Nombre: _____ Fecha: _____

Actividad *NUMB3RS*: Pelador de cebollas

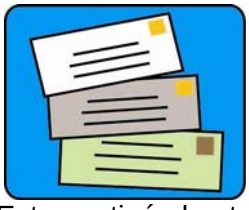
En el episodio “Charla mortal” el asesino envía por Internet videos de confesiones. Para rastrear los orígenes de esos videos Charlie descubre que el asesino está ocultando su ubicación en línea por medio de un esquema en forma de cebolla. Charlie explica que tal esquema es un modo de enviar contenido por una red conservando el anonimato.

Es como enviar por correo una serie de sobres dentro de sobres.

Se envía un sobre al nombre en la dirección.

Dentro del sobre hay otro sobre que se envía a la segunda dirección.

Dentro del segundo sobre hay otro. De nuevo, éste se envía a la siguiente dirección.



Esto continúa hasta que finalmente se revela el mensaje contenido en el último sobre: “Compre más sobres”.

Al final, la persona a quien le dicen que compre más sobres no sabe quién ni de dónde se envió el sobre original. Cada sobre es como una de las capas de una cebolla que se va pelando hasta que el mensaje en el interior llega a su destino. Funciona igual en Internet, pero en vez de sobres, el remitente emplea una serie de rutas, y en vez de abrir sobres, los distribuidores de la red (routers) emplean un algoritmo descodificador.

El siguiente es un algoritmo descodificador empleado para rastrear un mensaje por la red en forma de cebolla. Se emplea un mensaje de muestra.

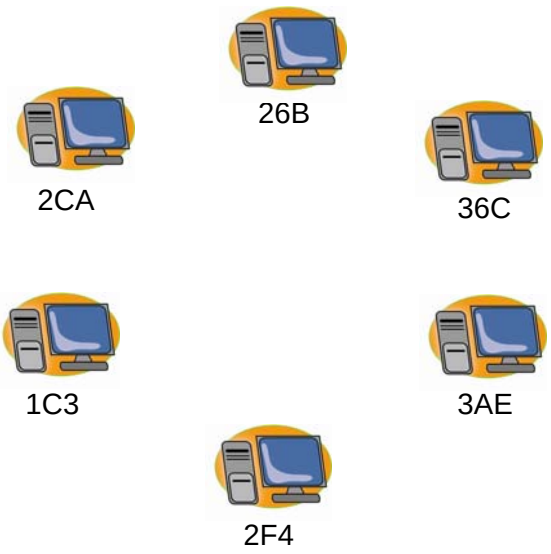
Pasos	**Ejemplo**
Cada distribuidor tiene asignado un número hexadecimal de tres dígitos. Los números hexadecimales (de base16) se emplean en lenguajes de computadora, como el HTML. Se escriben con los dígitos 0–9 y las letras A–F. Para nuestra red en forma de cebolla, traduce el número hexadecimal de distribución a un número decimal de tres dígitos. Este número decimal es la Clave del distribuidor. El primer dígito indica la dirección desde donde se empieza a contar (par desde la izquierda e impar desde la derecha), y los dígitos segundo y tercero indican las posiciones de los dos caracteres que deben intercambiarse.	El distribuidor de la red 1AD traduciría a $\left(1 \bullet 16^2\right) + \left(10 \bullet 16^1\right) + \left(13 \bullet 16^0\right) = 429$ 4 | 2 | 9 El primer dígito es par, así que se empieza a contar desde la izquierda | Intercambia los caracteres segundo y el noveno en el código Cuenta desde la izquierda e intercambia los caracteres segundo y noveno. 2**A**4BY3NR**5** → 2**5**4BY3NR**A**

© 2006 Texas Instruments Incorporated
Brock Wenciker, Escuela Secundaria Shawnee Mission East, Overland Park, KS

Elimina los caracteres primero y último del mensaje. Estos son los dígitos primero y último del siguiente distribuidor.	Eliminando 2 y A, el mensaje que queda 54BY3NR se enviaría a un distribuidor como 2CA.
Repite el algoritmo descodificador hasta que el primer y el último caracter sean AA. Este es el código final.	

Para esta actividad se ha codificado el segundo nombre de Charlie. Al descodificar su segundo nombre abajo, rastrea el camino del mensaje al pasar por la red en forma de cebolla.

Convierte los Números de distribución de su Número hexadecimal de distribución a sus correspondientes Claves de distribución decimales.



Número de distribución	Clave de distribución

Número de distribución	Clave de distribución	(Par)								Mensaje							(Impar)
1C3		A	D	2	3	2	3	D	4	W	3	C	A	R	4	E	B
Mensaje																	

El mensaje puede parecer codificado todavía pero en realidad está escrito en lenguaje 1337 (Leet) speak. En el episodio Charlie y el FBI analizan la charla en línea del asesino y encuentran que gran parte está escrita en Leet speak. Leet speak es una modificación del texto escrito en que suelen reemplazarse letras con números y símbolos. Por ejemplo, el título del programa, *NUMB3RS,* emplea el número 3 en lugar de la letra “E”.

1. ¿Cuál es el segundo nombre de Charlie?

2. ¿Qué distribuidor de la red no se empleó en el esquema en forma de cebolla?

© 2006 Texas Instruments Incorporated

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

Para codificar un mensaje, debemos invertir el algoritmo. Por ejemplo, para codificar la palabra **Calculus** podemos traducirla primero a Leet speak.

Pasos	Ejemplo
Primero, traduce el mensaje a Leet speak.	Calculus ↦ K4LCULUZ
Agrega la letra A al comienzo y al final de tu mensaje.	AK4LCULUZA
Con la Clave del distribuidor de la red correspondiente a cierto Número de distrbución que elijas intercambia los caracteres especificados. El primer dígito indica la dirección de donde se empieza a contar (par desde la izquierda e impar desde la derecha), y los dígitos 2.º y 3.º indican las posiciones de los dos caracteres que deben intercambiarse.	La Clave para el distribuidor 2F4 es 756. 7: El dígito es impar: empieza a contar desde la derecha 5 6: Intercambia los caracteres cinco y seis en el código AK4LCULUZAA ↦ AK4**CL**ULUZAA
Añade al comienzo y final de tu mensaje las letras primera y tercera del distribuidor de la red que deseas usar enseguida.	Para el distribuidor de la red 2F4 añade 2 al comienzo y 4 al final de tu mensaje. 2AK4CLULUZAA4
Repite estos pasos varias veces escogiendo diferentes distribuidores hasta que el mensaje esté codificado.	1C3 **C**AK4**2**LULUZAA4 1CAK42LULUZAA43 26B **L**CAK42LU**1**UZAA43 2LCAK42LU1UZAA43B 3AE 2LCAK42LU1UZA**3**4**A**B 32LCAK42LU1UZA34ABE 36C 32LCA**4K**2LU1UZA34ABE 332LCA4K2LU1UZA34ABEC 26B **2**32LCA4K**3**LU1UZA34ABEC 2232LCA4K3LU1UZA34ABECB 2F4 2232LCA4K3LU1UZA3**A4**BECB 22232LCA4K3LU1UZA3A4BECB4
Mensaje codificado	22232LCA4K3LU1UZA3A4BECB4

Con el algoritmo codificador y los Números de distribución de la actividad, codifica un mensaje. Luego, un compañero de clase debe descodificarlo.

Recursos adicionales

El applet en este sitio Web convierte números entre las formas decimal, binaria y hexadecimal:
http://www.willamette.edu/~gorr/classes/cs130/lectures/BinaryConversion/convert.html

La red en forma de cebolla Tor tiene centenares de miles de usuarios. Lee cómo funciona Tor en el sitio **http://tor.eff.org/overview.html.en**

Fort Consult escribió un ensayo sobre Practical Onion Hacking publicado en octubre de 2006. Puedes leerlo en **http://www.packetstormsecurity.org/0610-advisories/Practical_Onion_Hacking.pdf**.

© 2006 Texas Instruments Incorporated
Brock Wenciker, Escuela Secundaria Shawnee Mission East, Overland Park, KS