TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 1: Envío de mensajes y cifrado

Desde la antigüedad, cuando se empleaba la escritura para enviar mensajes o almacenar conocimientos existía el problema de la seguridad sobre la información. Es decir, se pretendía responder a la pregunta de ¿Cómo transmitir un mensaje de tal forma que solamente quien lo recibe sea capaz de entenderlo?

Si bien hay ejemplos muy antiguos como el uso de jeroglíficos no estándar por parte de los egipcios, fueron los griegos quienes emplearon técnicas de codificación para asegurar que un mensaje enviado por medio de un mensajero solo pudiera ser interpretado por el destinatario. El principal uso de estas técnicas era militar, ya que garantizaban que órdenes de altos mandos y estrategias, se pudieran comunicar a frentes de batalla sin que un mensajero supiera el contenido, evitando así traiciones o que el enemigo interceptase los mensajes. Fue en la antigua Grecia en donde se inventaron técnicas como el cifrado César que sustituía letras del alfabeto con desplazamientos y la escítala, que fue uno de los primeros dispositivos de cifrado.

Al cifrar los datos, se tenía un mensaje con caracteres legibles, en el lenguaje común a los implicado (griego, por ejemplo) sin embargo, estos caracteres no tenían sentido alguno para el lector convencional.

En el caso de la escítala, se empleaban dos varas del mismo grosor y una cinta de cuero o de papiro. Para transmitir un mensaje, previamente se entregaba tanto al emisor del mensaje como al receptor una de las dos varas del mismo grosor. Cuando se iba a enviar un mensaje, quien escribía debía enrollar el papiro sobre la vara en forma de espiral sin dejar espacios ni solapar la tira. Luego se escribía el mensaje longitudinalmente, en el sentido de la vara, como se ve en la figura 1.

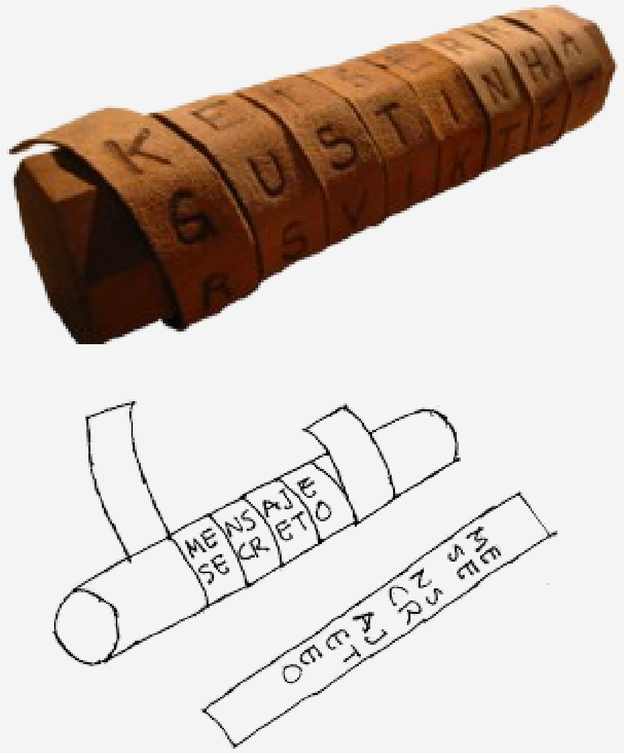

Figura 1: escítala

Al finalizar se desenrollaba la tira y se enviaba al receptor, quien, para decodificar el mensaje, tenía que enrollarla en la vara para recuperar los caracteres en orden y así leer el mensaje.

De forma similar operaba el cifrado césar. Que consistía en rotar las letras del alfabeto una cantidad determinada de posiciones para poder cifrar el contenido. El resultado del cifrado eran caracteres que no parecían tener ningún significado. Sin embargo, quien recibía el mensaje, sabía cuántas posiciones rotar las letras para recuperar el mensaje original.