Actividad RSA

Emilio López cano

2/16/2019

Codificar mensaje

Esta actividad se realiza en dos grupos.

1. Elige un par de números p, q, para crear tus claves pública y privada, de entre las siguientes opciones:

- 3 y 13
- 5 y 11
- 5 y 7
- 7 y 11
- 5 y 13

3. Calcula $\varphi(n) = (p-1) \cdot (q-1)$
4. Obtén tu clave pública:

- $n = p \cdot q$
- $e < \varphi(n)$ y sin divisores comunes

3. Obtén tu clave privada:

- d tal que $d \cdot e = 1 \ (mod\, \varphi(x))$. O sea, un número que multiplicado por e y dividido por $\varphi(x)$ dé 1.

4. Publica en la pizarra tu clave pública y anota la del otro grupo.
5. Codifica un mensaje (una o dos palabra máximo) con la clave pública del otro grupo.
6. Comparte el mensaje codificado en la pizarra.

Descodificar mensaje

7. El otro grupo habrá codificado un mensaje para ti que también está en la pizarra. Descodifícalo con tu clave privada.
8. Comprobad que los mensajes descodificados se corresponden con los enviados.

Criptoanálisis y hackeo de la clave

9. Busca una estrategia para averiguar la clave privada del otro grupo.
10. Repetid el ejercicio, pero en este caso un alumno de cada grupo intercepta el mensaje enviado y lo descifra antes que el receptor.

Codificación letras

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