



Figura 12. Charles Babbage.

Cuando Babbage abandonó su primera máquina, el gobierno perdió la confianza en él y decidió cortar por lo sano y retirarse del proyecto; ya había gastado 17.470 libras esterlinas, suficiente para construir un par de acorazados. Probablemente fue esta retirada de apoyo lo que provocó la siguiente queja de Babbage: «Propón a un inglés cualquier principio, o cualquier instrumento y, por admirables que éstos sean, verás que todo el esfuerzo de la mente inglesa se concentra en encontrar una dificultad, un defecto o una imposibilidad en ellos. Si le hablas de una máquina para pelar patatas, dirá que es imposible: si pelas una patata con esa máquina delante de él, dirá que no sirve para nada, porque no puede cortar una piña en rodajas».

La falta de financiación gubernamental significó que Babbage nunca completó el Motor de Diferencias N.^o 2. La tragedia científica era que la máquina de Babbage habría ofrecido la característica única de ser programable. En vez de meramente calcular una serie específica de tablas, el Motor de Diferencias N.^o 2 habría podido resolver una gran variedad de problemas matemáticos, dependiendo de las instrucciones que se le dieran. De hecho, el Motor de Diferencias N.^o 2 suministró el modelo, la plantilla, para los ordenadores modernos. El diseño incluía una «reserva» (memoria) y un «molino» (procesador), que le permitirían tomar decisiones y repetir instrucciones, que son equivalentes a los comandos «SI... ENTONCES...» y «RIZO» de la programación moderna.

Un siglo después, durante el curso de la segunda guerra mundial, las primeras encarnaciones electrónicas de la máquina de Babbage tendrían un profundo efecto en el criptoanálisis, pero durante su propia vida, Babbage hizo una contribución igualmente importante al desciframiento de códigos: consiguió descifrar la cifra Vigenère y al hacerlo realizó el mayor avance criptoanalítico desde que los eruditos árabes del siglo IX descifraron la cifra monoalfabética inventando el análisis de frecuencia. El trabajo de Babbage no requirió cálculos mecánicos ni cómputos complejos. Por el contrario, lo único que utilizó fue pura astucia.

A Babbage le interesaban las cifras desde que era muy joven. Más adelante, recordó cómo esa afición de su infancia a veces le causó problemas: «Los chicos mayores hacían cifras, pero si yo conseguía unas pocas palabras, generalmente descubría la clave. En ocasiones, la consecuencia de este ingenio resultó dolorosa: los dueños de las cifras detectadas a veces me daban una paliza, a pesar de que la culpa la tenía su propia estupidez». Estas palizas no le desanimaron y continuó cautivado por el criptoanálisis. En su autobiografía escribió que «descifrar es, en mi opinión, una de las artes más fascinantes».

Pronto adquirió reputación en la sociedad londinense como criptoanalista dispuesto a abordar cualquier mensaje cifrado, y a veces se le acercaban extraños para consultarle todo tipo de problemas. Por ejemplo, Babbage ayudó a un biógrafo desesperado que trataba de descifrar las notas de taquigrafía de John Flamsteed, el primer astrónomo real de Inglaterra. También auxilió a un historiador resolviendo una cifra de Enriqueta María, la esposa de Carlos I de Inglaterra. En 1854 colaboró con un abogado y utilizó el criptoanálisis para revelar una prueba crucial en un caso legal. A lo largo de los años, acumuló un gran archivo de mensajes cifrados, que planeaba usar como base para un libro seminal sobre el criptoanálisis, titulado *The Philosophy of Decyphering* («La filosofía del desciframiento»). El libro contendría dos ejemplos de todos los tipos de cifras, uno que sería descifrado como demostración y otro que sería dejado como ejercicio para el lector. Desgraciadamente, como sucedió con muchos otros de sus grandes planes, el libro nunca se completó.

Mientras la mayoría de los criptoanalistas habían abandonado toda esperanza de llegar a descifrar la cifra Vigenère, a Babbage le animó a intentar el desciframiento un intercambio de cartas con John Hall Brock Thwaites, un dentista de Bristol con un concepto bastante inocente de las cifras. En 1854, Thwaites afirmó haber inventado una nueva cifra, que, en realidad, era equivalente a la cifra Vigenère. Escribió al *Journal of*

the Society of Arts con la intención de patentar su idea, por lo visto sin darse cuenta de que llegaba con varios siglos de retraso. Babbage escribió a esa sociedad señalando que «la cifra... es muy antigua, y aparece en la mayoría de los libros». Thwaites no ofreció ningún tipo de disculpas y desafió a Babbage a descifrar su cifra. Que fuera o no descifrable no tenía nada que ver con el hecho de si era nueva o no, pero la curiosidad de Babbage se excitó lo suficiente como para embarcarse en la búsqueda de un punto débil en la cifra Vigenère.

Descifrar una cifra difícil es similar a escalar la cara muy escarpada de un acantilado. El criptoanalista busca cualquier resquicio o arista que pudiera proveer el más ligero apoyo. En una cifra monoalfabética, el criptoanalista se agarrará a la frecuencia de las letras, porque las letras más corrientes —en inglés, la **e**, la **t** y la **a**— destacarán no importa cómo hayan sido escondidas. En la polialfabética cifra Vigenère, las frecuencias están mucho más equilibradas, porque se usa la palabra cifra para cambiar entre diferentes alfabetos cifrados. Por eso, a primera vista, la roca parece perfectamente lisa.

Recuerde, la gran fuerza de la cifra Vigenère es que la misma letra será codificada de maneras diferentes. Por ejemplo, si la palabra clave es **KING** (rey), entonces cada letra del texto llano puede ser potencialmente codificada de cuatro maneras diferentes, porque la clave tiene cuatro letras. Cada letra de la clave define un alfabeto cifrado diferente en el cuadro Vigenère, tal como se muestra en la Tabla 7. La columna e del cuadro ha sido marcada para mostrar cómo se codifica de manera distinta dependiendo de qué letra de la clave defina la codificación:

Si se usa la **K** de **KING** para codificar la **e**, la letra resultante en el texto cifrado es la **O**.
Si se usa la **I** de **KING** para codificar la **e**, la letra resultante en el texto cifrado es la **M**.
Si se usa la **N** de **KING** para codificar la **e**, la letra resultante en el texto cifrado es la **R**.
Si se usa la **G** de **KING** para codificar la **e**, la letra resultante en el texto cifrado es la **K**.

Tabla 7. Un cuadro Vigenère utilizado en combinación con la clave KING. La clave define cuatro alfabetos cifrados separados, de forma que la letra e puede ser codificada como O, M, R o K.

Llano	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
1	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	
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
26	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	

De manera similar, palabras enteras serán descifradas de maneras diferentes: la palabra **the**, por ejemplo, podría ser codificada como **DPR**, **BUK**, **GNO** o **ZRM**, dependiendo de su posición en relación con la clave. Aunque esto dificulta muchísimo el criptoanálisis, tampoco hace que sea imposible. El dato importante que hay que notar es que si sólo hay cuatro maneras de codificar la palabra **the**, y el mensaje original contiene varios casos de la palabra **the**, entonces es altamente probable que alguna de las cuatro codificaciones posibles se repita en el texto cifrado. Vamos a demostrarlo con el siguiente ejemplo, en el que la línea **The Sun and the Man in the Moon** («El sol y el hombre en la luna») ha sido codificada usando la cifra Vigenère y la clave **KING**.

Clave	K I N G K I N G K I N G K I N G K I N G
Texto llano	t h e s u n a n d t h e m a n i n t h e m o o n
Texto cifrado	D P R Y E V N T N B U K W I A O X B U K W W B T

La palabra **the** es codificada como **DPR** en el primer caso, y luego como **BUK** en la

segunda y en la tercera ocasión. La causa de la repetición de **BUK** es que el segundo **the** está a ocho letras de distancia del tercer **the**, y ocho es un múltiplo del número de letras de la clave, que, como sabemos, tiene cuatro letras. En otras palabras, el segundo **the** fue codificado según su relación con la palabra clave (**the** cae debajo de **ING**), y para cuando llegamos al tercer **the**, la clave ha pasado exactamente dos veces, de manera que se repite esa relación y, por tanto, la codificación.

Babbage se dio cuenta de que este tipo de repetición le suministraba exactamente la asidera que necesitaba para conquistar la cifra Vigenère. Logró definir una serie de pasos relativamente simples que cualquier criptoanalista podía seguir para descifrar la hasta entonces *chiffre indéchiffrable*. Para demostrar su brillante técnica, imaginemos que hemos interceptado el texto cifrado que aparece en la Figura 13. Sabemos que ha sido codificado utilizando la cifra Vigenère, pero no sabemos nada sobre el mensaje original, y la clave es un misterio.

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

Figura 13. El texto cifrado, codificado utilizando la cifra Vigenère.

La primera fase del criptoanálisis de Babbage consiste en buscar secuencias de letras que aparecen más de una vez en el texto cifrado. Hay dos maneras en las que podrían surgir semejantes repeticiones. La más probable es que la misma secuencia de letras del texto llano haya sido codificada usando la misma parte de la clave. Como alternativa, existe una ligera posibilidad de que dos secuencias de letras diferentes del texto llano hayan sido codificadas usando diferentes partes de la clave, resultando por casualidad en

una secuencia idéntica en el texto cifrado. Si nos limitamos a secuencias largas, entonces podemos descartar en gran medida la segunda posibilidad y en este caso, sólo consideramos las secuencias repetidas que tengan cuatro letras o más. La Tabla 8 es un registro de tales repeticiones y de los espacios que hay entre la repetición. Por ejemplo, la secuencia **E-F-I-Q** aparece en la primera línea del texto cifrado y luego en la quinta línea, separada por 95 letras.

Además de utilizarse para codificar el texto llano y convertirlo en el texto cifrado, la clave la usa también el receptor para descifrar el texto cifrado y volverlo a convertir en el texto llano. Por eso, si pudiéramos identificar la clave, descifrar el texto no sería difícil. En esta fase aún no disponemos de suficiente información para deducir la clave, pero la Tabla 8 nos proporciona indicios muy buenos sobre su longitud. Tras enumerar qué secuencias se repiten, así como los espacios que hay entre las repeticiones, el resto de la Tabla se dedica a identificar los *factores* de los espaciamientos: los números por los que se pueden dividir los espaciamientos. Por ejemplo, la secuencia **W-C-X-Y-M** se repite tras 20 letras, por lo que los números 1, 2, 4, 5, 10 y 20 son factores, ya que pueden dividir exactamente a 20 sin dejar decimales. Estos factores sugieren seis posibilidades:

- (1) La clave tiene 1 letra y se recicla 20 veces entre las codificaciones.
- (2) La clave tiene 2 letras y se recicla 10 veces entre las codificaciones.
- (3) La clave tiene 4 letras y se recicla 5 veces entre las codificaciones.
- (4) La clave tiene 5 letras y se recicla 4 veces entre las codificaciones.
- (5) La clave tiene 10 letras y se recicla 2 veces entre las codificaciones.
- (6) La clave tiene 20 letras y se recicla 1 vez entre las codificaciones.

La primera posibilidad puede ser excluida, porque una clave que sólo tenga una letra da lugar a una cifra monoalfabética, sólo se usaría una línea del cuadro Vigenère para toda la codificación, y el alfabeto cifrado permanecería inalterado; es muy improbable que un criptógrafo hiciera algo así. Para indicar cada una de las demás posibilidades se ha colocado un signo ✓ en la columna apropiada de la Tabla 8. Cada ✓ indica una longitud potencial de la clave.

Tabla 8. Repeticiones y espacios entre ellas en el texto cifrado.

Secuencia repetida	Espacio entre repeticiones	Posible longitud de la clave (o factores)																		
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓															✓
P-S-D-L-P	5					✓														
W-C-X-Y-M	20	✓	✓	✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Para identificar si la clave tiene 2, 4, 5, 10 o 20 letras necesitamos observar los factores de todos los demás espaciamientos. Como la clave parece tener 20 letras o menos, la Tabla 8 enumera los factores equivalentes para cada uno de los espaciamientos. Hay una clara propensión por el espaciamiento divisible por 5. De hecho, todos los espaciamientos que aparecen son divisibles por 5. La primera secuencia repetida, **E-F-I-Q**, se puede explicar con una clave de 5 letras, reciclada 19 veces entre la primera codificación y la segunda. La segunda secuencia repetida, **P-S-D-L-P**, se puede explicar con una clave de 5 letras, reciclada sólo una vez entre la primera codificación y la segunda. La tercera secuencia repetida, **W-C-X-Y-M**, se puede explicar con una clave de

5 letras, reciclada 4 veces entre la primera codificación y la segunda. La cuarta secuencia repetida, **E-T-R-L**, se puede explicar con una clave de 5 letras, reciclada 24 veces entre la primera codificación y la segunda. En resumen, todo concuerda con una clave de 5 letras.

Asumiendo que la clave tiene efectivamente 5 letras, el siguiente paso es deducir cuáles son exactamente esas letras. Por ahora, llamemos a la clave $L_1-L_2-L_3-L_4-L_5$, de forma que L_1 represente a la primera letra de la clave, y así sucesivamente. El proceso de codificación habría empezado codificando la primera letra del texto llano según la primera letra de la clave, L_1 . La letra L_1 define una línea del cuadro Vigenère, y de hecho proporciona un alfabeto cifrado de sustitución monoalfabética para la primera letra del texto llano. Sin embargo, a la hora de codificar la segunda letra del texto llano, el criptógrafo habría usado L_2 para definir una línea distinta del cuadro Vigenère, proporcionando de este modo un alfabeto cifrado de sustitución monoalfabética diferente. La tercera letra del texto llano se codificaría según L_3 , la cuarta según L_4 y la quinta según L_5 . Cada letra de la clave proporciona un alfabeto cifrado diferente para la codificación. Sin embargo, la sexta letra del texto llano sería codificada de nuevo según L_1 , la séptima letra del texto llano sería codificada de nuevo según L_2 y el ciclo se repite después de eso. En otras palabras, la cifra polialfabética consta de cinco cifras monoalfabéticas, cada cifra monoalfabética es responsable de la codificación de un quinto del mensaje total y, lo que es más importante, ya sabemos cómo criptoanalizar las cifras monoalfabéticas.

Procederemos de la siguiente manera. Sabemos que una de las líneas del cuadro Vigenère, definida por L_1 , proporciona el alfabeto cifrado para codificar las letras 1^a , 6^a , 11^a , 16^a ... del mensaje. Por eso, si observamos las letras 1^a , 6^a , 11^a , 16^a ... del texto cifrado podríamos utilizar el análisis de frecuencia tradicional para deducir el alfabeto cifrado en cuestión. La Figura 14 muestra la distribución de la frecuencia de las letras que aparecen en las posiciones 1^a , 6^a , 11^a , 16^a ... del texto cifrado, que son **W, I, R, E...** Es preciso recordar ahora que cada alfabeto cifrado del cuadro Vigenère es simplemente un alfabeto normal desplazado entre 1 y 26 posiciones. Por eso, la distribución de frecuencias de la Figura 14 debería tener rasgos similares a la distribución de frecuencias de un alfabeto normal, excepto que habrá sido desplazado unas cuantas posiciones. Al comparar la distribución L_1 con la distribución normal debería ser posible calcular ese desplazamiento. La Figura 15 muestra la distribución de frecuencias normal en un fragmento de texto llano en inglés.

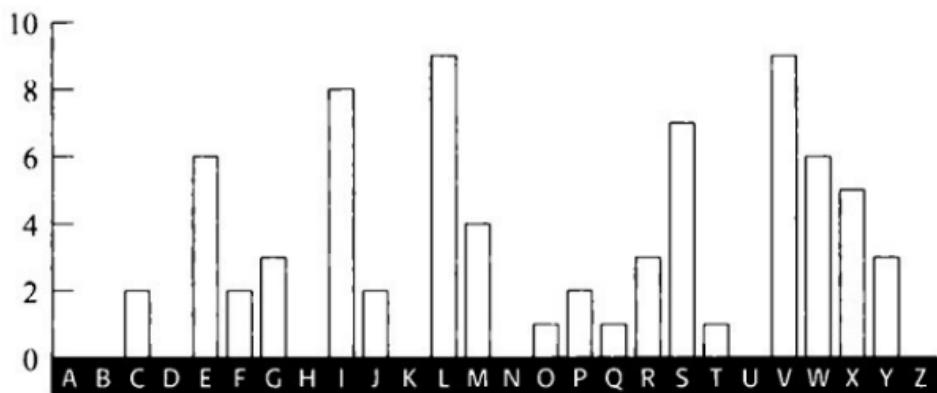


Figura 14. Distribución de frecuencias para las letras del texto cifrado, codificado utilizando el alfabeto cifrado L_1 (número de apariciones).



Figura 15. Distribución de frecuencias normal en inglés (número de apariciones basado en un fragmento de texto llano que contiene el mismo número de letras que el texto cifrado).

La distribución normal muestra cimas, mesetas y valles, y para hacerla encajar con la distribución de la cifra L_1 buscamos la combinación de rasgos más sobresaliente. Por ejemplo, los tres pilares de **R-S-T** en la distribución normal (Figura 15) y la larga depresión a su derecha, que se extiende a lo largo de seis letras, de la **U** hasta la **Z**: ambas cosas juntas forman un par muy característico de rasgos. Los únicos rasgos similares en la distribución L_1 (Figura 14) son los tres pilares de **V-W-X**, seguidos de la depresión que se extiende a lo largo de seis letras, de la **Y** a la **D**. Esto sugeriría que todas las letras codificadas según L_1 se han desplazado cuatro posiciones o, en otras palabras, que L_1 define un alfabeto cifrado que comienza **E, F, G, H...** A su vez, esto significa que la primera letra de la clave, L_1 , es probablemente la **E**. Esta hipótesis se puede poner a prueba desplazando la distribución L_1 cuatro lugares y comparándola con la distribución normal. La Figura 16 muestra ambas distribuciones para poder comparar. La coincidencia entre las cimas mayores es muy grande, implicando que resulta seguro asumir que la clave comienza efectivamente por **E**.

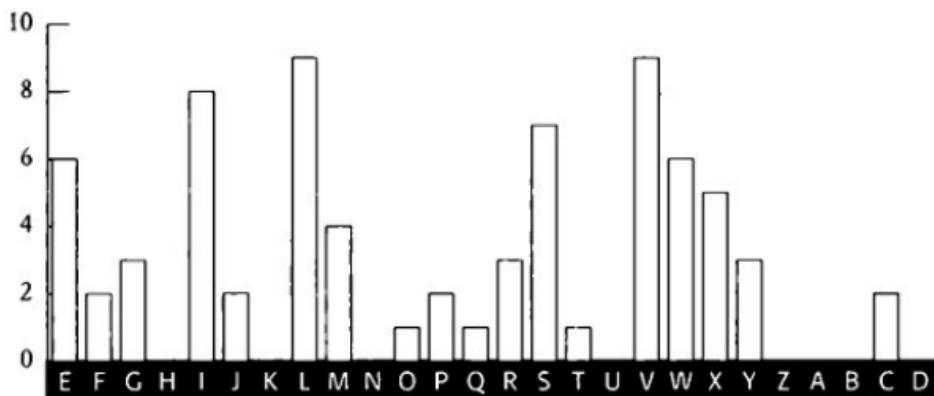


Figura 16. La distribución L_1 desplazada cuatro lugares (arriba), comparada con la distribución de frecuencias normal (abajo). Todas las cimas y las depresiones principales encajan.

Resumiendo, buscar repeticiones en el texto cifrado nos ha permitido identificar la longitud de la clave, que resultó ser de cinco letras. Esto nos permitió dividir el texto cifrado en cinco partes, cada una de ellas codificada según una sustitución monoalfabética definida por una letra de la clave. Analizando la fracción del texto cifrado que fue codificado según la primera letra de la clave, hemos podido mostrar que esta letra L_1 es probablemente la E. Este proceso se repite para identificar la segunda letra de la clave. Así, establecemos una distribución de frecuencias para las letras $2^a, 7^a, 12^a, 17^a \dots$ del texto cifrado. De nuevo, la distribución resultante, que se muestra en la Figura 17, se compara con la distribución normal para deducir el desplazamiento.

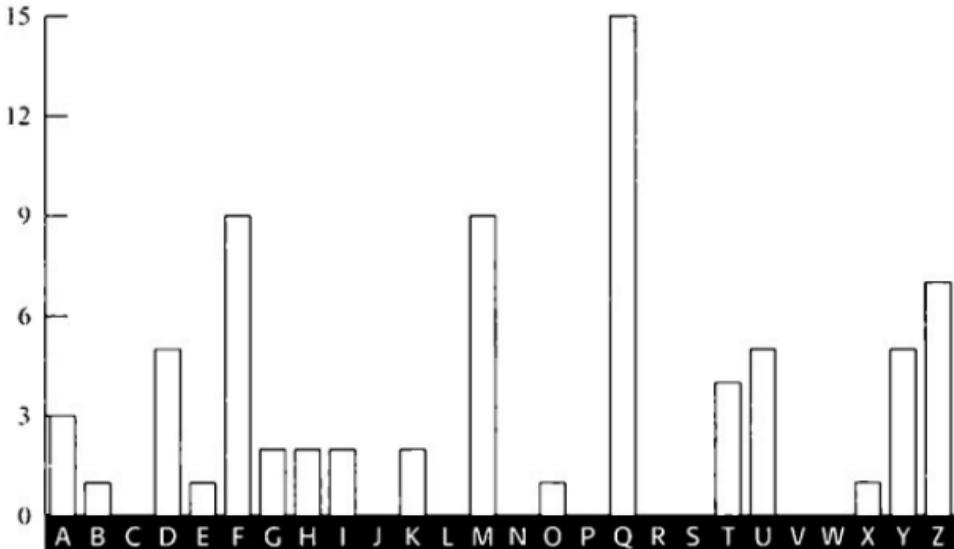


Figura 17. Distribución de frecuencias para las letras del texto cifrado, codificado usando el alfabeto cifrado L_2 (número de apariciones).

Esta distribución es más difícil de analizar. No hay candidatas obvias para las tres cimas vecinas que se corresponden con **R-S-T** en la distribución normal. No obstante, la depresión que se extiende de la **G** a la **L** es muy característica, y probablemente se corresponde con la depresión que esperamos ver extendiéndose de la **U** a la **Z** en la distribución normal. Si esto fuera así, esperaríamos que las tres cimas **R-S-T** aparecerían en la **D**, la **E** y la **F**, pero falta la cima de la **E**. Por ahora, desestimaremos la cima que falta como una irregularidad estadística y seguiremos nuestra reacción inicial, que es que la depresión de la **G** a la **L** es un rasgo apreciable de desplazamiento. Esto sugeriría que todas las letras codificadas según L_2 han sido desplazadas 12 posiciones, o, en otras palabras, que define un alfabeto cifrado que comienza **M, N, O, P...** y que la segunda letra de la clave, L_2 , es la **M**. Una vez más, esta hipótesis se puede poner a prueba desplazando la distribución L_2 doce lugares y comparándola con la distribución normal. La Figura 18 muestra ambas distribuciones y se ve que las cimas mayores encajan muchísimo, dando a entender que resulta seguro asumir que la segunda letra de la clave es efectivamente la **M**.

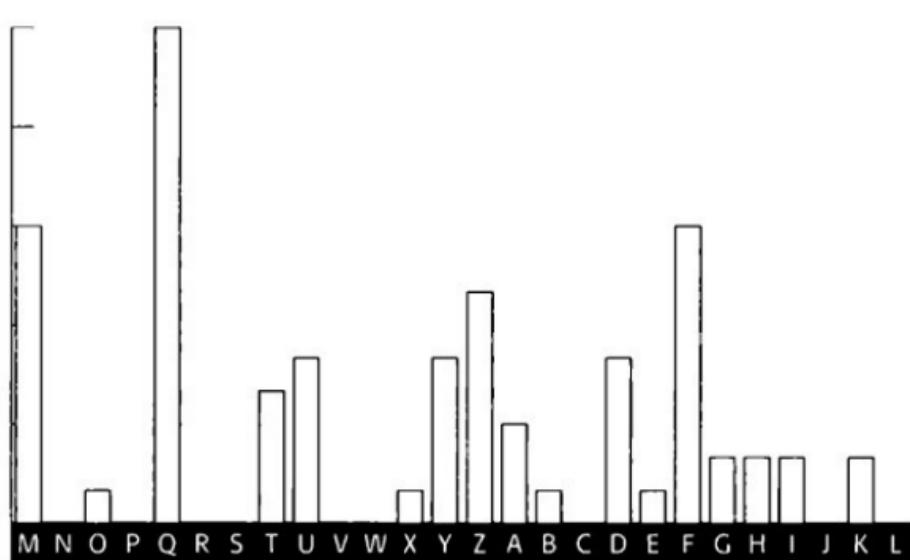


Figura 18. La distribución L_2 desplazada doce letras (arriba), comparada con la distribución de frecuencias normal (abajo). La mayoría de las principales cimas y depresiones coinciden.

No voy a continuar el análisis; baste decir que al analizar las letras 3^a, 8^a, 13^a... se deduce que la tercera letra de la clave es la **I**; al analizar las letras 4^a, 9^a, 14^a... se deduce que la cuarta letra es la **L**; y al analizar las letras 5^a, 10^a, 15^a... se deduce que la quinta letra es la **Y**. La clave es **EMILY**. Ahora es posible invertir la cifra Vigenère y completar el criptoanálisis. La primera letra del texto cifrado es la **W**, y fue codificada según la primera letra de la clave, la **E**. Invirtiendo el proceso, miramos el cuadro Vigenère y encontramos la **W** en la línea que comienza por **E**, y de esta forma descubrimos qué letra encabeza esa columna. Se trata de la **S**, por lo que la ponemos como la primera letra del texto llano. Repitiendo este proceso, vemos que el texto llano comienza **sittheedownandhavenoshame-cheekby-jowl...** Insertando las separaciones entre palabras y la puntuación adecuadas, llegamos por fin a:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:

What care I for any name?

What for order or degree?

Let me screw thee up a peg:

Let me loose thy tongue with wine:

Callest thou that thing a leg?

Which is thinnest?, thine or mine?

Thou shalt not be saved by works:

Thou hast been a sinner too:

Ruined trunks on withered forks,

Empty scarecrows, I and you!

Fill the cup, and fill the can:

Have a rouse before the morn:

Every moment dies a man,

Every moment one is born^[6].

Son versos de un poema de Alfred Tennyson titulado «The Vision of Sin» («La visión del pecado»). La clave resulta ser el nombre de pila de la esposa de Tennyson, Emily Sellwood. Decidí utilizar un fragmento de este poema en particular para un ejemplo de criptoanálisis porque inspiró una curiosa correspondencia entre Babbage y el gran poeta. Como agudo estadístico y compilador de índices de mortalidad, a Babbage le irritaban los versos «Cada momento muere un hombre, / Cada momento nace uno», que son las últimas líneas del texto llano previo. Por consiguiente, ofreció una corrección al poema de Tennyson, «por lo demás muy hermoso»:

Hay que señalar que si eso fuera cierto, la población del mundo estaría estancada... Yo le sugeriría que en la próxima edición de su poema, éste dijera: «Cada momento muere un hombre, Cada momento nace $1 \frac{1}{16}$ »... La cifra exacta es tan larga que no la puedo incluir en un verso, pero creo que la cifra $1 \frac{1}{16}$ será suficientemente exacta para la poesía.

Muy atentamente, etc.,

Charles Babbage.

El satisfactorio criptoanálisis de la cifra Vigenère realizado por Babbage fue logrado probablemente en 1854, poco después de su altercado con Thwaites, pero su descubrimiento no fue reconocido en absoluto, porque nunca lo publicó. El descubrimiento no salió a la luz hasta el siglo XX, cuando algunos eruditos examinaron las extensas notas de Babbage. Mientras tanto, su técnica fue descubierta independientemente por Friedrich Wilhelm Kasiski, un oficial retirado del ejército prusiano. Desde 1863, cuando publicó su gran avance criptoanalítico en *Die Geheimschriften und die Dechiffirkunst* («La escritura secreta y el arte del desciframiento»), la técnica ha sido conocida como la Prueba Kasiski, y la contribución de Babbage ha sido ignorada en gran medida.

Pero ¿por qué no publicó Babbage su desciframiento de una cifra tan vital? Ciertamente, tenía el hábito de no acabar sus proyectos y no publicar sus descubrimientos, lo que podría sugerir que éste es simplemente un ejemplo más de su actitud indolente. Sin embargo, hay una explicación alternativa. Su descubrimiento sucedió poco después del estallido de la guerra de Crimea, y una teoría es que ese descubrimiento proporcionó a los británicos una clara ventaja sobre su enemigo ruso. Es muy posible que la Inteligencia británica exigiera que Babbage mantuviese secreto su trabajo, proporcionándole de esta forma una ventaja de nueve años sobre el resto del mundo. Si esto fuera así, encajaría con la ya antigua tradición de encubrir los logros del desciframiento en beneficio de la seguridad nacional, una práctica que ha continuado en