Nombre:_____ Fecha:_____

Actividad *NUMB3RS*: El tablero de claves

En “la lista Janus” un terrorista queda gravemente herido cuando el FBI frustra su atentado con una bomba. En el hospital, logra indicar con los dedos una secuencia de números que Charlie reconoce como un mensaje en clave. Con ayuda de Don, Charlie comprende que se trata de una *clave de tablero de damas* y logra descifrar el mensaje después de experimentar con la clave. Es difícil descifrar una clave de tablero de damas porque cifra ciertas letras como un solo dígito y otras letras como un par de dígitos. El que intenta descifrar un mensaje interceptado no sabe las ubicaciones de los dígitos sencillos, y podría por lo tanto juntar dígitos que deben estar separados. El resultado sería una página de incoherencias.

Hay muchas variantes de esta clave. Los dígitos del primer renglón se pueden colocar en cualquier orden. Por lo general se usa una *palabra clave* de ocho letras (sin letras repetidas) en el primer renglón (indicada abajo con mayúsculas). Los dos números que no se usan con la palabra clave se convierten en rótulos de los dos últimos renglones y pueden ocupar cualquier lugar. Las casillas restantes en estos renglones corresponden a las letras restantes del alfabeto, por lo general en orden alfabético, con espacio para un punto y un *signo de barra* que se usa para codificar números. Por ejemplo:

	0	9	8	7	6	5	4	3	2	1
	M	A	T	H		C	O	D	E	
1	b	f	g	i	j	k	l	n	p	q
6	r	s	u	v	w	x	y	z	.	/

La clave tiene la forma de (renglón, columna). Los números sin usar del renglón superior son las únicas coordenadas de renglón posibles; por tanto, las letras de la palabra clave están cifradas como dígito sencillo.

1. ¿Cuántas claves son posibles sólo cambiando el lugar de los dígitos sin usar?

Para cifrar “Janus” las coordenadas son (1, 6); (_, 9); (1, 3); (6, 8) y (6, 9). La clave completa es 169136869. Observa que *“a”* no tiene coordenada de renglón y aparece como dígito sencillo. Quien reciba el mensaje (y tenga la palabra clave, por supuesto) sabe que donde hay un 1 o un 6 comienza un par. Los espacios entre palabras no van cifrados. Eso le daría otra pista al interceptor.

2. Cifra lo siguiente:
- **a.** “attack the dock” _____
- **b.** “rush shipment” _____

3. Compara la extensión de cada mensaje con la extensión de la clave. ¿Qué notas?

4. Las letras más usadas (en orden descendente) en inglés son **e-t-a-o-i-n-s-r**. En algunas variantes del tablero de claves se usan estas letras en lugar de una palabra clave. ¿Por qué sería esto conveniente?

5. Un argumento para usar una palabra clave en lugar de letras es la facilidad para memorizar. Una manera es la mnemotecnia: “Estonia-R”. ¿Qué par de palabras comunes fáciles de memorizar que se pueden formar con las letras “e-t-a-o-i-n-s-r”?

6. Descifra: 1040106813326010601731 82.

L. Charles (Chuck) Biehl, Escuela Charter de Wilmington, Wilmington, DE

El objeto de esta actividad es dar a los estudiantes un vistazo breve y sencillo de un tema matemático muy extenso. TI y NCTM lo invitan a usted y a sus estudiantes a aprender más sobre este tema con las extensiones que se ofrecen abajo y con su propia investigación independiente.

Extensiones

Introducción

La clave del tablero de claves es uno de tantos códigos y claves históricos. Las palabras *clave* y *código* se usan como sinónimos. La diferencia principal es que en una *clave* se sustituyen o cambian letras sencillas o pares de letras, mientras que en los códigos se sustituyen palabras completas, frases o conjuntos de números. Los dos aparecen a lo largo de la historia desde hace aproximadamente 4,000 años.

Para el estudiante

- Al usar la clave cifras de esta actividad para enviar números, se usa el carácter "/" al comienzo y al final de una serie de números. A menudo se duplica cada dígito para reducir los errores de transmisión. Por ejemplo el mensaje "I need 500 sandwiches" se cifra como INEED/500/SANDWICHES ("61" es "/") y, por tanto, resulta: 171322361550000616991336617572 69.

- Para mayor seguridad, se le puede agregar otro nivel de codificación a la clave de tablero agregándole un *número clave* secreto antes de enviarlo. Supongamos que se escogen como número clave los primeros cinco dígitos de π: 31415. Esto se agrega a la clave sin llevar la suma (sólo se anota el dígito de las unidades), de modo que la clave anterior se convierte en:

  $$\begin{array}{l} \quad 171322361550000616991336617572 69 \\ +\ 31415314153141531415314153141531 \\ \quad 485475402081415920044477148987 90 \end{array}$$

- Para **más** seguridad aún, esta clave se puede pasar por la misma clave de tablero para convertirla en letras. Se obtiene:
  OTCOHCOMEMTLKAEMMOOOHHLTATHAM

- Usando el tablero y el número clave, recupera el mensaje original.

Tema relacionado

Otros ejemplos de claves históricas son la de César (shift), la de los masones, la clave ADFVDX (Primera Guerra Mundial), la clave Vigenère y una lista casi infinita de otras muy interesantes. Tal vez la más famosa de las claves mecánicas es ENIGMA (Segunda Guerra Mundial). Hay muchos libros y recursos en la red electrónica para aprender acerca de estas claves y su importancia histórica.

Recursos adicionales

Para una introducción interactiva al concepto general de la criptografía, ver:
http://williamstallings.com/Crypt-Tut/Crypto%20Tutorial%20-%20JERIC.swf

Un libro excelente sobre códigos y claves a lo largo de la historia es el de Simon Singh: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*.

L. Charles (Chuck) Biehl, Escuela Charter de Wilmington, Wilmington, DE