Generalitat de Catalunya Departament d'Educació IES Nicolau Copèrnic	FITXA D'ACTIVITAT CRÈDIT 1	*CODI ESI.C1* *REVISIÓ 0*
	EXPLOTACIÓ DE SISTEMES INFORMÀTICS	*DATA 15/09/2007*

FITXA D'ACTIVITAT: UD1NA4.A1 i UD1NA4.A2 — Duració: 0,5 hores + deures

NOM ACTIVITAT: Exercici de criptoanàlisi

Descripció:

Solucionar un problema de criptoanàlisi. Els alumnes han de desxifrar un text xifrat amb una codificació de substitució de caràcters utilitzant les tècniques simples de criptoanàlisi explicades a classe.

Objectius didàctics:

- Aplicar els processos de criptoanàlisi amb l'objectiu de desxifrar un text codificat.

Organitzadors previs:

- **UD1.NA1:** Elaboració dels apunts al dossier virtual.

Continguts de procediments	Fets, conceptes i sistemes conceptuals	Actituds, valors i normes
0. Identificació de sistemes de comunicacions 0d. Documentació de les activitats realitzades i els resultats obtinguts.	**0*. Conceptes bàsics de telemàtica** 0d. Components d'un sistema de comunicacions (emissors i receptors, equips terminals de dades i equips de comunicacions, canal, soroll i interferències).	**1.** Execució sistemàtica en el procés de resolució de problemes. **3.** Ordre i mètode de treball. **4f.** Cura en l'elaboració de documentació.

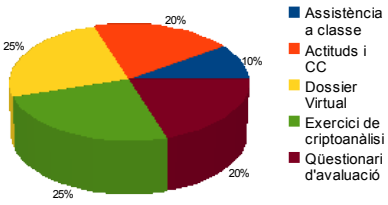
Seqüència d'activitats	Durada	Metodologia	Recursos	Lloc	Formes d'organització
– **NA4.A1** Codificació de la informació. Tipus de codis i funcions. – Explicació teòrica mitjançant transparències dels sistemes de codificació. Xifratge i criptoanàlisi. – **NA4.A2** Desxifrar un text xifrat amb un codi de xifratge de transposició de caràcters. – Explicació de l'exercici. – Desxifrar un text xifrat.	25 min. 5 min. deures	Els alumnes han d'incorporar a l'apartat adequat dels apunts de la unitat didàctica 1 les explicacions sobre codificació, xifratge i criptoanàlisi i desxifrar un text xifrat.	- Dossier Virtual (Mediawiki) - Navegador web Firefox amb corrector ortogràfic. - Base de dades Moodle amb diferents textos xifrats. Els textos són extrets de les explicacions teòriques de la unitat (transparències digitals) - Pàgines web sobre criptoanàlisi i criptografia clàssica.	AO*	Explicacions del professorat (P) més l'elaboració de la gràfica per part de l'estudiant (I)

Criteris d'avaluació:

Què avaluar?	Com avaluar?	Quan avaluar?
- La solució de l'exercici. - La responsabilitat a l'hora d'entregar la tasca a Moodle acuradament i a temps.	Comparant les solucions dels alumnes amb els textos xifrats originals.	En finalitzar les activitats.

Pes especific d'aquesta activitat

L'exercici de criptoanàlisi té un pes d'un **25%** de la nota final de la unitat didàctica 1. Els continguts comptaran com a continguts de procediments tot i que diferents aspectes poden tenir repercussió sobre part de la nota d'actitud.



Bibliografia i enllaços d'interès:

- Textos xifrats
- Base de dades Moodle on posar les solucions
- Cambra Negra. Consells i trucs per desxifrar un text

***Llegenda:**

- **P:** Activitats centrades en el professorat
- **G:** Activitats centrades en el grup-classe
- **g:** Activitats en petit grup
- **I:** Activitats individuals
- **AO:** Aula ordinària (amb un ordinador per alumne/a, connexió a Internet i un projector digital)
- **Lab:** Laboratori de xarxes
- **Tall:** Aula taller