**Nil Mató Massaguer**

1. **Què garanteix la privadesa de les dades (data privacy)?**

Garanteix que les dades no puguin ser accedides lliurament. només podran accedir a les dades aquells individus que estiguin autoritzats, és a dir que tinguin la clau per desxifrar-ho.

1. **De quines paraules gregues prové la paraula criptografia i què volen dir?**

Prove de les paraules *kryptos* que significa amagat o secret i *gráphin* que significa escriptura.

1. **En què consisteix el xifrat de dades?**

Consisteix en transformar un conjunt de dades originals (en clar) a un conjunt de dades totalment diferent i incomprensible (xifrades). Amb l’ajut de les eines necessàries és possible desxifrar les dades.

1. **Què és la criptoanàlisi?**

És el conjunt de tècniques utilitzades per a desxifrar codis encriptats sense conèixer el sistema utilitzat par a la codificació.

1. **En què consisteixen els mètodes mono alfabètics? Anomena'n un i explica detalladament en què consisteix.**

Consisteix en que cada caràcter es substitueix sempre per un determinat caràcter del text xifrat.

    Un exemple és el Xifrat de Cèsar el qual consisteix en que cada lletra és substituïda per la tercera lletra següent de l’alfabet. La lletra “A” serà substituïda per la lletra “C” per exemple.

1. **Els mètodes mono alfabètics es basen en la transposició i la substitució, en què consisteix cadascun d'aquests dos mètodes**

    Els mètodes mono alfabètics basats en la transposició consisteixen en un tipus de xifrat en el qual canviem les lletres de posició seguint un esquema definit. Aquest tipus d’algorismes són de clau simètrica ja  que és necessari que tant el que el desxifra com el que el desxifra sàpiguen la clau. Aquesta clau pot ser en el propi missatge xifrat.

    Els mètodes basats en la substitució és un sistema en el qual unitats de text són substituïdes per un text xifrat seguint un sistema regular. Aquestes unitats es poden substituir per una sola lletra, per parelles, per trios o barrejant les opcions. El receptor ha de realitzar el mateix però a inversa. Aquest a diferencia del de transposició el text manté el mateix ordre.

1. **En què consisteixen els mètodes polialfabètics? Anomena'n un i explica detalladament en què consisteix..**

**Es diu que un sistema de xifrat és polialfabètics quan cada caràcter no es substitueix sempre per el mateix caràcter.**

**Un exemple és el xifrat de Alberti consisteix en dos discos concèntrics on el disc de fora al final de l’alfabet conté els números 1,2,3,4. I consisteix en alinear els dígits del disc de fora amb una lletra del disc de dintre i llavors les altres lletres queden codificades.**

****

1. **A quina època es considera que s'inicia la criptografia actual?**

Es va iniciar a la segona meitat dels anys 70 amb la invenció del sistema DES ( Data Encryption Standard ).

1. **Els principals problemes de seguretat que resol la criptografia són: privacitat, autenticitat, integritat i no-repudi. Defineix aquests 4 conceptes.**

Privacitat: La informació no es pot ser llegida per les persones autoritzades o que sàpiguen com desxifrar-ho.

Autenticitat: Es pot confirmar que el missatge rebut ha estat enviat per la persona que esperaves que l’envies.

Integritat: La informació no pot ser alterada durant l’enviament.

no-repudi: No es pot negar el missatge rebut.