Criptografia

Desenvolupat per: Adrià Pons, Nora Jarque

Resum

La criptografia està present en el nostre dia a dia en molts àmbits: en la seguretat d'Internet, al fer transaccions bancàries, etc. Amb aquesta proposta intentarem apropar els alumnes al món de la criptografia, explicant i posant en pràctica alguns dels mètodes històrics més famosos de codificació de missatges.

Nivell

ESO/Batxillerat (per les activitats proposades, potser és més adient per a la ESO)

Contingut

S'introduiran diferents mètodes de codificació, intentant seguir un ordre cronològic.

- Veurem el codi Cèsar i altres mètodes de xifrat que es basen en la substitució de cada lletra per alguna altra lletra o signe, anomenats xifrats monoalfabètics.
- Descobrirem altres mètodes que consisteixen en cobrir el missatge o col·locar-lo en diferents posicions per tal de llegir-lo (com mètodes amb reixetes o l'escítala espartana).
- Comentarem mètodes que utilitzen una paraula clau per tal que una lletra no sempre es transformi en la mateixa, anomenats xifrats polialfabètics.
- Aprendrem altres mètodes com el xifrat de Vernam, que utilitza nombres binaris.
- Finalment, acabarem amb una breu explicació sobre la màquina Enigma i com es va aconseguir desxifrar els codis que produïa. D'aquí arribem a la idea que la criptografia està present a quasi tota la seguretat tecnològica que utilitzem en el nostre dia a dia.

Si hi ha temps, acabarem fent una breu i molt senzilla explicació sobre els missatges xifrats amb clau pública i privada i les signatures digitals.

Proposta d'activitats

- Amb cada mètode vist, donarem un missatge xifrat que els alumnes intentaran desxifrar o demanarem que en codifiquin algun en concret per tal de comprendre el procediment.
- Podem mostrar la implementació amb C++ d'algun procediment explicat anteriorment (com, per exemple, el codi Cèsar o un altre mètode monoalfabètic on els alumnes decideixin l'alfabet de xifrat).
- En relació amb el mètode de Vernam, podem calcular la mitjana de les notes de l'últim examen fet a classe entre tots els alumnes sense que ningú conegui les dades exactes dels altres, per exemple.

Proposta de desenvolupament

Si algun dels alumnes està interessat en fer un anàlisi més profund del tema per un possible treball de recerca, es pot posar en contacte amb nosaltres.