La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura.

4.2.1. Envia a un compañero un mensaje cifrado con Polybios. El mensaje deberá incluir una pregunta que el compañero deberá contestar. Anota ambos mensajes con y sin cifrado.

AE DC DD DE AD BD CD = estudio

4.2.2. Clasifica todos los métodos de cifrado estudiados en el apartado 4.2, según las categorías que acabamos de espedificar.

- Sistema de transposición: simples y dobles.
- Sistemas de sustitución: literal, numéricas y esteganográficas.

4.9.1. Inventa un método de cifrado simétrico para comunicarte de manera segura con un compañero. Describe sus características.

El algoritmo AES, dicho algoritmo se caracteriza por ser un cifrado simétrico por bloques con longitud de clave variable; la longitud de la clave por defecto es de 128 bits pero también puede establecerse a 192 o 256 bits. El funcionamiento de dicho algoritmo puede separarse en dos partes o procesos diferentes, el primero, sería el proceso de cifrado y el segundo correspondiente al proceso de generación de subclaves. El bloque a cifrar tiene una longitud de 128 bit, mientras que la clave puede variar de 128, 192 o 256 bits, según la cantidad de rondas estándar que se apliquen al texto 10, 12 y 14 respectivamente

4.9.2. Descubre el resultado de cifrar mediante el algoritmo César la siguiente frase: La máquina Enigma fue utilizada por los alemanes utilizando como palabra clave “secreta”.
Descifrado:
jy káosgly clgeky dsc srgjgxyby nmp jmq yjckylcq srgjgxylbm amkm nyjyzpy ajytc “qcapcry”
Utilizando un valor de 128.