SdA 3: Hackers y primos: el enigma de tu WhatsApp

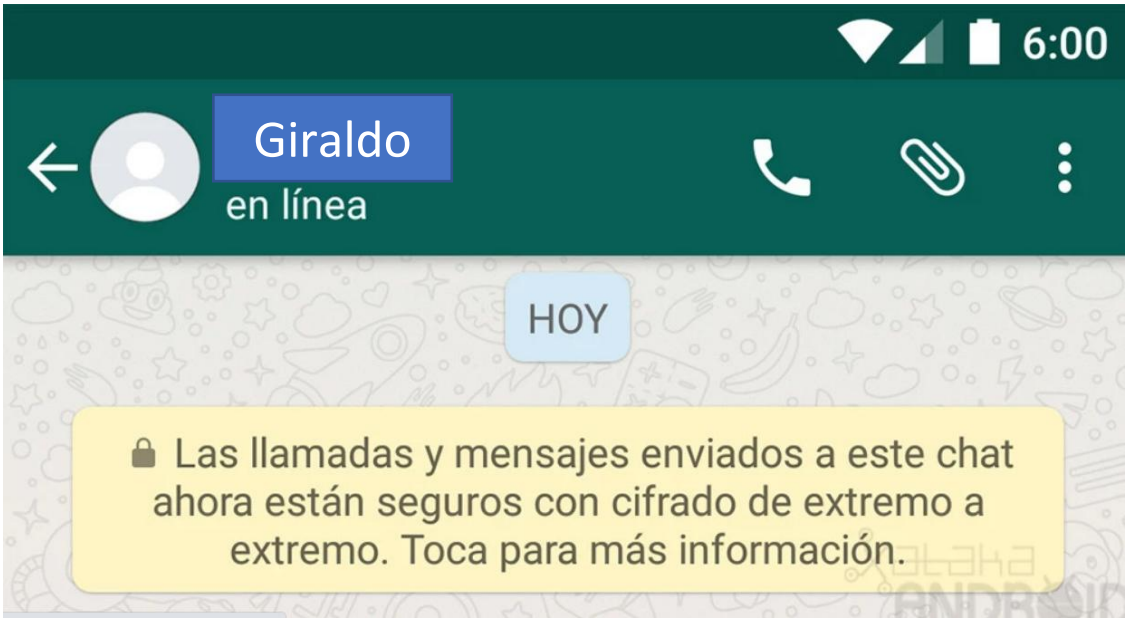
Vivimos conectados: WhatsApp, compras online, banca digital, redes sociales… Todo ello funciona gracias a un «secreto» matemático milenario: los números primos. En esta SdA, os vais a convertir en un equipo de ciberseguridad que debe comprender, investigar y divulgar cómo los primos protegen nuestra privacidad.

«Misión Alpha: un mensaje ha sido interceptado»
El director del instituto recibe un correo anónimo: «Vuestras contraseñas están en peligro. Solo quienes comprendan los números primos podrán protegerlas». Adjunta un mensaje cifrado que nadie entiende. Os han elegido como ***equipo de ciberdefensores del centro****. ¿Aceptáis el reto?*

- ¿Cómo es posible que WhatsApp diga que nuestros mensajes son «seguros»?
- ¿Qué tienen que ver los números con la privacidad?
- ¿Quién protege realmente nuestras contraseñas?

FASE 1: Descifrando el enemigo – «Interceptamos un mensaje»
Nuestro primer trabajo como ciberdefensores es aprender a leer mensajes cifrados. Los ordenadores solo entienden números, así que toda la información digital se traduce a ellos.

Nuestras conversaciones de WhatsApp son «seguras».
El mensaje que se muestra en la imagen nos dice que nuestras llamadas y mensajes están cifradas, esto es, que solo las van a poder escuchar/leer los interesados y nadie más.



Pero ¿cómo funciona esto? Vamos a verlo con un ***ejemplo muy sencillo*** (el caso real de WhatsApp es bastante más complicado)

1º) Los ordenadores solo trabajan con números, por lo que cualquier palabra/frase lo que hacen es escribirla con números (en sistema binario)

2º) Nosotros, por simplificar, trabajaremos con números naturales, y a cada letra le asociamos un número:

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
11	12	13	14	15	16	17	18	19	20
U	**V**	**W**	**X**	**Y**	**Z**	**Espacio**			
21	22	23	24	25	26	0			

Vamos a descifrar el código 144202053038

a) Agrupamos las cifras de dos en dos, de derecha a izquierda:
14 42 02 05 30 38

b) A cada grupo de dos cifras le aplicamos la siguiente regla:
Si es par, lo dividimos entre 2.
Si es impar, lo multiplicamos por 3 y el sumamos 1.

En nuestro caso:

14 es par $\Rightarrow 14:2=\boxed{7}$

42 es par $\Rightarrow 42:2=\boxed{21}$

02 es par $\Rightarrow 02:2=\boxed{1}$

05 es impar $\Rightarrow 5\cdot 3+1=\boxed{16}$

30 es par $\Rightarrow 30:2=\boxed{15}$

38 es par $\Rightarrow 38:2=\boxed{19}$

c) El número que se obtiene es: 7 21 1 16 15 19

d) Ahora, mirando en la tabla anterior, cambiamos cada número por la letra correspondiente:

$$\left.\begin{array}{rcl} 7 & \Rightarrow & \text{G} \\ 21 & \Rightarrow & \text{U} \\ 1 & \Rightarrow & \text{A} \\ 16 & \Rightarrow & \text{P} \\ 15 & \Rightarrow & \text{O} \\ 19 & \Rightarrow & \text{S} \end{array}\right\} \Rightarrow \text{El mensaje es GUAPOS}$$

Misión 1: Descifra la palabra 44020602061830281038.

FASE 2: Construyendo nuestra arma secreta – «La Criba de Eratóstenes»

Para proteger datos, primero necesitamos conocer a nuestros «aliados»: los números primos. Hace más de 2.000 años, un genio griego inventó una máquina para encontrarlos.

Construye una tabla con los números del 1 al 100, como la que sigue:

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Misión 2: Busca información, en el libro o en Internet, sobre la Criba de Eratóstenes, y responde a las siguientes cuestiones:

a) Breve biografía de Eratóstenes
b) ¿En qué consiste la Criba de Eratóstenes? (Hay describir dicho algoritmo)
c) Escribe los números primos que hay entre 1 y 100.
d) ¿Consideras que es un buen método para calcular números primos? Razona tu respuesta.
e) ¿Cuál es el único primo que es un número par?
f) En la lista existen números primos tales que, si les das la vuelta a sus cifras, obtenemos también un número primo, como por ejemplo 13 y 31. ¿Qué otras parejas encuentras como esta?

FASE 3: El lenguaje de los ciberdefensores – «Definiciones clave»
Todo equipo profesional necesita un vocabulario común. Antes de avanzar, debemos dominar los conceptos.

Misión 3: Define número primo y número compuesto. ¿El 1 es primo o compuesto? Razona tu respuesta.

FASE 4: Las matemáticas tienen nombre de mujer – «Sophie Germain»
La historia de la criptografía no sería la misma sin una mujer que tuvo que hacerse pasar por hombre para poder estudiar. Conozcamos su legado.

Misión 4: Investiga
Busca información sobre los números primos de Sophie Germain y contesta a las siguientes preguntas:

a) Breve biografía de Sophie Germain
b) ¿Cuándo un número es un primo de Sophie Germain o primo de Germain?
c) Escribe algunos números primos de Sophie Germain.
d) ¿Hay infinitos números primos de Sophie Germain?

FASE 5: Los primos en el mundo real – «¿Dónde los encontramos?»
Ya sabemos qué son, cómo encontrarlos y quiénes los estudiaron. Pero… ¿para qué sirven de verdad?

Misión 5: Investiga
Indica, al menos, dos usos, en la vida real, de los números primos.

FASE 6: Producto Final – «La Feria de la Ciberseguridad»
Ha llegado el momento de demostrar lo que hemos aprendido. El instituto celebra la «Feria de la Ciberseguridad» y vosotros sois los ponentes.

Tarea final (por equipos de 3-4 personas)
Cada equipo debe crear:

1. **Una infografía digital o en cartulina** que responda:
    - ¿Qué son los números primos?
    - ¿Quién fue Sophie Germain?
    - ¿Cómo protegen los primos tu WhatsApp?
    - Un dato curioso (cigarras, gúgol, etc.).
2. **Un cifrado propio** (inventado por el equipo) para enviar un mensaje secreto a otro equipo, que deberá descifrarlo.
3. **Una exposición oral de 3 minutos** en la feria, explicando su trabajo a compañeros de otros cursos.

¡¡Importante!!

Recordad que la evaluación mide vuestro progreso y competencias reales: la copia, el plagio o el uso inapropiado de la IA invalidan vuestro proceso de aprendizaje y se calificarán con «NI» en los criterios correspondientes.