Criptografía Clásica

DSIC-UPV

2014

Contenido

Bibliografía

- Cryptography: Theory and Practice. Douglas R. Stinson. CRC Press. 1995.
- The codebreakers. David Khan. Scribner. 1996.

Criptoanálisis básico

La seguridad de un sistema criptográfico no depende de mantener en secreto el método de cifrado utilizado

Principios de Kerchhoff (1883)

Sistemas monoalfabéticos

Criptografía de clave simétrica
Cifrado de Polibio (s II a.C.)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	L	M	N	Ñ	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Criptografía de clave simétrica
Cifrado de Polibio (s II a.C.)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	L	M	N	Ñ	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

CAPTURADOAGENTEENDESTINO

$\Downarrow$

131141455143111435112215334515 33...

Sistemas monoalfabéticos
Caesar

Ihuh olehqwhu krplqhv, lg txrg yroxqw, fuhgxqw

Sistemas monoalfabéticos
Caesar

Ihuh olehqwhu krplqhv, lg txrg yroxqw, fuhgxqw

Fere libenter homines, id quod volunt, credunt

Sistemas monoalfabéticos
Caesar

- $e(x) = x + 3 \text{ mód } 27$
- $d(y) = y - 3 \text{ mód } 27$

Sistemas monoalfabéticos
Caesar

- $e(x) = x + 3$ mód 27
- $d(y) = y - 3$ mód 27

Cifrado por desplazamiento:

- $e_k(x) = x + k$ mód 27
- $d_k(y) = y - k$ mód 27

Sistemas monoalfabéticos
Caesar

- $e(x) = x + 3$ mód 27
- $d(y) = y - 3$ mód 27

Cifrado por desplazamiento:

- $e_k(x) = x + k$ mód 27
- $d_k(y) = y - k$ mód 27

Espacio de claves: Desplazamientos posibles

Número de claves: Talla del alfabeto

Sistemas monoalfabéticos: Sustitución simple

- Sustitución simple:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
O	C	T	A	V	I	P	Z	B	D	E	F	G	H	J	K

P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	Ñ	Q	R	S	U	W	X	Y

Sistemas monoalfabéticos: Sustitución simple

- Sustitución simple:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
O	C	T	A	V	I	P	Z	B	D	E	F	G	H	J	K

P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	Ñ	Q	R	S	U	W	X	Y

  - $e_k(x) = \pi(x)$
  - $d_k(y) = \pi^{-1}(y)$

e(CENT RALN UCLE AR) = TVHQ NOFH RTFV ON

Espacio de claves: Permutaciones posibles del alfabeto

Número de claves: (Talla del alfabeto)!

Sistemas monoalfabéticos: Afín

- $e_{a,b}(x) = ax + b$ mód 27
- $d_{a,b}(y) = a^{-1}(y - b)$ mód 27

Sistemas monoalfabéticos: Afín

- $e_{a,b}(x) = ax + b$ mód 27
- $d_{a,b}(y) = a^{-1}(y - b)$ mód 27

Por ejemplo, tomando $a = 2$ y $b = 5$:

$e(P) = aP + b$ mód $27 = 2 \cdot 16 + 5$ mód $27 = 10 \rightarrow K$

$d(K) = a^{-1}(K - b)$ mód $27 = 2^{-1}(10 - 5)$ mód $27 = 16 \rightarrow P$

Sistemas monoalfabéticos: Afín

- $e_{a,b}(x) = ax + b$ mód 27
- $d_{a,b}(y) = a^{-1}(y - b)$ mód 27

Por ejemplo, tomando $a = 2$ y $b = 5$:
$e(P) = aP + b$ mód $27 = 2 \cdot 16 + 5$ mód $27 = 10 \rightarrow K$
$d(K) = a^{-1}(K - b)$ mód $27 = 2^{-1}(10 - 5)$ mód $27 = 16 \rightarrow P$

$e(\text{PLAN TANU CLEA R}) = \text{KAFE RFET JANF Ñ}$

Sistemas monoalfabéticos: Afín

- $e_{a,b}(x) = ax + b$ mód 27
- $d_{a,b}(y) = a^{-1}(y - b)$ mód 27

Trabajando módulo m:

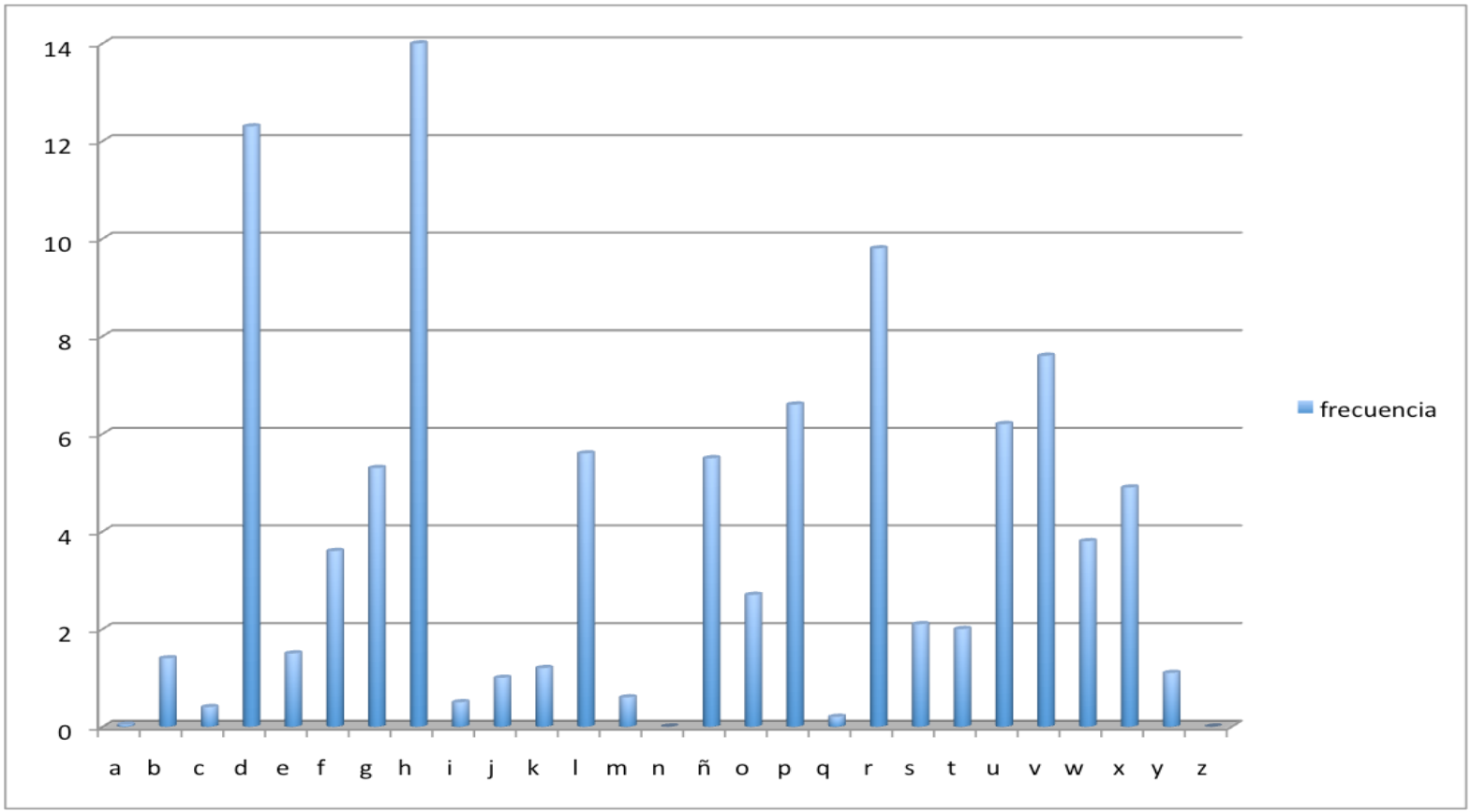
$$m = \prod_{i=1}^{n} p_i^{e_i} \qquad \phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Espacio de claves: (# Factores) · (# Desplazamientos)
Número de claves: $\phi(m) \cdot m$

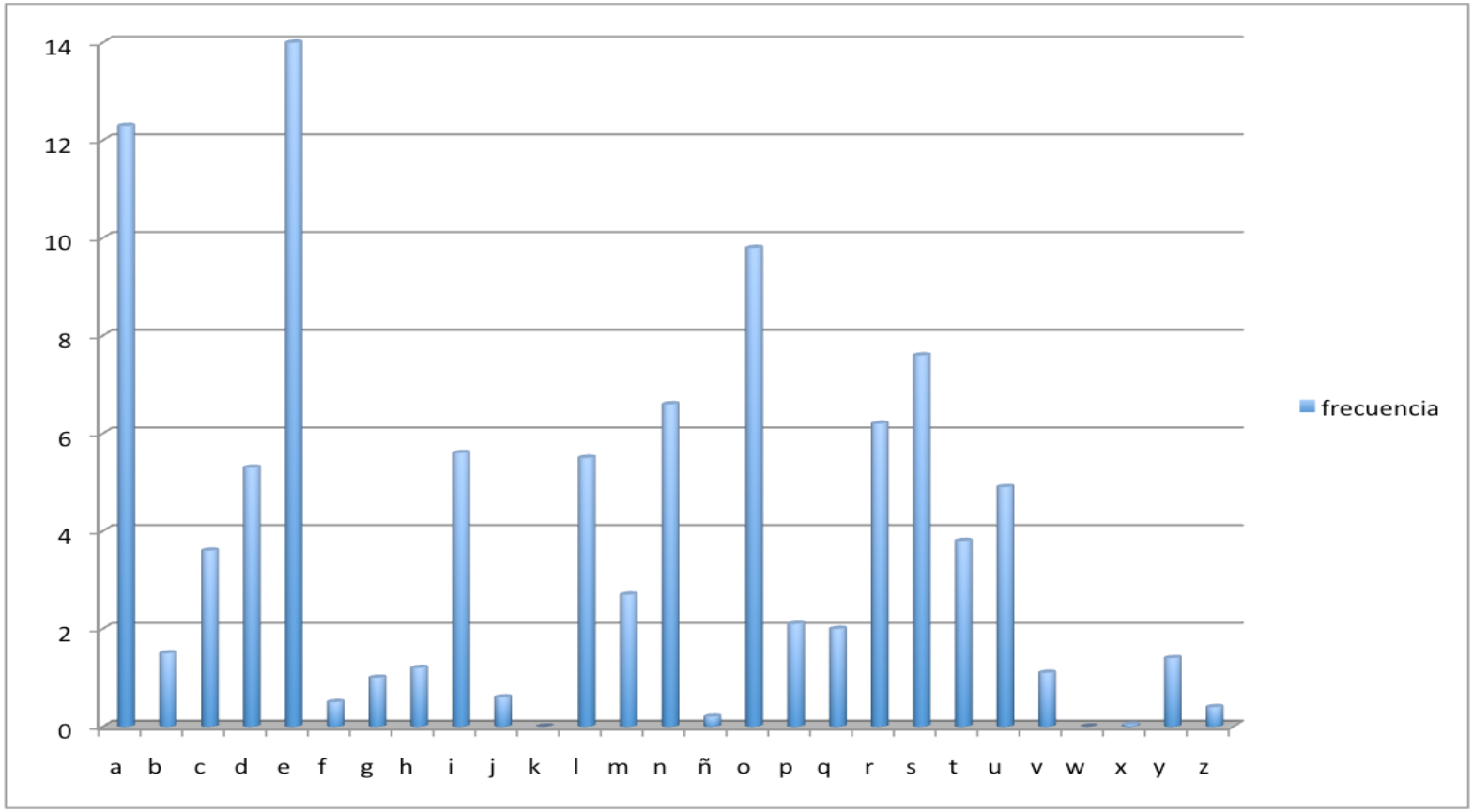
Criptoanálisis monoalfabético
Cifrado por desplazamiento

Frecuencia Alta		Frecuencia Media		Frecuencia Baja	
e	14.0	u	4.9	v	1.1
a	12.3	t	3.8	g	1.0
o	9.8	c	3.6	j	0.6
s	7.6	m	2.7	f	0.5
n	6.6	p	2.1	z	0.4
r	6.2	q	2.0	ñ	0.2
i	5.6	b	1.5	x	0.04
l	5.5	y	1.4	k	0.0004
d	5.3	h	1.2	w	0.0002

Criptoanálisis monoalfabético
Cifrado por desplazamiento



Criptoanálisis monoalfabético
Cifrado por desplazamiento



Criptoanálisis monoalfabético: Sustitución simple

Frecuencia Alta		Frecuencia Media		Frecuencia Baja	
e	14.0	u	4.9	v	1.1
a	12.3	t	3.8	g	1.0
o	9.8	c	3.6	j	0.6
s	7.6	m	2.7	f	0.5
n	6.6	p	2.1	z	0.4
r	6.2	q	2.0	ñ	0.2
i	5.6	b	1.5	x	0.04
l	5.5	y	1.4	k	0.0004
d	5.3	h	1.2	w	0.0002

Criptoanálisis monoalfabético: Sustitución simple

Frecuencia Alta		Frecuencia Media		Frecuencia Baja	
e	14.0	u	4.9	v	1.1
a	12.3	t	3.8	g	1.0
o	9.8	c	3.6	j	0.6
s	7.6	m	2.7	f	0.5
n	6.6	p	2.1	z	0.4
r	6.2	q	2.0	ñ	0.2
i	5.6	b	1.5	x	0.04
l	5.5	y	1.4	k	0.0004
d	5.3	h	1.2	w	0.0002

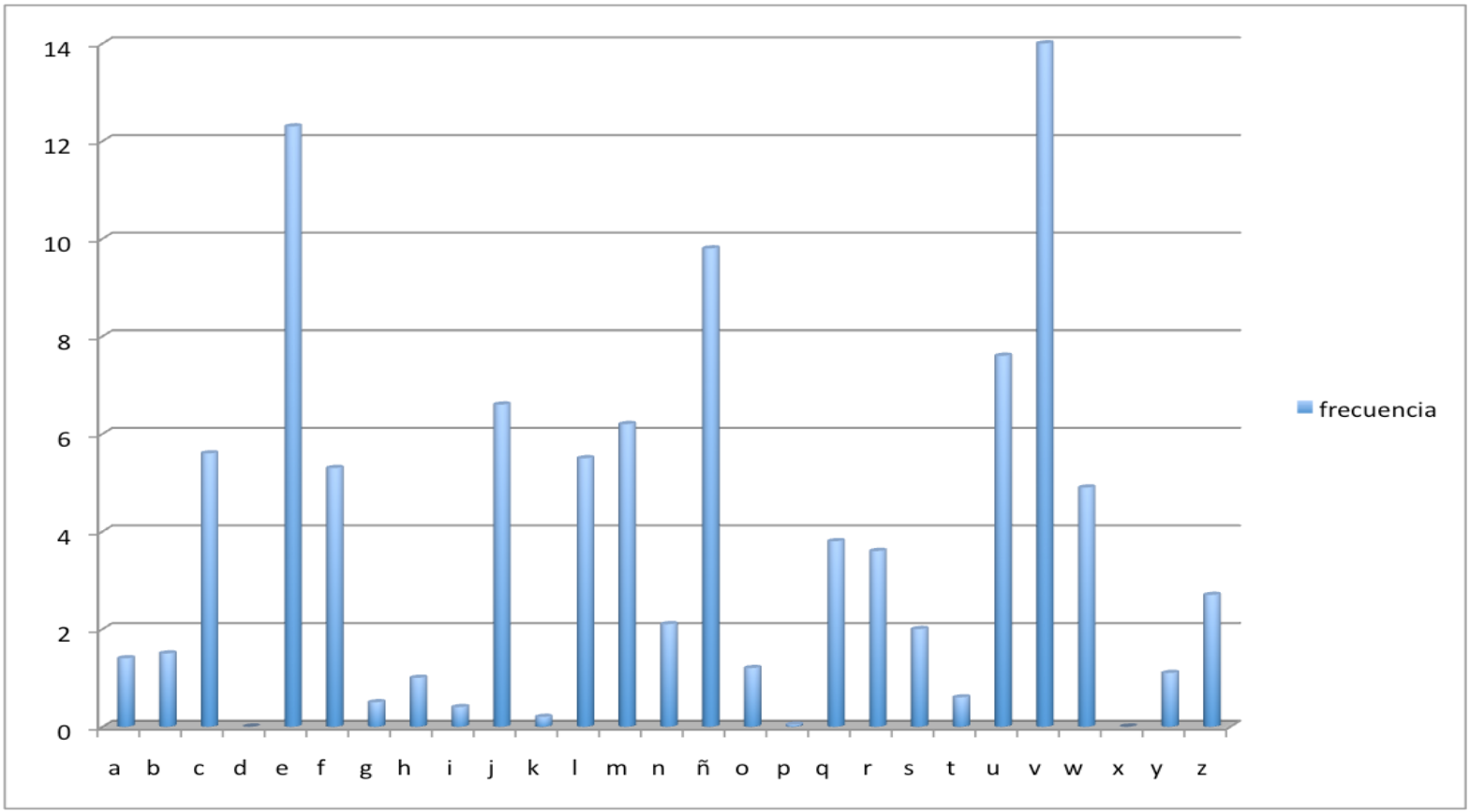
Bigramas más frecuentes: es, ue, en, de, qu, os, er, el, as, ra

Criptoanálisis monoalfabético: Sustitución simple

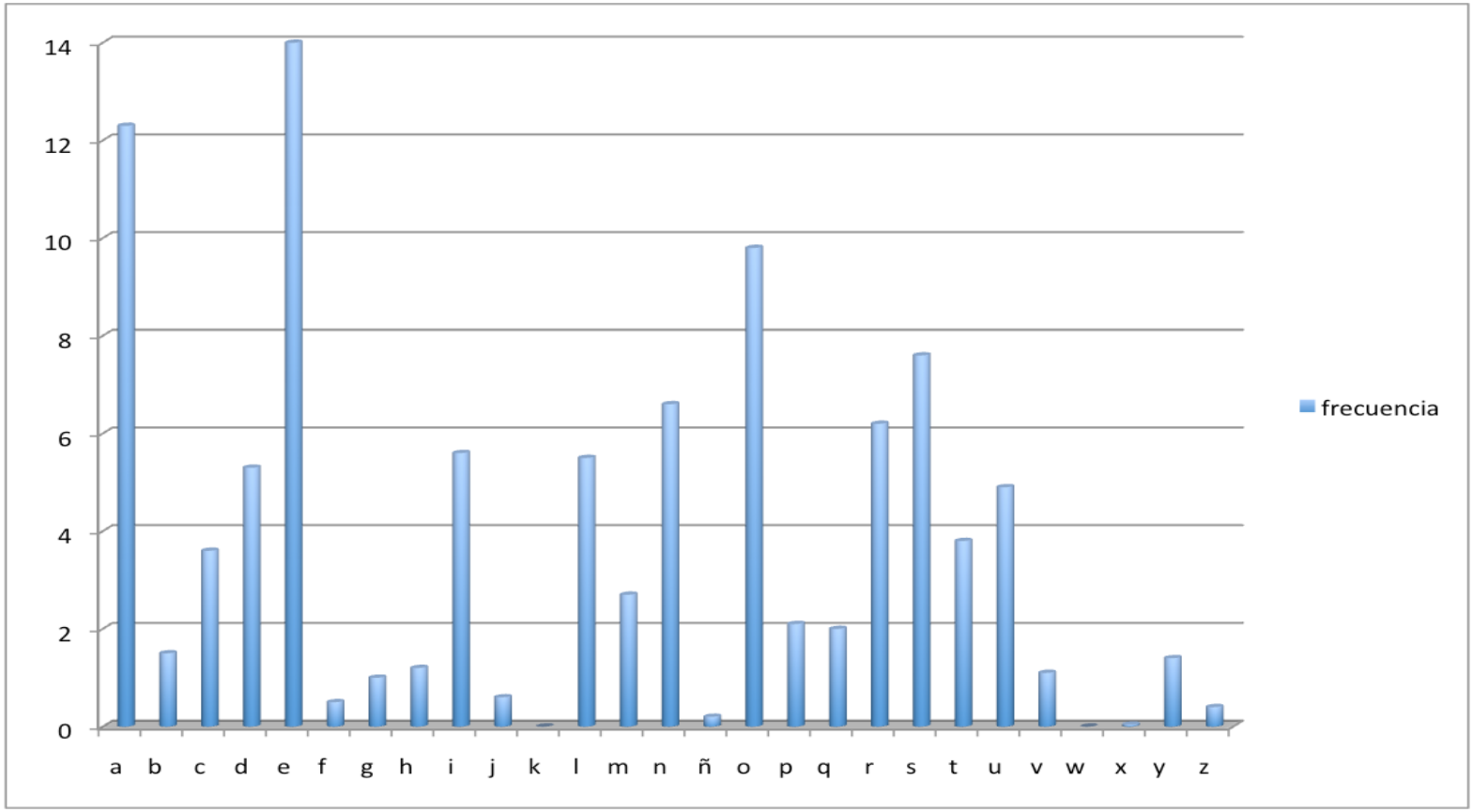
Frecuencia Alta		Frecuencia Media		Frecuencia Baja	
e	14.0	u	4.9	v	1.1
a	12.3	t	3.8	g	1.0
o	9.8	c	3.6	j	0.6
s	7.6	m	2.7	f	0.5
n	6.6	p	2.1	z	0.4
r	6.2	q	2.0	ñ	0.2
i	5.6	b	1.5	x	0.04
l	5.5	y	1.4	k	0.0004
d	5.3	h	1.2	w	0.0002

Bigramas más frecuentes: es, ue, en, de, qu, os, er, el, as, ra
Trigramas más frecuentes: que, est, ent, oqu, del, con, ien, ues, ade, aqu

Criptoanálisis monoalfabético
Cifrado por desplazamiento



Criptoanálisis monoalfabético
Cifrado por desplazamiento



Criptoanálisis monoalfabético: Afín

Frecuencia Alta		Frecuencia Media		Frecuencia Baja	
e	14.0	u	4.9	v	1.1
a	12.3	t	3.8	g	1.0
o	9.8	c	3.6	j	0.6
s	7.6	m	2.7	f	0.5
n	6.6	p	2.1	z	0.4
r	6.2	q	2.0	ñ	0.2
i	5.6	b	1.5	x	0.04
l	5.5	y	1.4	k	0.0004
d	5.3	h	1.2	w	0.0002

Criptoanálisis monoalfabético: Afín

- Texto cifrado:
  "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- Suponemos $e(E) = Y$ y $e(A) = P$, por lo tanto

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- Suponemos $e(E) = Y$ y $e(A) = P$, por lo tanto

$$\begin{cases} 4a + b \text{ mód } 27 = 25 \\ b \text{ mód } 27 = 16 \end{cases} \Rightarrow \begin{cases} a = 9 \\ b = 16 \end{cases}$$

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- Suponemos $e(E) = Y$ y $e(A) = P$, por lo tanto

$$\begin{cases} 4a + b \text{ mód } 27 = 25 \\ b \text{ mód } 27 = 16 \end{cases} \Rightarrow \begin{cases} a = 9 \\ b = 16 \end{cases}$$

- La suposición no era correcta

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- la conjetura válida es: $e(E) = Y$ y $e(A) = F$

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- la conjetura válida es: $e(E) = Y$ y $e(A) = F$

$$\begin{cases} 4a + b \text{ mód } 27 = 25 \\ b \text{ mód } 27 = 5 \end{cases} \Rightarrow \begin{cases} a = 5 \\ b = 5 \end{cases}$$

Criptoanálisis monoalfabético: Afín

- Texto cifrado: "EÑZKGYLFSOZPPCYSXÑZFIYPXYRPDRGXÑFTZ"
- Símbolos más frecuentes: Y 4 veces, P 4 veces, Z 4 veces, F 3 veces, Ñ 3 veces, X 3 veces
- la conjetura válida es: $e(E) = Y$ y $e(A) = F$

$$\begin{cases} 4a + b \text{ mód } 27 = 25 \\ b \text{ mód } 27 = 5 \end{cases} \Rightarrow \begin{cases} a = 5 \\ b = 5 \end{cases}$$

- Mensaje: "PROBLEMASCONNUESTROAGENTEINFILTRADO"

Sistemas polialfabéticos

Cifrado polialfabético
Vigenèrè. Descripción

- En un cifrado polialfabético, la clave consiste en una secuencia de cierta longitud n de valores numéricos
- Los símbolos del mensaje se cifran por desplazamiento
- En general, el símbolo que ocupa una cierta posición se cifra de acuerdo con el elemento de la clave congruente con su posición módulo n

- En un cifrado polialfabético, la clave consiste en una secuencia de cierta longitud n de valores numéricos
- Los símbolos del mensaje se cifran por desplazamiento
- En general, el símbolo que ocupa una cierta posición se cifra de acuerdo con el elemento de la clave congruente con su posición módulo n

  Clave: $k = (k_1, k_2, \ldots, k_m)$, donde $k_i \in \mathbb{Z}_{27}$
  Denotando con x_i el i-esimo símbolo a cifrar:
  $e_k(x_i) = x_i + k_{i \text{ mód } m}$ mód 27

- En un cifrado polialfabético, la clave consiste en una secuencia de cierta longitud n de valores numéricos
- Los símbolos del mensaje se cifran por desplazamiento
- En general, el símbolo que ocupa una cierta posición se cifra de acuerdo con el elemento de la clave congruente con su posición módulo n
- El descifrado se consigue deshaciendo los desplazamientos indicados por la clave

  Clave: $k = (k_1, k_2, \ldots, k_m)$, donde $k_i \in \mathbb{Z}_{27}$
  Denotando con x_i el i-esimo símbolo a cifrar:
  $d_k(y_i) = y_i - k_{i \text{ mód } m} \text{ mód } 27$

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e							

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e	c	l	a	v	e	c	l

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e	c	l	a	v	e	c	l

x:	20	4	24	20	15	0	2	8	5	18	0	18

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e	c	l	a	v	e	c	l

x:	20	4	24	20	15	0	2	8	5	18	0	18
k:	2	11	0	22	4	2	11	0	22	4	2	11

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e	c	l	a	v	e	c	l

x:	20	4	24	20	15	0	2	8	5	18	0	18
k:	2	11	0	22	4	2	11	0	22	4	2	11
y:	22	15	24	15	19	2	13	8	0	22	2	2

Cifrado polialfabético
Vigenèrè. Ejemplo

x:	T	E	X	T	O	A	C	I	F	R	A	R
k:	c	l	a	v	e	c	l	a	v	e	c	l

x:	20	4	24	20	15	0	2	8	5	18	0	18
k:	2	11	0	22	4	2	11	0	22	4	2	11
y:	22	15	24	15	19	2	13	8	0	22	2	2
y:	V	O	X	O	S	C	N	I	A	V	C	M

Criptoanálisis polialfabético
Cifrado Vigenèrè

Basado en la detección del número de alfabetos utilizado y la aplicación de técnicas basadas en análisis de frecuencias

Criptoanálisis polialfabético
Cifrado Vigenèrè

Basado en la detección del número de alfabetos utilizado y la aplicación de técnicas basadas en análisis de frecuencias

Kasiski:

- Un grupo de símbolos que aparezca k veces en un texto, será cifrado k/n veces con el mismo alfabeto, donde n denota el número de alfabetos
- Dado un determinado segmento, si las distancias entre estas posiciones son $d_1, d_2, ..., d_k$, el periodo es divisor del máximo común divisor de las distancias

Criptoanálisis polialfabético
Cifrado Vigenèrè

Basado en la detección del número de alfabetos utilizado y la aplicación de técnicas basadas en análisis de frecuencias

Kasiski:

- Un grupo de símbolos que aparezca k veces en un texto, será cifrado k/n veces con el mismo alfabeto, donde n denota el número de alfabetos
- Dado un determinado segmento, si las distancias entre estas posiciones son $d_1, d_2, ..., d_k$, el periodo es divisor del máximo común divisor de las distancias

Ind. de coincidencia: Se fundamenta en la distribución de la frecuencia de los símbolos en un texto cifrado y en el lenguaje natural

Criptoanálisis polialfabético
Método de Kasiski

- Criptograma:

FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFcuñn
FCBSMHAAANAUEVNHDCFVJFRNICFAHcuñnWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI

Criptoanálisis polialfabético
Método de Kasiski

- Criptograma:

```
FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFcuñn
FCBSMHAAANAUEVNHDCFVJFRNICFAHcuñnWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI
```

- El tetragrama CUÑN aparece en las posiciones 43 y 76 del texto

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

Dado un texto cifrado es posible establecer una medida de dispersión de las frecuencias de los símbolos del mensaje respecto a una distribución uniforme:

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

Dado un texto cifrado es posible establecer una medida de dispersión de las frecuencias de los símbolos del mensaje respecto a una distribución uniforme:

$$MD = \sum_{i=0}^{26} \left(p_i - \frac{1}{n} \right)^2 = \sum_{i=0}^{26} \left(p_i^2 - \frac{2p_i}{n} + \frac{1}{n^2} \right) = \sum_{i=0}^{26} \left(p_i^2 \right) - 0{,}037$$

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

Dado un texto cifrado es posible establecer una medida de dispersión de las frecuencias de los símbolos del mensaje respecto a una distribución uniforme:

$$MD = \sum_{i=0}^{26} \left(p_i - \frac{1}{n} \right)^2 = \sum_{i=0}^{26} \left(p_i^2 - \frac{2p_i}{n} + \frac{1}{n^2} \right) = \sum_{i=0}^{26} \left(p_i^2 \right) - 0{,}037$$

En un texto donde los símbolos presentan una distribución própia del castellano:

$$IC = \sum_{i=0}^{26} \left(p_i^2 \right) = 0{,}072 \quad \Rightarrow \quad 0 \leq MD \leq 0{,}035$$

Intuitivamente, el IC mide la probabilidad de que dos símbolos tomados al azar de un texto cifrado sean iguales.

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

El IC puede estimarse utilizando la frecuencia de los símbolos en el criptograma:

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

El IC puede estimarse utilizando la frecuencia de los símbolos en el criptograma:

$$IC \simeq \frac{\sum_{i=0}^{26} f_i(f_i - 1)}{N(N-1)}$$

donde f_i denota el número de ocurrencias del caracter i-esimo en un criptograma de N símbolos

El IC puede estimarse utilizando la frecuencia de los símbolos en el criptograma:

$$IC \simeq \frac{\sum_{i=0}^{26} f_i(f_i-1)}{N(N-1)}$$

donde f_i denota el número de ocurrencias del caracter i-esimo en un criptograma de N símbolos De este modo:

$$IC = MD + 0{,}037 \quad \Rightarrow \quad 0{,}037 \leq IC \leq 0{,}072$$

$p = 1$	$IC = 0{,}072$	$p = 4$	$IC = 0{,}046$
$p = 2$	$IC = 0{,}054$	$p = 10$	$IC = 0{,}040$
$p = 3$	$IC = 0{,}049$	$p >>$	$IC = 0{,}037$

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

- Criptograma (más extenso):

FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFCUÑN
FCBSMHAAANAUEVNHDCFVJFRNICFAHCUÑNWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI ...

Criptoanálisis polialfabético

Cálculo del Indice de Coincidencia

- Criptograma (más extenso):

```
FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFCUÑN
FCBSMHAAANAUEVNHDCFVJFRNICFAHCUÑNWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI ...
```

$$p = 1 \quad \Rightarrow \quad IC = 0{,}0471363$$

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

- Criptograma (más extenso):

```
FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFCUÑN
FCBSMHAAANAUEVNHDCFVJFRNICFAHCUÑNWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI ...
```

$$p = 1 \quad \Rightarrow \quad IC = 0{,}0471363$$
$$p = 2 \quad \Rightarrow \quad IC = \{0{,}0479231, 0{,}0463764\}$$

Criptoanálisis polialfabético

Cálculo del Indice de Coincidencia

- Criptograma (más extenso):

```
FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFCUÑN
FCBSMHAAANAUEVNHDCFVJFRNICFAHCUÑNWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI ...
```

$$p = 1 \quad \Rightarrow \quad IC = 0{,}0471363$$
$$p = 2 \quad \Rightarrow \quad IC = \{0{,}0479231, 0{,}0463764\}$$
$$p = 3 \quad \Rightarrow \quad IC = \{0{,}0739754, 0{,}0753505, 0{,}072086\}$$

Criptoanálisis polialfabético
Cálculo del Indice de Coincidencia

- Criptograma (más extenso):

```
FSGWHAYPVJFRNIIYVRHLRMVRGNPBSGWDÑNWGBAGÑHFCUÑN
FCBSMHAAANAUEVNHDCFVJFRNICFAHCUÑNWGÑSOUFMUMCGS
AXHSJKZUEIWZCUFHYLQYJIYHMYKÑBSOFSFXWYCFTOAGÑAP
UQYUJIYWGÑNQCWRHSBJLUDJLHYKVJKRNWAFSIHAJYKGCVÑ
XWFUNAUWGKWPCWQYMRWFCFHTCSWQYLPMADÑAJUUCHWAGAC
KAACHAKHPULVGIYCUÑWACHWGGSGUEDFAÑNWAFFHGXAJYKG
JLZJÑVGARHMCNWGÑKIWMIMSYCLHULSOWFJFSMWPOWAÑWGF
HGYCFHYFHJLQYWANSAWZÑMWGULVXWÑNIRMHRFKRNNYÑSQJ
VRÑHQJWGJWGFWKRJEISVRVAYSICWHPJFJCFPYFHYI ...
```

$$
\begin{aligned}
p = 1 &\Rightarrow IC = 0{,}0471363 \\
p = 2 &\Rightarrow IC = \{0{,}0479231, 0{,}0463764\} \\
p = 3 &\Rightarrow IC = \{0{,}0739754, 0{,}0753505, 0{,}072086\} \\
p = 4 &\Rightarrow IC = \{0{,}0470939, 0{,}046151, 0{,}0487458, 0{,}0464554\}
\end{aligned}
$$

Criptoanálisis polialfabético
Cifrado Vigenèrè

- Una vez detectado el número de alfabetos, puede aplicarse un análisis de frecuencias como el ya visto
- Efectivamente, el número de alfabetos es 3
- Mensaje:

```
LASCONEXIONESPUEDENSERDEMUCHASCLASESHISTORicas
NOHAYNINGUNAMISOPINIONESPOLITicasESTABANYATOMA
NDOFORMAMUCHOANTESDEQUEOYERAHABLARDELINGUISTIC
AYLAQUEESTUDIEENAÑOSPOSTERIORESENLAUNIVERSIDAD
ERAUNAESPECIEDETECNOLOGIADESCRIPTIVACONENMIOPI
NIONPOCASIMPLICACIONESMASAMPLIASENLOSDIVERSOSM
OVIMIENTOSESTRUCTURALISTASFUERONFRECUENTESLOSI
NTENTOSDEENSANCHARESASIDEASPEROELRESULTADODETO
DOESOESCREOMUYDEBILYPOCOCONVINCENTE ...
```

Cifrado polialfabético
M-94

MK-85C

(foto robbo@ev1.net *Crypto Machine Page*)

- Implementación del disco de Jefferson (1795). Conjunto de (25) discos de aluminio engarzados en torno a un eje.
- Identificados mediante el caracter siguiente al símbolo `A`, cada disco contiene una permutación del alfabeto
- El mensaje se cifraba en bloques de 25 caracteres.
- Una vez dispuestos en horizontal los símbolos de un bloque, las restantes horizontales ofrecen cifrados posibles
- Para uso táctico hasta 1945. Actualmente *DRYAD* implementa en esencia la misma idea.

Cifrado mediante códigos

Cifrado mediante códigos
Descripción

- Se basa en la sustitución de fragmentos de mensaje por un *código*. Los códigos se compilan en un *nomenclator*
- Los códigos de uso general deben incluir un modo de deletrear palabras no incluidas en el nomenclator
- Los códigos se debilitan si codifican pequeños fragmentos de mensaje. El uso de *homófonos* pretenden paliar los efectos de sustituciones breves.
- Los códigos simples se ordenan en función del código. Los códigos más extensos se ordenan doblemente
- Códigos pequeños pueden presentarse en forma matricial
- Mientras mayor es el código, mayor la seguridad. La adición de una capa de cifrado (usualmente polialfabético) ha sido utilizada con este motivo

Cifrado mediante códigos

Presentación de códigos

CÓDIGO	MENSAJE
AAB	A
ABD	AB
ACF	ABANDON
ADH	ABOUT
AEJ	ACCIDENT
AFO	ACTION
AGB	ACTIVE
AHI	ACTIVITY
...	...

Cifrado mediante códigos
Presentación de códigos

CIFRADO	
KTOL	A
YNIF	A
ACEJ	AB
VADH	ABANDON ING S
WOJA	ABILITY
AFOH	ABLE
LBGB	ABLE TO
TZAM	ABOUT
...	...

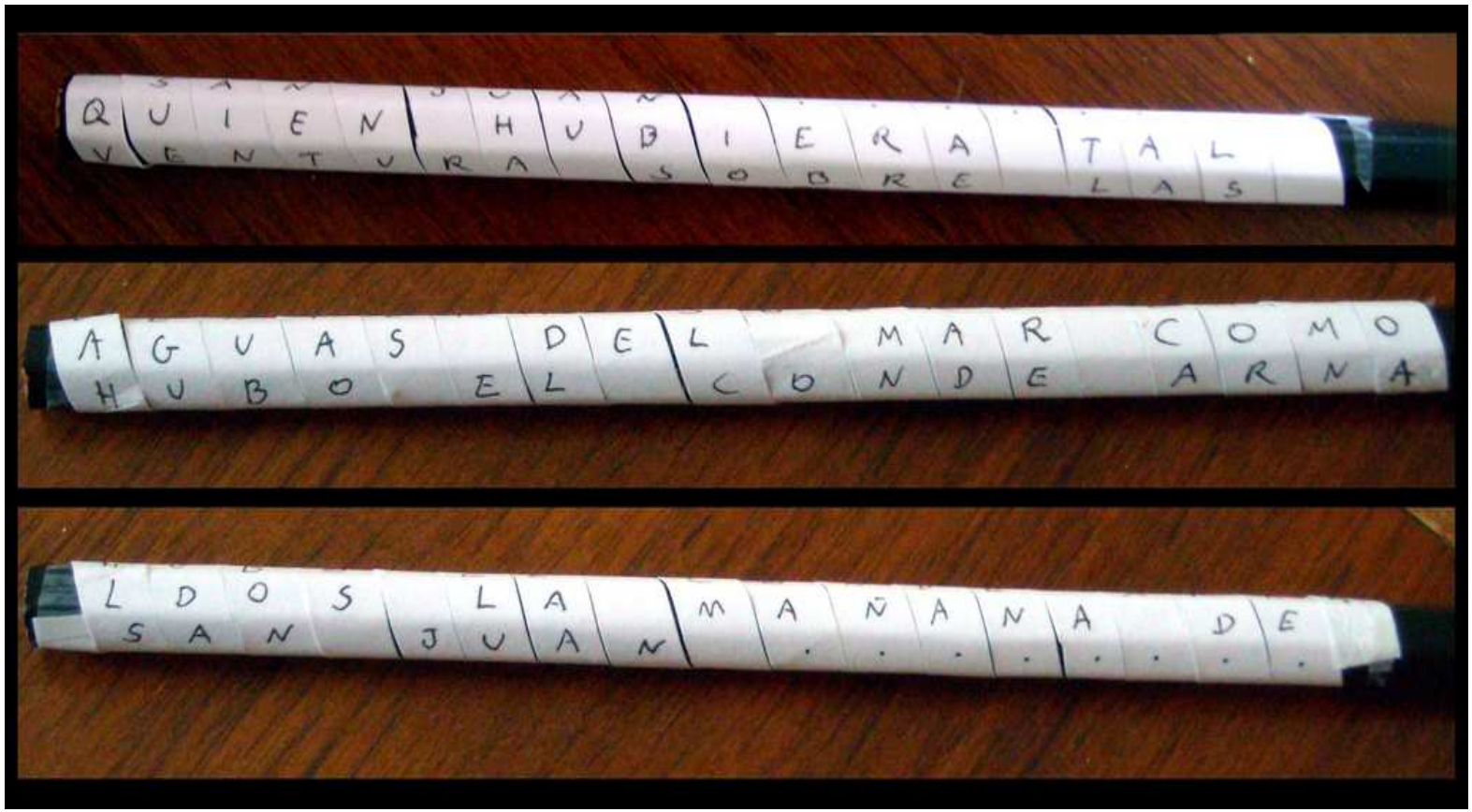
DESCIFRADO	
ABAB	RESISTANCE
ABEC	SIZE
ABID	CHEMICAL
ABOF	T-72
ABUG	QUALITY
ACAH	AB
ACEJ	VERIFY ING S
ACIK	15
...	...

Cifrado mediante códigos
Criptoanálisis

- El ataque se basa en la identificación de sílabas
- Las sílabas identificadas permiten identificar nuevas entradas
- El conocimiento del idioma es importante para poder obtener una ventaja de la sintaxis del mensaje
- La codificación de números suponen una debilidad debido a los patrones que suelen presentar en un mensaje
- Para evitar el efecto de un error de transmisión, los códigos se envían repetidamente
- Es posible que un código no sea totalmente descifrado, y pese a ello sea posible descifrar mensajes desde una fase temprana del ataque

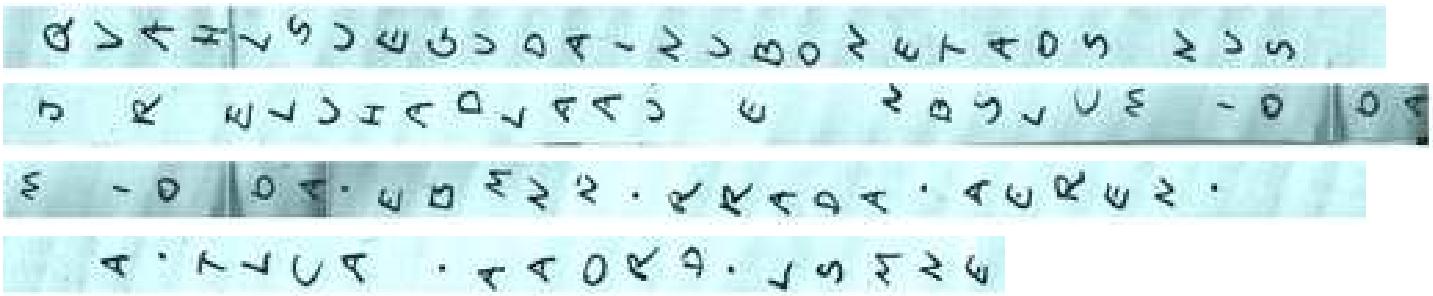
Sistemas por transposición

Sistemas basados en transposición
Scitala espartana



fuente: *predicadormalvado.blogspot.com.es/*

Sistemas basados en transposición
Scitala espartana



fuente: *predicadormalvado.blogspot.com.es/*

Sistemas de cifrado por transposición
Cifrado por permutación columnar simple

OANCDSICNIEBPCCEATRUTONLEIALDRDMANSERONAEUOECSIX

Sistemas de cifrado por transposición

Cifrado por permutación columnar simple

OANCDSICNIEBPCCEATRUTONLEIALDRDMANSERONAEUOECSIX

O	A	N	C	D	S	I	C	N	I	E	B
P	C	C	E	A	T	R	U	T	O	N	L
E	I	A	L	D	R	D	M	A	N	S	E
R	O	N	A	E	U	O	E	C	S	I	X

Sistemas de cifrado por transposición

Cifrado por permutación columnar simple

OANCDSICNIEBPCCEATRUTONLEIALDRDMANSERONAEUOECSIX

O	A	N	C	D	S	I	C	N	I	E	B
P	C	C	E	A	T	R	U	T	O	N	L
E	I	A	L	D	R	D	M	A	N	S	E
R	O	N	A	E	U	O	E	C	S	I	X

OPERACIONCANCELADADESTRUIRDOCUMENTACIONSENSIBLE

Sistemas de cifrado por transposición

Cifrado por permutación columnar simple

OANCDSICNIEBPCCEATRUTONLEIALDRDMANSERONAEUOECSIX

O	A	N	C	D	S	I	C	N	I	E	B
P	C	C	E	A	T	R	U	T	O	N	L
E	I	A	L	D	R	D	M	A	N	S	E
R	O	N	A	E	U	O	E	C	S	I	X

OPERACIONCANCELADADESTRUIRDOCUMENTACIONSENSIBLE

Cuando la disposición cambia en función de un patrón, el sistema se denomina de *transposición por ruta*.

Sistemas de cifrado por transposición
Transposición con clave numérica

- La clave determina una permutación sobre un bloque de caracteres

8	3	10	7	4	1	5	2	6	9
R	E	S	P	L	A	N	D	O	R

Sistemas de cifrado por transposición
Transposición con clave numérica

- La clave determina una permutación sobre un bloque de caracteres
- El mensaje se cifra en bloques de tantos simbolos como la longitud de la clave

Sistemas de cifrado por transposición

Transposición con clave numérica

- La clave determina una permutación sobre un bloque de caracteres
- El mensaje se cifra en bloques de tantos simbolos como la longitud de la clave
- Tomando p.e. como clave `LAPIZ` $(3, 1, 4, 2, 5)$, y el mensaje: `ELEN VIOE STAR ALIS TOAT IEMP O`

E	L	E	N	V
I	O	E	S	T
A	R	A	L	I
S	T	O	A	T
I	E	M	P	O

Sistemas de cifrado por transposición

Transposición con clave numérica

- La clave determina una permutación sobre un bloque de caracteres
- El mensaje se cifra en bloques de tantos simbolos como la longitud de la clave
- Tomando p.e. como clave `LAPIZ` $(3, 1, 4, 2, 5)$, y el mensaje: `ELEN VIOE STAR ALIS TOAT IEMP O`

E	L	E	N	V
I	O	E	S	T
A	R	A	L	I
S	T	O	A	T
I	E	M	P	O

E	E	N	L	V
E	I	S	O	T
A	A	L	R	I
O	S	A	T	T
M	I	P	E	O

Sistemas de cifrado por transposición
Transposición con clave numérica

- La clave determina una permutación sobre un bloque de caracteres
- El mensaje se cifra en bloques de tantos simbolos como la longitud de la clave
- Tomando p.e. como clave `LAPIZ` $(3, 1, 4, 2, 5)$, y el mensaje: `ELEN VIOE STAR ALIS TOAT IEMP O`

E	L	E	N	V
I	O	E	S	T
A	R	A	L	I
S	T	O	A	T
I	E	M	P	O

E	E	N	L	V
E	I	S	O	T
A	A	L	R	I
O	S	A	T	T
M	I	P	E	O

criptograma: `EEAO MEIA SINS LAPL ORTE VTIT O`

Sistemas de cifrado por transposición
Criptoanálisis

- Determinar el tamaño de la matriz
- Pueden descartarse alternativas considerando la frecuencia de vocales en cada fila
- La reconstrucción de la permutación puede realizarse por anagramación

Sistemas poligráficos

Sistemas poligráficos
Playfair

- Cifra el mensaje considerando pares de dos símbolos (s_1, s_2)

Sistemas poligráficos
Playfair

- Cifra el mensaje considerando pares de dos símbolos (s_1, s_2)
- La clave es una matriz donde se disponen los símbolos del alfabeto (5×5)

Sistemas poligráficos
Playfair

- Cifra el mensaje considerando pares de dos símbolos (s_1, s_2)
- La clave es una matriz donde se disponen los símbolos del alfabeto (5×5)

Algoritmo: sean (x_1, y_1) y (x_2, y_2) las coordenadas de s_1 y s_2 en la matriz clave.

- Si $x_1 = x_2 \Rightarrow ((x_1, y_1 + 1 \text{ mód } 5), (x_2, y_2 + 1 \text{ mód } 5))$
- Si $y_1 = y_2 \Rightarrow ((x_1 + 1 \text{ mód } 5, y_1), (x_2 + 1 \text{ mód } 5, y_2))$
- Si $x_1 \neq x_2 \wedge y_1 \neq y2 \Rightarrow ((x_1, y_2), (x_2, y_1))$
- Si $s_1 = s_2$ insertar un símbolo sin significado
- Si al final queda un único caracter sin cifrar, insertar un símbolo sin significado

Sistemas poligráfico
Playfair

clave:

a	l	g	r	o
b	c	d	e	f
h	i	k	m	n
p	q	s	t	u
v	w	x	y	z

mensaje:	EV	ID	EN	CI	AD	EL	...
criptograma:	BY	KC	FM	IQ	GB	CR	...

Criptoanálisis poligráfico
Cifrado Playfair

- Objetivo reconstrucción de la matriz clave
- Proceso iterativo que considera hipótesis iniciales basadas en el criptograma: repeticiones en el criptograma; bigramas XC-CX; ...
- Los bigramas con letras en común permiten ubicar más caracteres en la matriz
- La reconstrucción ha de considerar las tres posibles situaciones de los caracteres del bigrama
- La matriz resultante puede ser mayor de 5×5, pudiendo compactarse posteriormente
- El criptoanálisis Playfair es un caso particular del criptoanálisis del sistema *four squares*

Sistemas poligráficos
Hill

- Cifra el mensaje considerando bloques de k símbolos

Sistemas poligráficos
Hill

- Cifra el mensaje considerando bloques de k símbolos
- La clave es una matriz $K_{k\times k}$ de valores en Z_m tal que $mcd(|K|, 27) = 1$

$$K = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & & & \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix};$$

Sistemas poligráficos
Hill

- Cifra el mensaje considerando bloques de k símbolos
- La clave es una matriz $K_{k\times k}$ de valores en Z_m tal que $mcd(|K|, 27) = 1$

$$K = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & & & \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix};$$

Algoritmo: considerando el mensaje $x = x_1x_2x_3x_4\dots$

$$K \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix}; \qquad K^{-1} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}$$

Sistemas poligráficos
Hill

Tomando $K = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix}$; $K^{-1} = \begin{pmatrix} 1 & 26 \\ 5 & 6 \end{pmatrix}$; $X = GATO$

Sistemas poligráficos
Hill

Tomando $K = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix}$; $K^{-1} = \begin{pmatrix} 1 & 26 \\ 5 & 6 \end{pmatrix}$; $X = GATO$

$$e(GA) = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 12 \end{pmatrix}$$

Sistemas poligráficos
Hill

Tomando $K = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix}$; $K^{-1} = \begin{pmatrix} 1 & 26 \\ 5 & 6 \end{pmatrix}$; $X = GATO$

$$e(GA) = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 12 \end{pmatrix}$$

$$e(TO) = \begin{pmatrix} 3 & 5 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \end{pmatrix}$$

Criptoanálisis poligráfico
Cifrado Hill

- Ataque basado en *mensaje conocido*

Criptoanálisis poligráfico
Cifrado Hill

- Ataque basado en *mensaje conocido*
- Sea $x = x_1x_2x_3\ldots$ un fragmento del mensaje e $y = y_1y_2y_3\ldots$ su correspondiente criptograma

Criptoanálisis poligráfico
Cifrado Hill

- Ataque basado en *mensaje conocido*
- Sea $x = x_1x_2x_3\ldots$ un fragmento del mensaje e $y = y_1y_2y_3\ldots$ su correspondiente criptograma
- Suponiendo la clave de tamaño 3, es posible construir el sistema:

$$K \cdot \begin{pmatrix} x_1 & x_4 & x_7 \\ x_2 & x_5 & x_8 \\ x_3 & x_6 & x_9 \end{pmatrix} = \begin{pmatrix} y_1 & y_4 & y_7 \\ y_2 & y_5 & y_8 \\ y_3 & y_6 & y_9 \end{pmatrix}$$

Criptoanálisis poligráfico
Cifrado Hill

- Ataque basado en *mensaje conocido*
- Sea $x = x_1x_2x_3\ldots$ un fragmento del mensaje e $y = y_1y_2y_3\ldots$ su correspondiente criptograma
- Suponiendo la clave de tamaño 3, es posible construir el sistema:

$$K \cdot \begin{pmatrix} x_1 & x_4 & x_7 \\ x_2 & x_5 & x_8 \\ x_3 & x_6 & x_9 \end{pmatrix} = \begin{pmatrix} y_1 & y_4 & y_7 \\ y_2 & y_5 & y_8 \\ y_3 & y_6 & y_9 \end{pmatrix}$$

- Es posible calcular la clave si la matriz *mensaje* es invertible

Máquinas de rotores

Máquinas de rotores
Contexto histórico

- Durante el periodo de entre guerras, la criptografía se basaba en el uso de códigos
- Estos sistemas no eran suficientemente robustos y los servicios de inteligencia llegaron a atacarlos con éxito
- Francia disponía de la estructura más eficiente, con estaciones de escucha y personal distribuido en distintas secciones especializadas
- Este esquema es implantado en Polonia, donde se empezó a reclutar a matemáticos, en lugar de excusivamente a lingüistas como hasta el momento
- A principios de 1926 se detectan una serie de mensajes indescifrables de la marina alemana...

Máquinas de rotores
Contexto histórico

- Un grupo del servicio polaco de inteligencia llega a la conclusión que Alemania había abandonado el cifrado mediante códigos, habiéndo adoptado un sistema mecánico de cifrado polialfabético
- Los estudios preliminares concluyeron la imposibilidad del criptoanálisis en tiempo eficiente
- Esta conclusión coincide con la de los observadores que vigilaban el cumplimento de las condiciones impuestas a Alemania al final de la guerra

Máquinas de rotores
Enigma

- A principios de los años 20 del s.XX existían diversas patentes de *máquinas de cifrar*
- Dos ingenieros (A. Scherbius y R. Ritter) compran una de las licencias y desarrollan la máquina Enigma
- Basándose en un mecanismo de relojería, tres o cuatro ruedas (según versiones) engranadas realizaban un cifrado polialfabético con una clave de gran tamaño
- En versiones comerciales, el conexionado interior de cada rueda era considerado secreto
- En versiones militares, era necesario que el acceso a la máquina no afectara la seguridad. El protocolo de operación incluía códigos (configuración) diarios. El protocolo establecía que parte del código diario se enviara cifrado

Máquinas de rotores
Enigma

http://www.ilord.com/

Máquinas de rotores
Descripción cifrado Enigma

- Banco de rotores (3 o 4 de un conjunto mayor) cada uno con tantos contactos como símbolos en el alfabeto (26). Los rotores están conectados mediante un mecanismo de relojería
- Cada rotor realiza un desplazamiento de su entrada y lo comunica al siguiente rotor
- Un reflector fuerza a la señal de vuelta a traves de los rotores
- Cada caracter introducido provoca un desplazamiento de los rotores
- Un tablero de permutaciones aplica una operación de intercambio a algunos símbolos previamente a la transmisión a los rotores
- El resultado es un cifrado polialfabético con gran periodo

- Las posibles configuraciones diarias de la máquina se distribuían en hojas de claves. Cada sección del ejército disponía de su propia red de distribución
- La información consistía de:

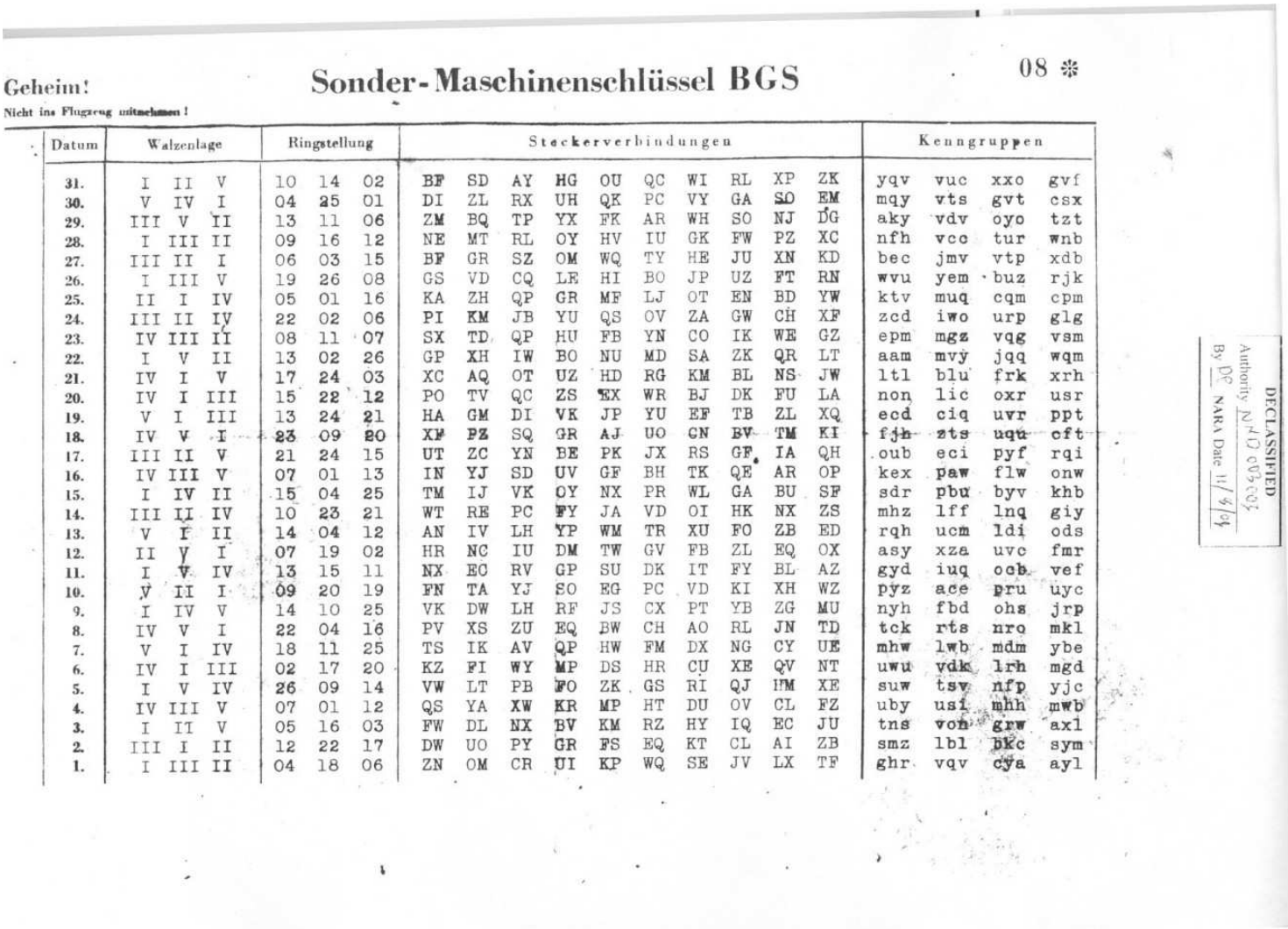
  Walzenlage : Elección y orden de los rotores

  Ringstellung : Posición del cableado de cada uno de los rotores respecto el alfabeto del anillo

  Steckerverbindungen : Conexiones a efectuar en el panel de permutaciones

  Kenngruppen : Grupos para la identificación de la clave por parte del receptor

Máquinas de rotores
Enigma: Key sheet



Geheim! — Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS — 08 ❊

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vcc tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ FM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

Dirk Rijmenants' *Cipher Machines and Cryptology*

Máquinas de rotores
Procedimiento de operación de Enigma (Ejercito. Después de 1940)

- Selección de rotores, disposición interna y conexiones de acuerdo la configuración diaria (*Walzenlage*, *Ringstellung* y *Steckerverbindungen*)
- Selección de un *Kenngruppen* válido en el día (p.e. `JKM`)
- Selección aleatoria de una disposición de los rotores (p.e. `WZA`)
- Selección aleatoria de una clave de mensaje (p.e. `SXT`)
- Cifrado de la clave de mensaje (`SXT`) utilizando la disposición escogida (`WZA`) (obteniendo p.e. `UHL`)
- Cifrado del mensaje utilizando la clave escogida (`SXT`)

Máquinas de rotores
Enigma: formato de mensaje


```
1230 = 3tle = 1tl = 250 = WZA UHL =

FDJKM LDAHH YEOEF PTWYB LENDP
MKOXL DFAMU DWIJD XRJZY DFRIO
MFTEV KTGUY DDZED TPOQX FDRIU
CCBFM MQWYE FIPUL WSXHG YHJZE
AOFDU FUTEC VVBDP OLZLG DEJTI
HGYER DCXCV BHSEE TTKJK XAAQU
GTTUO FCXZH IDREF TGHSZ DERFG
EDZZS ERDET RFGTT RREOM MJMED
EDDER FTGRE UUHKD DLEFG FGREZ
ZZSEU YYRGD EDFED HJUIK FXNVB
```

Dirk Rijmenants' *Cipher Machines and Cryptology*

- Considerando el cableado interno de los rotores, sería posible conseguir del orden de 10^{114} configuraciones distintas
- El espacio de claves (configuraciones operativas) era del orden de 10^{23} configuraciones distintas (equivalente a una clave de 77 bits)
- Se consideraba secreto el cableado interno de los rotores
- Versiones de la marina introdujeron un reflector configurable y un banco mayor de rotores (8)
- Para la época (electro-mecánica), el criptoanálisis suponía un gran desafío

- Antes de 1939 los polacos realizaron los primeros avances en el criptoanálisis
- Aprovechando *defectos* de operación averiguan el cableado de los rotores
- Catalogan las posibles configuraciones y claves diarias. Construyen para ello máquinas Enigma en paralelo (*Polish Bomba*)
- Antes de la invasión alemana, comunican a Francia la información disponible

- Antes de la guerra, se traslada a Blentchley Park la *Escuela de Códigos y Cifras del Gobierno* (GC&CS)
- Entre los miembros del equipo se encontraba A. Turing que ya había implementado una pequeña calculadora
- Aprovechando la experiencia previa y los resultados de los polacos, Turing diseña la *British Bombe* que ayuda en la detección de las configuraciones (claves) diarias de Enigma
- Pese al avance en capacidad de cómputo, las modificaciones que se introducían periódicamente provocaban *silencios* temporales

Máquinas de rotores
Otras máquinas

Lorenz SZ-40/42

(foto Ralph Simpson. *Crypto Machine Page*)

- Maquina de cifrado del alto mando alemán
- Proporcionaba el cifrado/descifrado on line, siendo capaz de manejar grandes volúmenes de datos a alta velocidad
- Antes de acabar la guerra, con objeto de atacar el cifrado de esta máquina, se construye *Colossus*, el primer computador digital (aprox. 1700 válvulas)

M-209

(Dirk Rijmenants' *Cipher Machines and Cryptology*)

- Antes y durante la segunda GM B. Hagelin desarrollan multitud de máquinas: la `B-21` en 1925; la `C-35` en 1935 (encargo francés); la `C-36` en 1936 y la `C-38` en 1938
- La `C-38` se produce bajo licencia por el ejercito americano desde 1940 hasta los años 60 bajo designación `M-209`
- La `M-209` disponía de 6 rotores de 17, 19, 21, 23, 25 y 26 contactos
- Considerada criptográficamente insegura, fue utilizada para cifrado táctico

Máquinas de rotores
Otras máquinas

NEMA

(foto Richard Jelbert. *Crypto Machine Page*)

- La falta de seguridad en el sistema de cifrado el gobierno suizo construye su propio sistema. Listo en 1945 se pone en activo en 1947
- En esencia una ENIGMA, disponía de 10 rotores (4×2, un reflector y un rotor especial) pero sin panel de conexiones
- Retirada del servicio en 1992

Máquinas de rotores
Otras máquinas

KL7 ADONIS

(foto John Alexander. *Crypto Machine Page*)

- Introducida por la NSA en 1952 como sustitura de SIGABA (en activo desde los años 40)
- Para difrado off-line. Disponía de 8 rotores con paso configurable mediante micro-conmutadores
- Ofrecía un compromiso en la época para la comunicación segura sin revelar tecnología sensible
- Considerada obsoleta en 1963. En servicio hasta 1983. Algunos detalles continúan clasificados

Máquinas de rotores
Otras máquinas

FIALKA M-125

(foto John Alexander. *Crypto Machine Page*)

- Entra en servicio en 1965. Columna vertebral de las comunicaciones durante la guerra fría
- Construcción basada en ENIGMA pero con 10 rotores. El cableado interior de cada rotor era configurable de entre 30 posibles
- Un lector de tarjetas perforadas permitía variar gran cantidad de parámetros de forma sencilla
- El reflector incluía un circuito que evita que un caracter no pueda cifrarse con él mismo

Máquinas de rotores
Otras máquinas

Gretacoder-805

(foto John Alexander. *Crypto Machine Page*)

- Construcción basada en un microprocesador con memoria de 4000 caracteres
- Incluía impresora, un modem para la transmisión de la señal a través de lineas telefónicas (protocolo V.21) e interfaz para cinta de cassette

Máquinas de rotores
Otras máquinas

MK-85C

(foto John Alexander. *Crypto Machine Page*)

- Basada en la MK-85 (en esencia un micro computador de 1980 basado en equivalentes occidentales)
- La pantalla matricial mostraba el resultado del cifrado/descifrado
- Tamaño máximo del mensaje de 750 caracteres alfanuméricos
- Espacio de claves de 10^{100}

Máquinas de rotores
Recursos

- Field Manual NO 34-40-2 Headquarters Department of the Army: enlace
- Información histórica y técnica tanto de Enigma como de otras máquinas (incluye simuladores): enlace
- Cripto Machine Page: enlace
- Crypto Museum: enlace
- Enigmaco.de: simulador flash de una máquina de tres rotores (por Frank Spieß): enlace