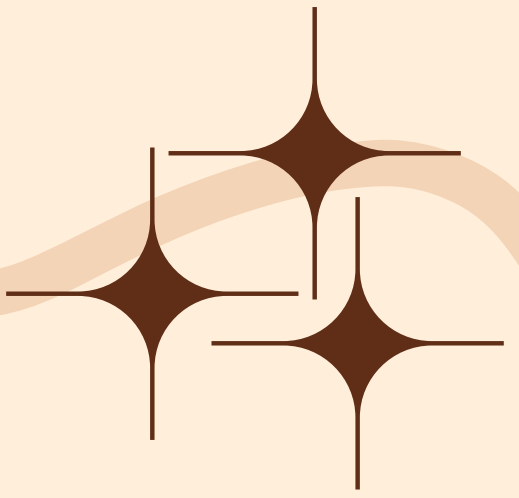





CRYPTO ENGINEERING

CIPHER GAME PRO MAX



113550021 陳孟楷 113550058 蔡昀呈
113550155 胡睿剛 113550158 王金平



OVERVIEW

- 功能介紹
- DEMO
- 架構介紹
- 安全性相關

FUNCTIONS

DISK

- 註冊、登入帳號
- 設定兩階段驗證
- 上傳、下載、刪除檔案
- 多人共用檔案

KMS

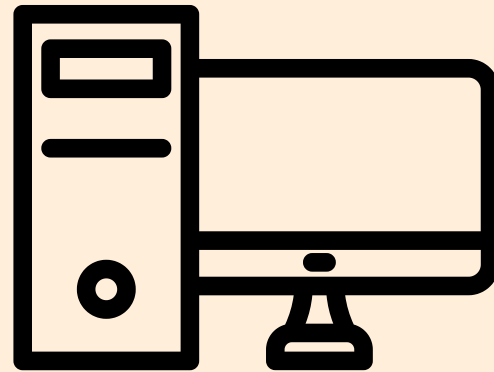
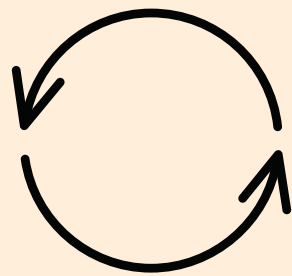
- 分發證書
- 以證書驗證使用者身分
- 防重放攻擊



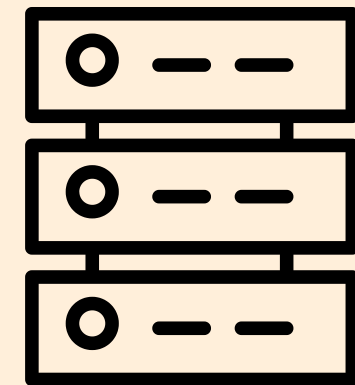
DEMO

STRUCTURE - DRIVE

ENCRYPTED/
DECRYPTED DATA



GET KEY



KMS SERVER

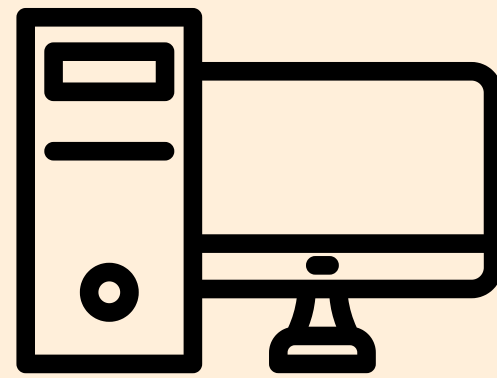
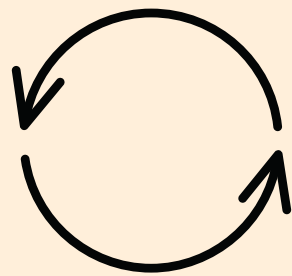
SAVE/GET DATA



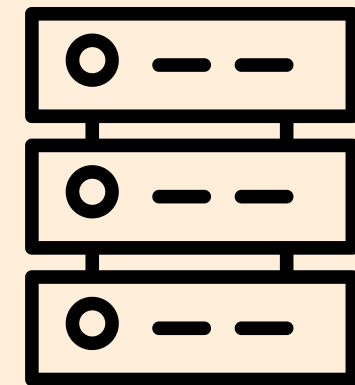
DISK SERVER

FUNCTION - UPLOAD FILE

2. AES → DATA
PK → AES



1. GET PK, PID



KMS SERVER

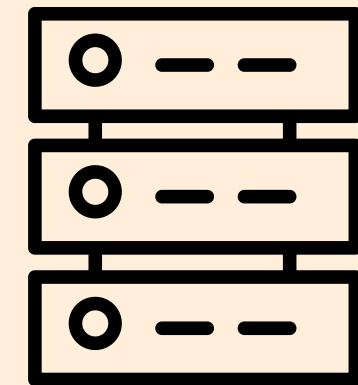
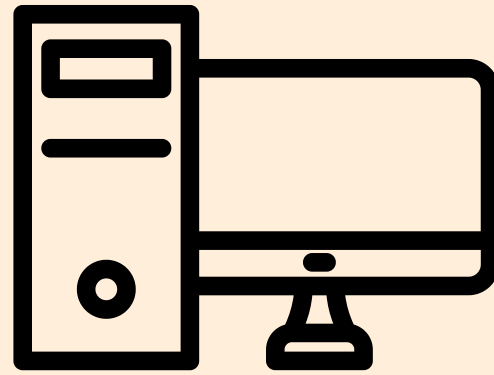
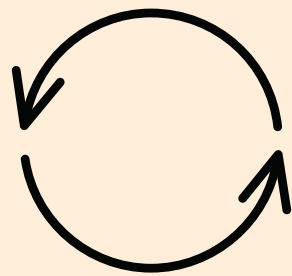
3. SAVE DATA



DISK SERVER

FUNCTION - DOWNLOAD FILE

3. SK → KEY
KEY → DATA

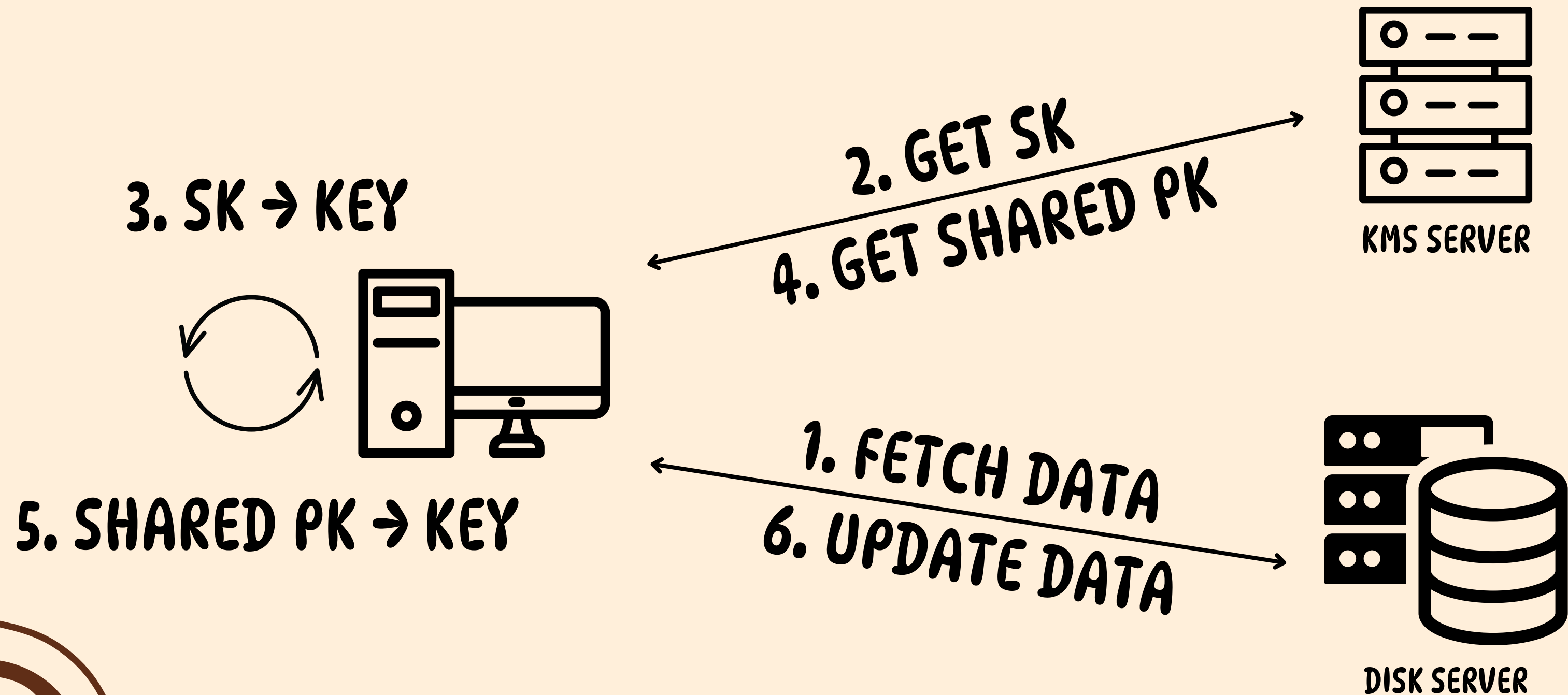


KMS SERVER



DISK SERVER

FUNCTION - SHARE FILE



SECURITY - REPLAY PROTECTION

證書申請

- 新證書：已存在使用者申請新證書時，需要附帶舊的證書以及新的公鑰
- 證書重發：相同密鑰的證書重發有五分鐘的冷卻時間，加上伺服器過濾五分鐘前的所有封包

SECURITY - REPLAY PROTECTION

證書認證

- 紀錄每個使用者的證書流水號，每次來存取金鑰時，都會發一張新的證書
- 只有封包中證書的流水號與當前使用者紀錄的流水號相同時，才視為有效的證書

Thanks ♡

