# Sistemes Operatius
# Lab 4 – Atacant el Capitol

**Enigma 3**

(LAB 4) GoldKey

La resistència ha interceptat un missatge encriptat a partir d'un xifratge AES (Advance Encryption Standard) amb mode cbc, Initialization Vector (iv.txt) i la seva clau de desencriptació (clue.txt), enviat pel capitol a la seva seu de TimeControl. Se sospita que el missatge conté el nom de l'agent encarregat d'eliminar la resistència (solució de l'enigma). Per tal de saber quin es el mètode de desencriptació a utilitzar, la resistència fa servir un AI (més Artificial que Intel·ligent) coneguda.
Nota: Guia a l'AI cap a una solució de comandes en linux

*Objectius d'aquesta sessió*

- *Utilitzar codi extern*
- *Implementació d'un model client / servidor*
- *Connexió de processos remots*

la resistència ens ha proporcionat el dummy4, que substituirà a l'anterior, i les indicacions que ens permetran accedir al Capitol. Hem d'adaptar aquest dummy4 al nostre TT per a que pugui atacar el banc de temps.
En aquesta sessió cada equip podrà atacar de forma individual a un Capitol remot i provar els seus replicants (mireu el fitxer README.txt).

## 1. Capitol

Per seguretat, la resistència no ens proporcionarà les dades de configuració finals per accedir al Capitol fins al mateix dia de la competició. Ara ens proporciona unes dades temporals que ens permetran accedit a una replica del Capitol que es troba en remot, molt a prop del Capitol real.

## 2. Time Thief

El TT ha de crear els replicants i esperar que acabin d'atacar el banc de temps que es troba al Capitol. Evidentment, els replicants han de tenir accés a aquest canal remot.
Tal i com ja hem fet, a mida que els replicants vagin finalitzant la seva missió, el TT ha de recuperar el codi de finalització de cadascú (valor entre 0 i 127) i l'acumularà amb la resta de codis dels altres replicants. Aquest valor serà entregat al Capitol a través d'un canal

de control per saber si el processament s'ha realitzat correctament. En cas que qualsevol dels replicants no hagi pogut completar la seva missió amb èxit, el TT avortarà la missió d'atac i enviarà un missatge informatiu.

En tot moment hem d'aprofitar el dummy4, proporcionat per la resistència, que ens facilitarà les diferents tasques a desenvolupar.
El codi del TT ha de contenir els següents valors:

```
#define TEAMNAME "" // insert between "" your team name
#define ENIGMA3 ""// insert between "" solution of enigna 3
#define SILVERKEY ""  // insert SILVERKEY between ""
#define GOLDKEY "" // use only for SIOP Challenge : insert GOLDKEY between ""
```

a) Identifica l'enunciat amb els continguts de l'assignatura
b) Realitza un pseudocodi que expliqui clarament, en termes de l'assignatura, com es prepara el TT per l'atac al banc de temps.
c) Modifica el TT amb les noves accions.

**3. Replicants**

Adapteu (si cal) el replicant per a que funcioni correctament (ara no ataca directament a un banc de temps a traves d'un canal de comunicació local sinó que ho fa remotament degut a que el Capitol es troba físicament a un altre lloc)

a) Identifica l'enunciat amb els continguts de l'assignatura
b) Realitza un pseudocodi que expliqui clarament, en termes de l'assignatura, com es prepara el replicant per l'atac al banc de temps.
c) Modifica el replicant amb les noves accions.