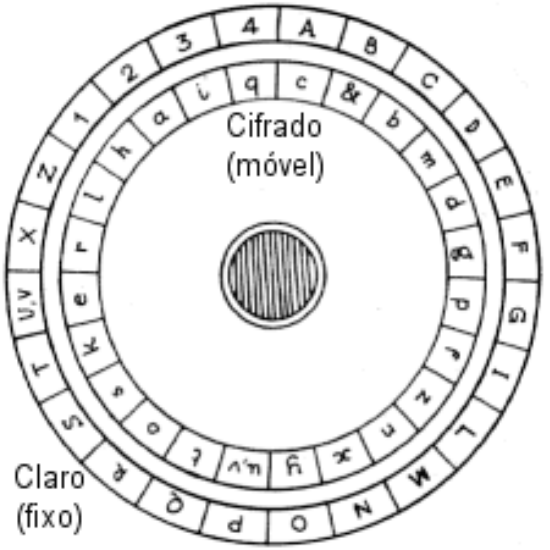
(*) Thomas Jefferson (1743-1826), autor de la Declaración de Independencia de EEUU. El primero en fabricarlo en serie fue Etienne Bazeries en 1891.

Criptografía histórica

Máquinas de cifra (1ra generación)

El disco de Wheatstone, construido en 1860, estaba compuesto por dos discos concéntricos para generar una cifra polialfabética:





Davies Fig 2.18, p29

Criptografía histórica

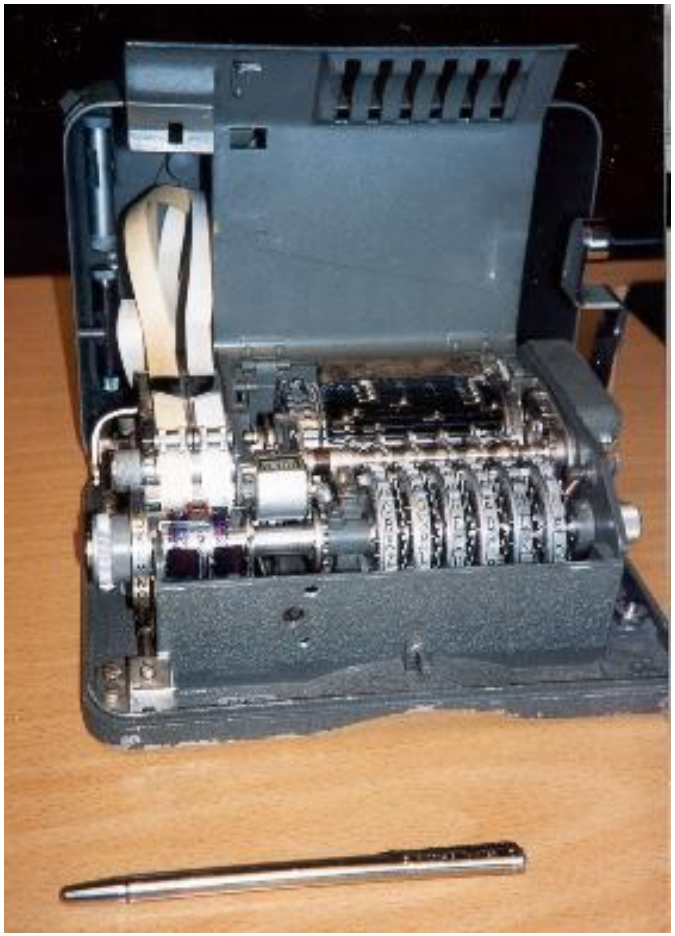
Máquinas de cifra (2da generación)

- El siguiente paso en el crecimiento de la cifra requirió el uso de máquinas de cifra mecánicas
- Estas habilitaron el uso de complejas variaciones de la cifra de sustitución
- Fueron ampliamente usadas en WW2
- La historia de su uso y análisis es una de las historias mas grandes jamas contadas
- Incluyen a la Enigma Alemana, la Hagelin Sueca y la Púrpura Japonesa.

Criptografía histórica

Máquinas de cifra (2da generación)

Hagelin (Suecia)



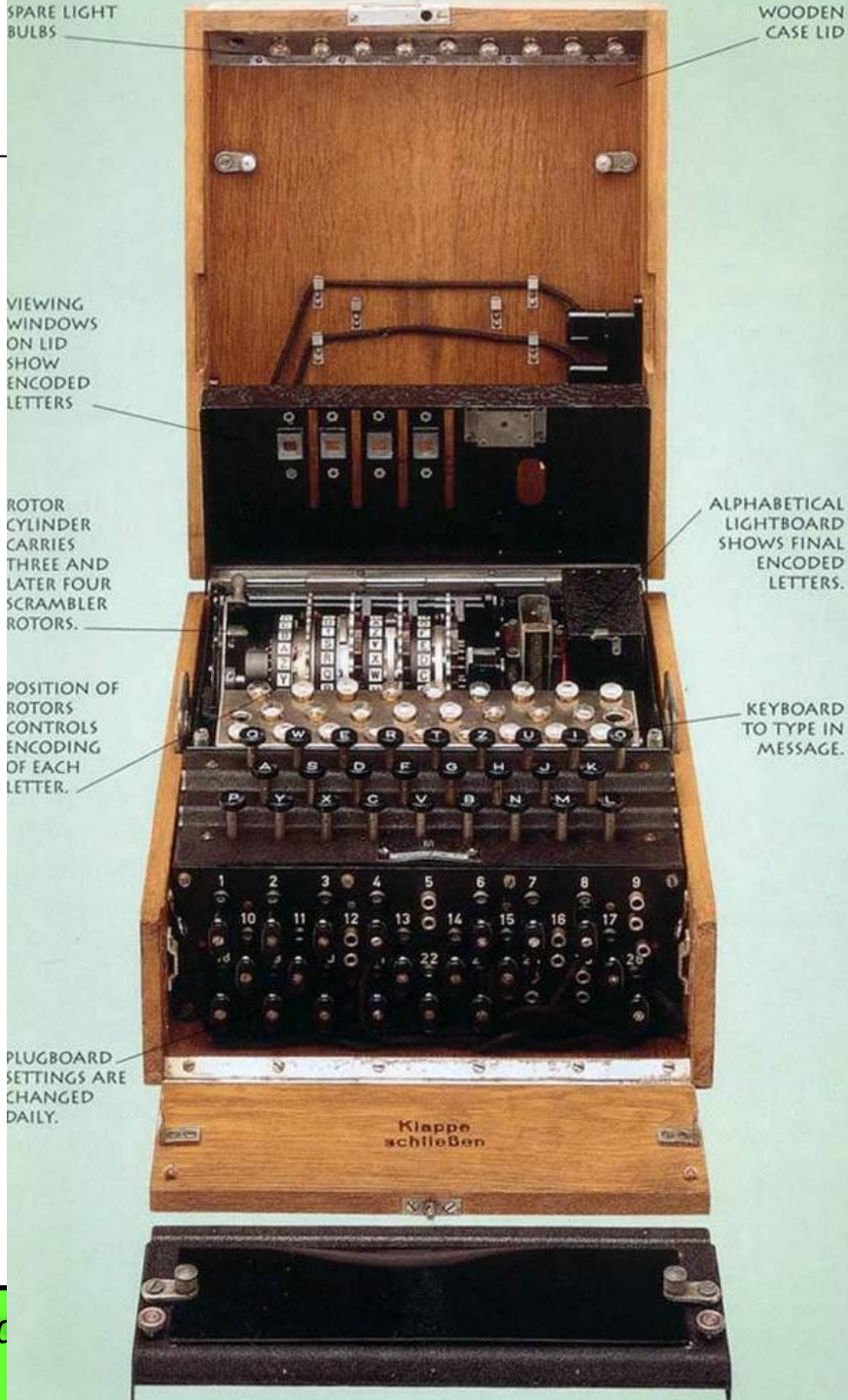
Purpura (Japón)

Criptografía histórica

Interior de una Enigma

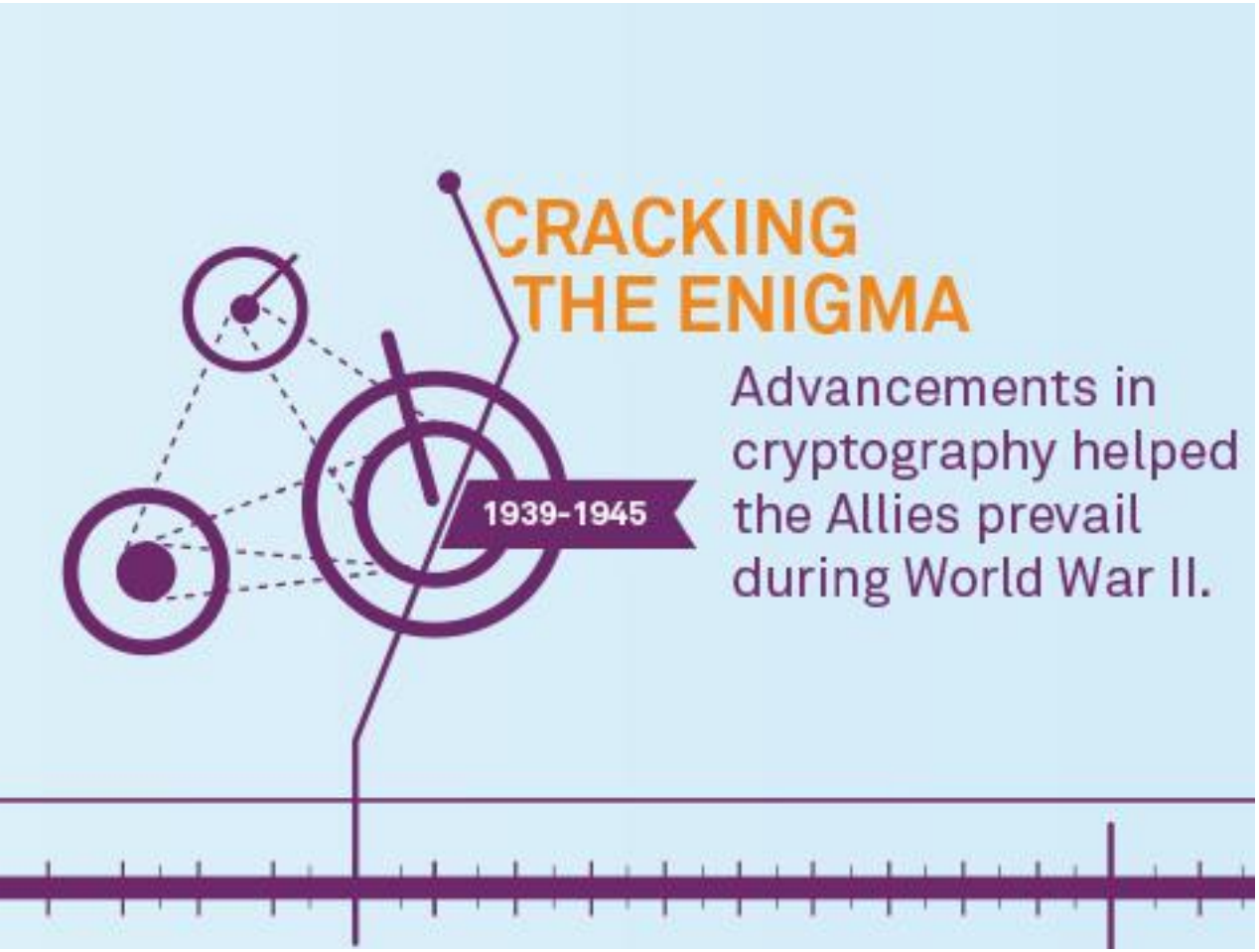
Máquina de rotor, hacía una sustitución de alfabeto de forma continua, usando:

- Un teclado
- Un clavijero para intercambiar letras
- Tres (o mas) discos que sustituían una letra por otra y que rotaban continuamente
- Un reflector que rebotaba la señal hacia los tres discos y el clavijero
- Lámparas que iluminaban c/letra de salida



Criptografía histórica

Que bueno, encontramos al fin algo seguro ?

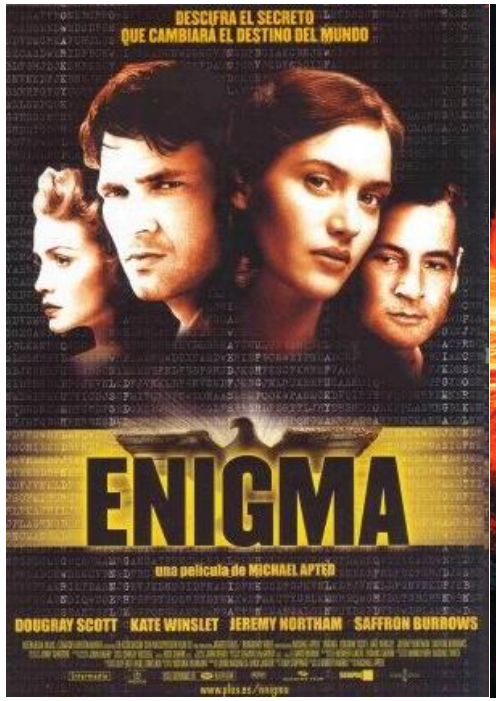


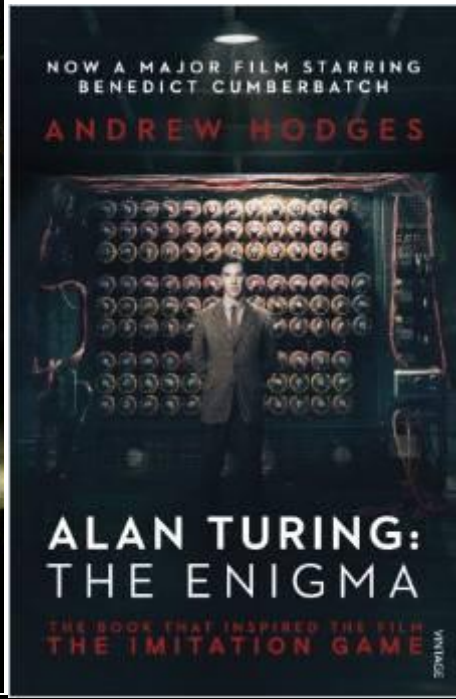
http://www.bletchleypark.org.uk/

Criptografía histórica

Algunas películas

- U 571 (2000)
- Enigma (2001; 2015)
- Códigos de guerra (2002)






GRACIAS!