Generalitat de Catalunya
Departament d'Educació

M9-PSP: ACTIVITAT 1

UF1. SEGURETAT I CRIPTOGRAFIA

CFGS DESENVOLUPAMENT D'APLICACIONS MULTIPLATAFORMA

Institut Eugeni d'Ors
Vilafranca del Penedès

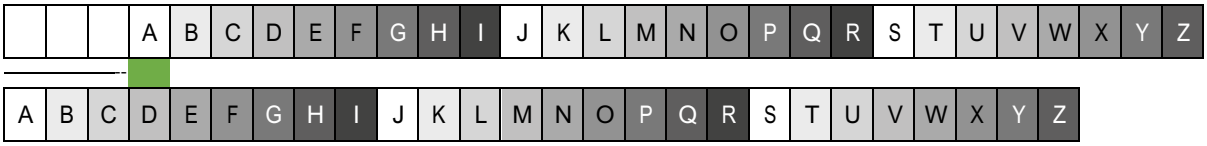
ÍNDEX

OBJECTIU GENERAL DE L'ACTIVITAT

Introduir la teoria del xifratge simètric amb un exemple bàsic de tècnica de xifratge.

EL XIFRAT CÈSAR

El xifrat César, també conegut com xifrat per desplaçament, codi de César, desplaçament de César o decalatge de Cèsar, és una de les tècniques de xifratge més simples i que més s'ha utilitzat al llarg de la història. Es tracta d'una mena de xifratge per substitució en el qual cada lletra del text original és reemplaçada per una altra lletra que es troba avançada un nombre fix de posicions en l'alfabet. Per exemple, amb un desplaçament de 3, la lletra A seria substituïda per la lletra D, la lletra B seria reemplaçada per la lletra E, etc. Aquest mètode de codificació deu el seu nom a Juli Cèsar, qui l'usava per a comunicar-se amb els seus generals.



El xifratge César desplaça cada lletra un determinat nombre d'espais en l'alfabet. En aquest exemple s'utilitza un desplaçament de tres espais (***shift hey***), de manera que una lletra A en el text original es converteix en una lletra D en el text codificat.

En moltes ocasions el xifratge César forma part de sistemes més complexos de codificació, com el ***xifratge Vigenère*** o, fins i tot, el sistema ROT13. Com tots els xifratges de substitució alfabètica simple, el xifratge César es desxifra amb facilitat, per la qual cosa, en la pràctica no protegeix les comunicacions amb massa seguretat.

Des del punt de vista matemàtic, el xifratge César pot ser modelitzat mitjançant una operació de suma en aritmètica modular 26 (si l'alfabet utilitzat té 26 lletres). Així, cada lletra de l'alfabet llatí (de la A fins la Z) queda identificada per un enter de 0 a 25. El text pla es codifica introduint el desplaçament de tres posicions, és a dir, sumant el valor de la clau (en aquest cas, 3). En conseqüència:

```
<lletra xifrada> = (<lletra clara> + clau) mod26
<lletra clara> = (<lletra xifrada> - clau) mod26
```

LLETRA	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CODI	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

CODI D'HONOR

L'ús de la IA ha de ser una eina d'aprenentatge i millora personal, no una forma de trampa que minvi el teu progrés, comprensió dels conceptes i capacitat d'assolir reptes més complexos.

1. **Autenticitat en l'Aprenentatge**: Utilitza la intel·ligència artificial per entendre els problemes i desenvolupar les teves habilitats, no per evadir els reptes d'aprenentatge.
2. **Col·laboració Ètica**: Col·labora amb altres estudiants de manera ètica i transparent. Ajuda'ls a comprendre i superar els obstacles, però no els donis solucions completes si això compromet la seva pròpia comprensió.
3. **Reconeixement dels Recursos**: Si utilitzes codi, solucions o materials d'altres fonts, assegura't de reconèixer i citar adequadament aquests recursos. L'honestedat intel·lectual és fonamental.
4. **Responsabilitat Personal**: La responsabilitat del teu aprenentatge i èxit recau en tu mateix. Utilitza les eines d'intel·ligència artificial com a suport, no com a substitut de l'esforç.

ACTIVITATS

1. Codifica i descodifica el següent missatge utilitzant una clau de desplaçament de valor 7

   Text original: La sort està tirada

   Text xifrat:

2. Utilitzant Java com llenguatge base, codifica un programa que permeti xifrar i desxifrar una paraula utilitzant el xifratge Cèsar. El programa ha de mostrar la següent sortida:

```
Introdueix una paraula per xifrar: Papallona

Introdueix el desplaçament: 3

El missatge xifrat és: sdsdoorqd

Vols desxifrar el missatge? (s/n): s

El missatge desxifrat és: papallona

Programa finalitzat
```

3. Afegeix al codi anterior una nova utilitat que permeti llegir un conjunt de paraules separades per <ENTER> emmagatzemades en un fitxer de text i que generi un nou fitxer amb totes les paraules encriptades.