ESCOLA I CRIPTOGRAFIA

223

Síntesi

ESCOLA I CRIPTOGRAFIA és un projecte que pretén apropar a l'alumne a les matemàtiques i a la història des de una de les seves vessants més lúdiques, la criptografia.

L'apassionant món dels codis secrets i els xifrats amaguen tot un variat reguitzell d'algoritmes (funcions, funcions inverses, aritmètica modular…) que són apropats als alumnes de ESO i Batxillerat mitjançant dues xerrades introductòries (CODIS SECRETS; ALAN TURING I LA MÀQUINA ENIGMA*) i un taller on poden practicar el criptoanàlisi de diversos sistemes criptogràfics (xifrat del Cèsar, xifrat de Polibi, discs monoalfabètics I polialfabètics, xifrat de Gilbert Vernam, xifrat Pigpen…)

Un dels punts qualitatius d'aquest projecte és poder apropar un **exemplar original de màquina ENIGMA** als alumnes tot fen una demostració del seu funcionament.

**Aquestes xerrades són creació del matemàtic Dr.James Grime (Universitat de Cambridge), i han estat adaptades al català i castellà amb el seu permís.*

Descripció

ESCOLA I CRIPTOGRAFIA és una iniciativa d'Oscar Font, dissenyador gràfic, músic de jazz a l'orquestra LA LOCOMOTORA NEGRA i gran aficionat a la criptografia.

…*"Sempre ha estat interessat en la Segona Guerra Mundial i en especial la Batalla de l'Atlàntic, on centenars de vaixells mercants van ser enfonsats pels nombrosos submarins alemanys que vigilaven aquelles aigües. Les comunicacions d'aquests U-Boot amb l'alt comandament alemany i fins i tot entre ells mateixos es realitzaven mitjançant codi Morse. Ara bé, els missatges que s'enviaven havien estat prèviament xifrats amb la màquina ENIGMA…"*

El col·leccionisme d'estris criptogràfics i el contacte permanent amb col·leccionistes d'arreu del món va donar fruits el dia que li va sorgir la possibilitat d'adquirir una màquina ENIGMA original.

L'any 2011 va començar a fer classes de criptografia a escoles i instituts. Actualment, gràcies a l'experiència adquirida i a la recent incorporació de la màquina ENIGMA, aquelles primeres classes han esdevingut un viatge apassionant per la història de la criptografia.

El projecte està format per xerrades i tallers:

XERRADES:
ALAN TURING I LA MÀQUINA ENIGMA
ACTIVITAT APROPIADA PER ALUMNES DE 4t d'ESO I BATXILLERAT
Un apropament a la vida d'aquest gran matemàtic, tot fent un paral·lelisme amb el desenvolupament de la màquina ENIGMA, que precísament en Turing va contribuïr a desxifrar.

La cloenda de la xerrada és **una demostració del funcionament d'una màquina ENIGMA original**, el mateix model utilitzat per la Wehrmacht durant la Segona Guerra Mundial.

**És molt recomanable que els alumnes hagin vist la pel·lícula IMITATION GAME abans de l'activitat.*

Oscar Font
Trombó i clarinet a LA LOCOMOTORA NEGRA
escolaicriptografia@gmail.com
http://escolaicriptografia.weebly.com
@Enigmatitis

Nivell: ESO, Batxillerat
Aspectes que es treballen: Comprensió del fet criptogràfic lligat a les matemàtiques
Material: Paper i llapis

CODIS SECRETS

ACTIVITAT APROPIADA PER ALUMNES d'ESO I BATXILLERAT

Xerrada sobre els mètodes clàssics de criptografia i les matemàtiques dels codis. Un viatge per la història dels missatges secrets des de l'antiga Grècia fins a la Segona Guerra Mundial.

És perfecte com a activitat complementària a les assignatures de matemàtiques, ciències o història. També és molt recomanable com a complement de cursos d'estiu, seminaris i tallers.

La cloenda de la xerrada és **una demostració del funcionament d'una màquina ENIGMA original**, el mateix model utilitzat per la Wehrmacht durant la Segona Guerra Mundial.

TALLER:

TALLER DE CRIPTOGRAFÍA

ACTIVITAT APROPIADA PER ALUMNES DE 3r, 4t d'ESO I BATXILLERAT

El Taller s'inicia amb una breu explicació del que ha estat la criptografia a lo llarg dels segles. A continuació es proposen uns exercicis de xifrat i desxifrat perquè els alumnes (per grups) es familiaritzin amb els principis fonamentals de la criptografia. Per dur a terme aquests exercicis es repartiran elements d'us comú entre criptògrafs.

Les explicacions i els exercicis pràctics volen familiaritzar als alumnes amb els conceptes:

CLAU
XIFRAR / DESXIFRAR
CODIFICAR / DESCODIFICAR
CODI DE SUBSTITUCIÓ
CODI DE TRANSPOSICIÓ
CRIPTOGRAFÍA SIMÈTRICA
CRIPTOGRAFÍA ASIMÈTRICA

Per aconsseguir aquestes fites, durant els exercicis pràctics hauran de fer anar els mecanismes pròpis de codificació i descodificació clàssica, és a dir, els ALGORITMES oportuns per a cada cas.

Tot i la senzillesa de la propsta, resulta interessant veure com fins i tot molts dels alumnes amb més reticències a les matemàtiques, s'interèssen per aquesta vessant amb components d'història, intriga i misteri.

La durada del taller és de 50 minuts
El TALLER DE CRIPTOGRAFÍA és una prolongació natural i complementaria de la xerrada CODIS SECRETS

OSCAR FONT
607932063
http://escolaicriptografia.weebly.com