

Cryptography Engineering

Final Project

Cipher Game Plus 第二組 那不然就隨便取？

112550031 陳炤宇
112550044 吳宇藤
112550074 彭博脩
112550171 賴承浩
112550190 劉彥廷

Outline

- 動機與背景
- 問題目標與實作成果
- Demo
- Q&A

動機與背景

動機與背景:

1. 近期臺灣傳出醫療機構等關鍵單位遭駭客入侵勒索，進而突顯資料保護與內部傳輸安全的重要性。
2. 現行的雲端服務中，用戶無法完全掌握加密金鑰，因此仍存在雲端服務公司私自解密資料的可能性。

因此我們從Quiz 2延伸發想，希望設計一套機制，確保資訊與檔案的傳輸維持高度的安全性，實現如Google CSE的原理，避免金鑰暴露於伺服器或第三方平台。

問題目標與實作成果

目標：

可以登入、上傳檔案並在前端加密、後臺無法查看明文、下載後會被解密成明文的工具。

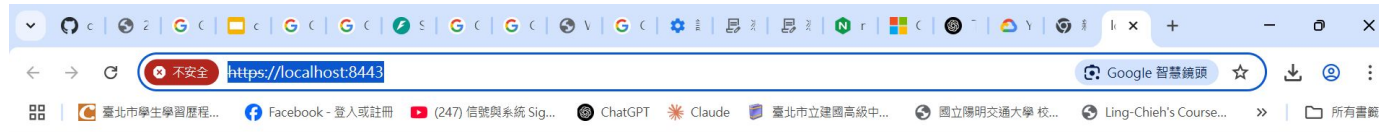
成果：

1. 用2FA註冊登入，來進去網站
2. 上傳檔案後，先經前端加密，送入後端加密密鑰，並將加密後的密鑰和檔案一起上傳到cloud
3. 下載後，用戶可看到解密後的明文

架構：

1. 建立CA, 簽發server與client, 並把client加入瀏覽器內
2. 選取憑證
3. 註冊並且登入
4. 2FA
5. 上傳與下載檔案, 也可以刪除

Demo - PKI(CA):沒有憑證



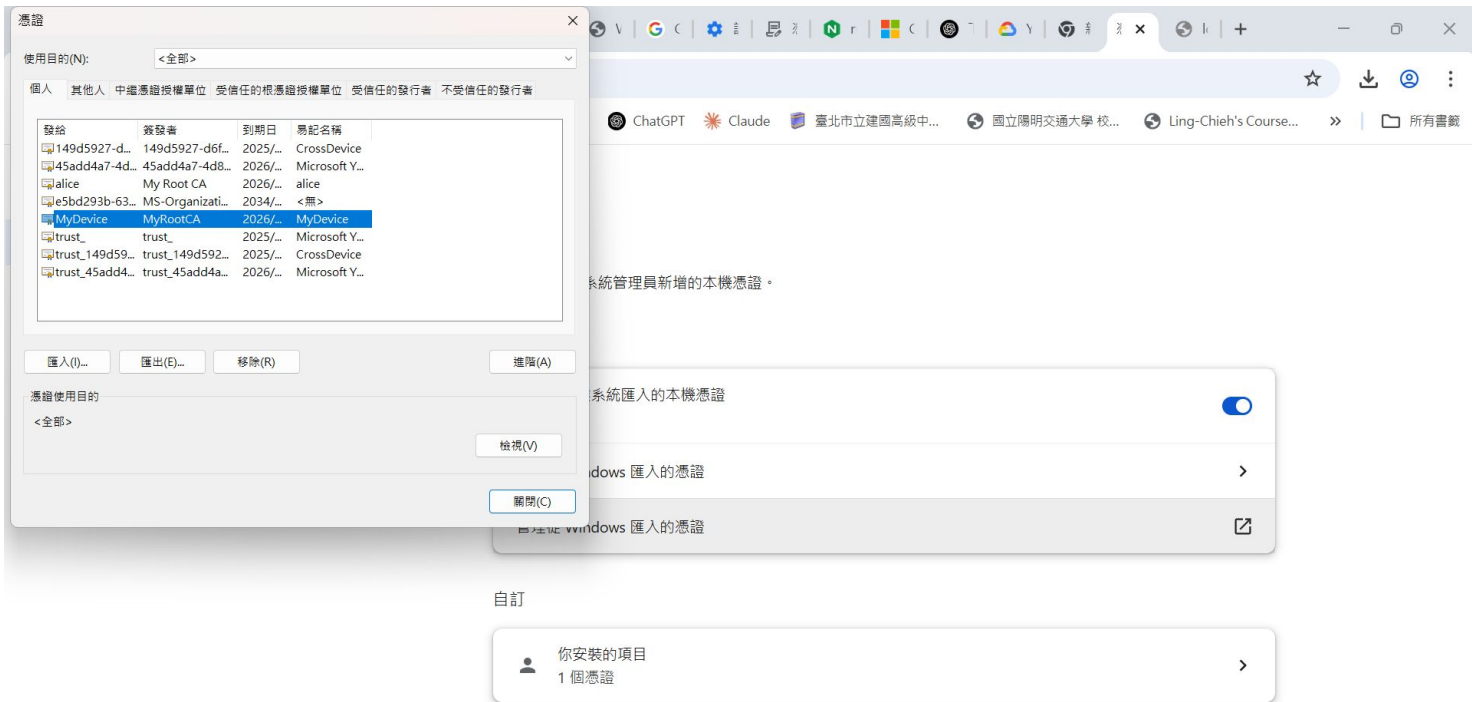
存取 **localhost** 的要求遭到拒絕

localhost 不接受你的登入憑證，或是你可能未提供登入憑證。

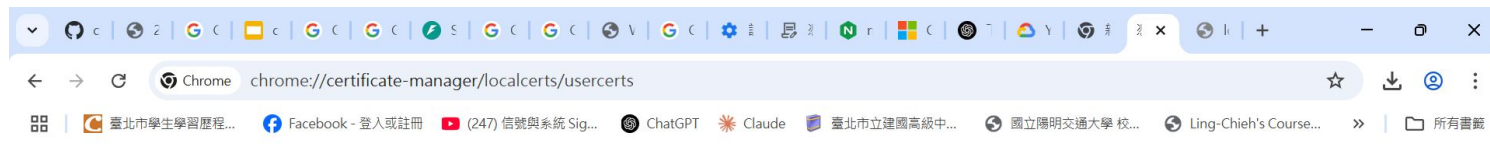
建議您與系統管理員聯絡。

ERR_BAD_SSL_CLIENT_AUTH_CERT

Demo - PKI(CA):匯入憑證



Demo - PKI(CA)



憑證管理員

本機憑證

您的憑證

Chrome Root Store

你安裝的項目

信任的憑證

匯入

匯出

MyRootCA

c6a8ee5c44ed5913a5920e4c46861d90...

中繼憑證

匯入

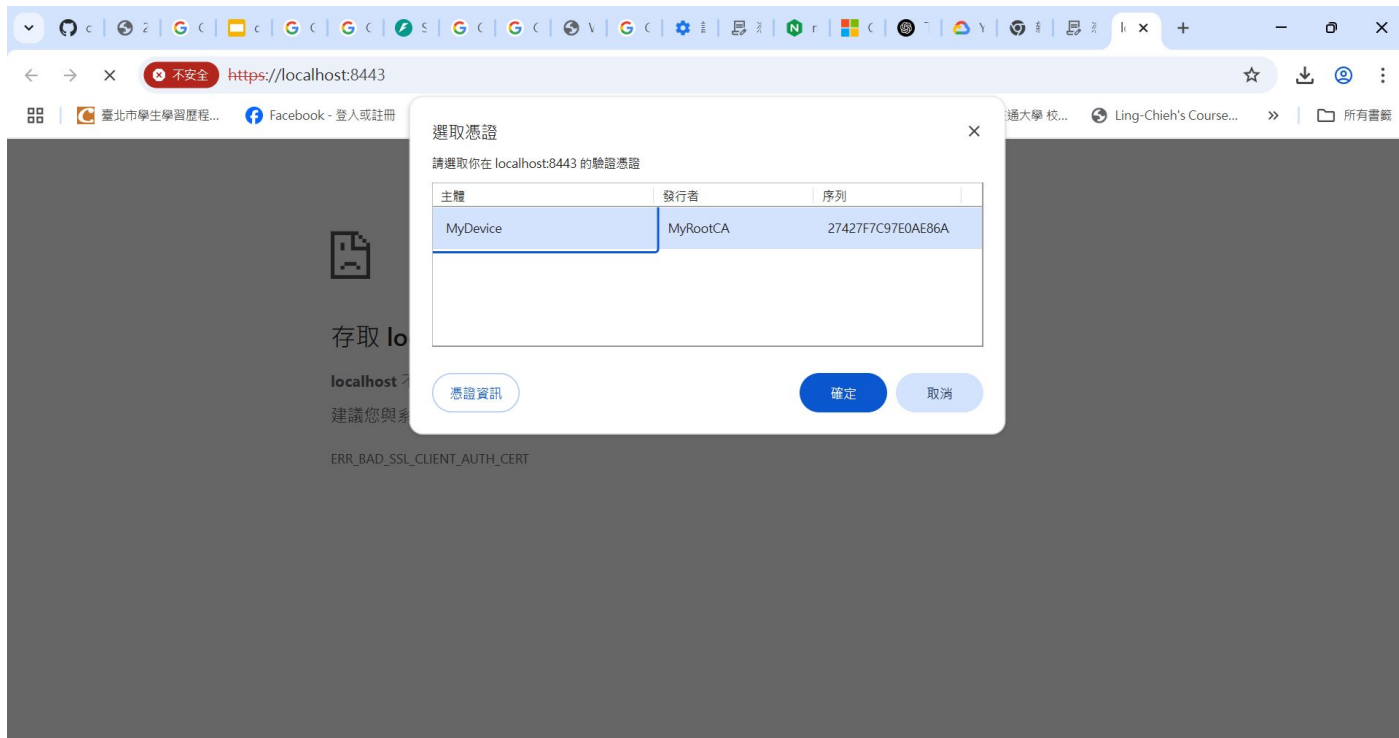
沒有憑證

不受信任的憑證

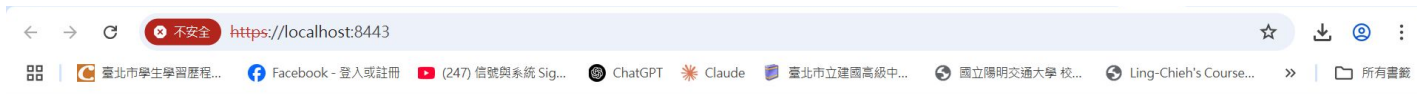
匯入

沒有憑證

Demo - PKI(CA):選取正確憑證



Demo - PKI(CA):驗證成功



您好，MyDevice

憑證驗證成功！

前往下一步

Demo - 註冊



安全檔案上傳 Demo (mTLS)

使用者 ID :

開始註冊

Demo - 註冊成功並開啟2FA



安全檔案上傳 Demo (mTLS)

使用者 ID :

User1

開始註冊



6位密碼

驗證

請掃描 QR code 並輸入 6 位數密碼

Demo - 成功登入2FA開啟檔案上傳下載功能



安全檔案上傳 Demo (mTLS)

使用者 ID :

User1

開始註冊



741688

驗證

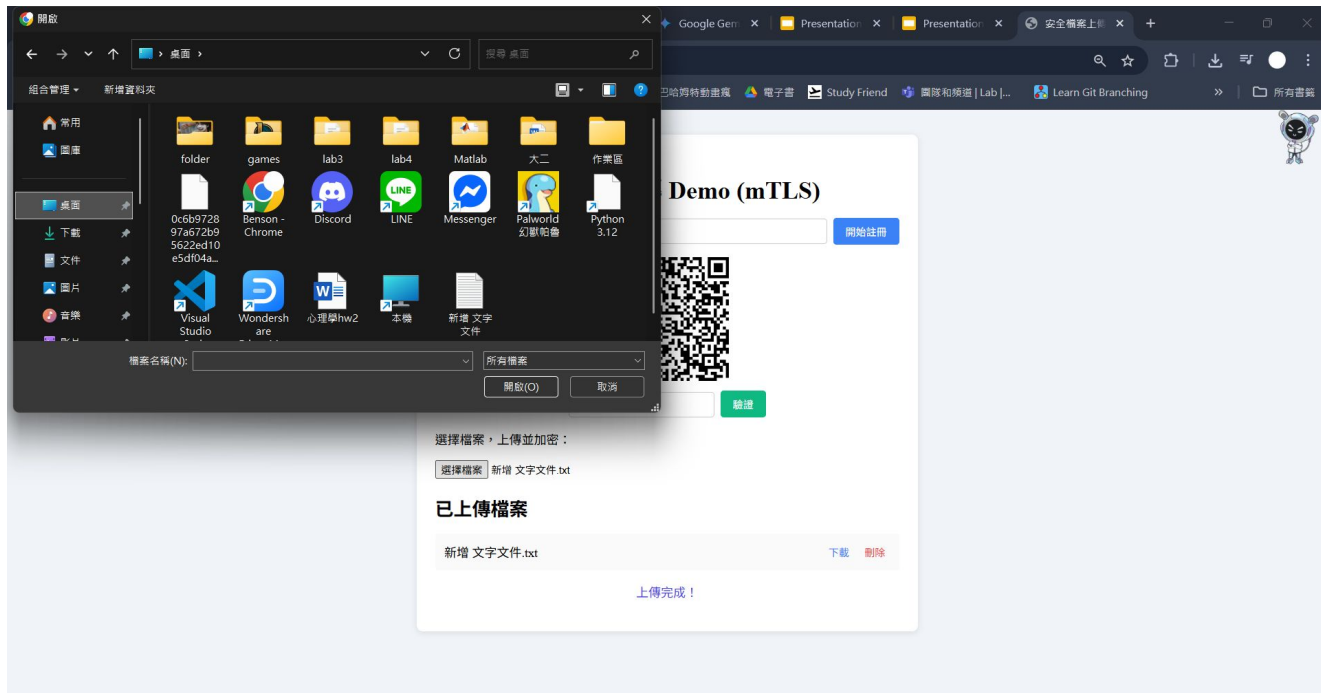
選擇檔案，上傳並加密：

選擇檔案

未選擇任何檔案

TOTP 驗證成功！

Demo - 選擇要上傳的檔案



Demo - 顯示上傳成功的檔案

安全檔案上傳 Demo (mTLS)

使用者 ID :

User1

開始註冊



741688

驗證

選擇檔案，上傳並加密：

選擇檔案

新增 文字文件.txt

已上傳檔案

新增 文字文件.txt

下載 刪除

上傳完成！

Demo - 刪除

安全檔案上傳 Demo (mTLS)

使用者 ID : [開始註冊](#)



[驗證](#)

選擇檔案，上傳並加密：

[選擇檔案](#) [新增 文字文件.txt](#)

上傳完成！

安全檔案上傳 Demo (mTLS)

使用者 ID : [開始註冊](#)



[驗證](#)

選擇檔案，上傳並加密：

[選擇檔案](#) [新增 文字文件.txt](#)

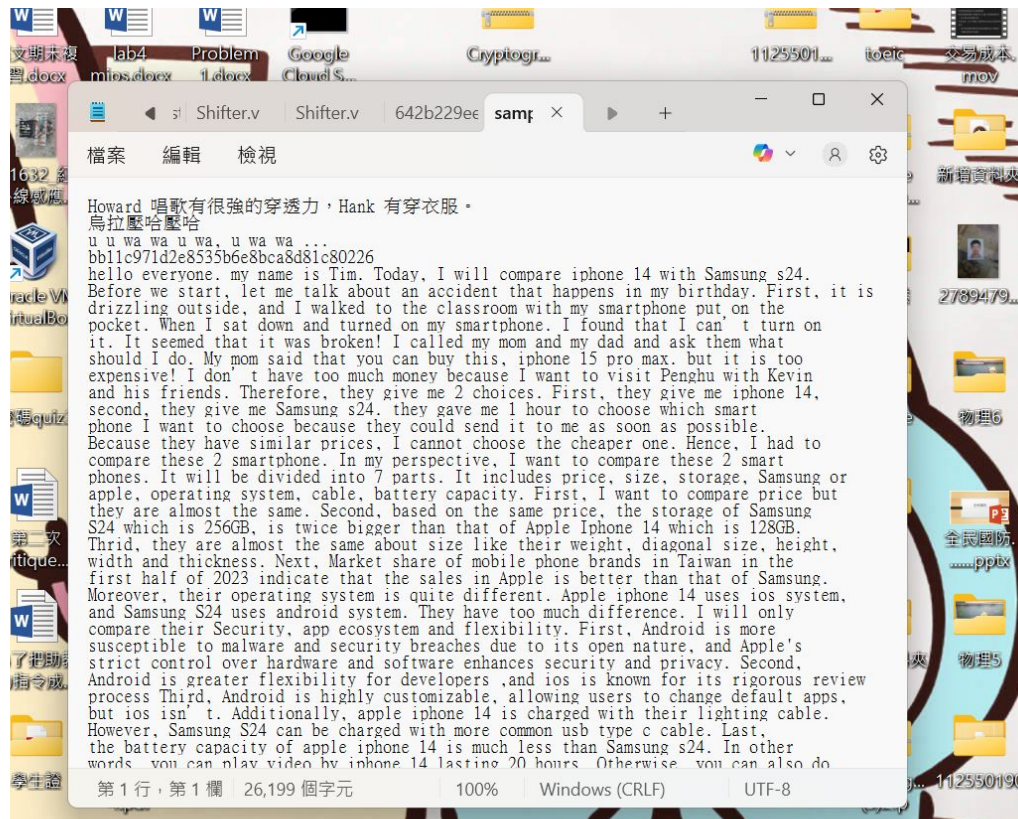
已上傳檔案

新增 文字文件.txt

[下載](#) [刪除](#)

上傳完成！

Demo - 下載:原檔



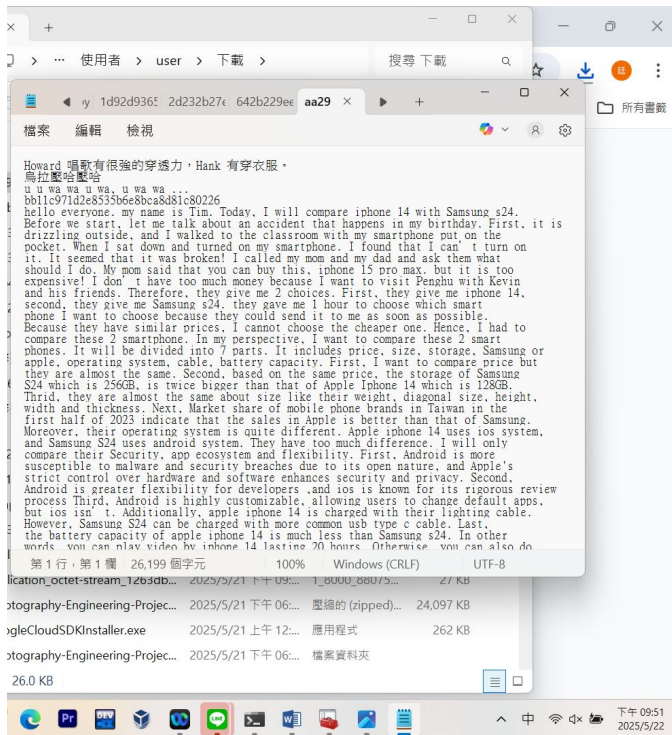
Demo - 下載:載下來的檔案

近期下載記錄



aa2931c3c88d473f1e0fbcfed077774e

26.1 KB • 20 分鐘前



Demo - KMS

使用AES-GCM加密檔案

```
17  async function encryptAndUpload(file, userId) {
18      const aesKey = await crypto.subtle.generateKey(
19          { name: "AES-GCM", length: 256 },
20          true,
21          ["encrypt"]
22      );
23      const iv = crypto.getRandomValues(new Uint8Array(12));
24      const ciphertext = await crypto.subtle.encrypt(
25          { name: "AES-GCM", iv },
26          aesKey,
27          await file.arrayBuffer()
28      );
```

Demo - KMS

匯出AES key

```
29     const rawKey = new Uint8Array(  
30         await crypto.subtle.exportKey("raw", aesKey)  
31     );
```

Demo - KMS

從google cloud取得RSA公鑰


```
33 const { pem } = await fetch(`${API}/kms/public-key`, { credentials: 'include' })
34   .then(r => { if (!r.ok) throw new Error("讀取公鑰失敗"); return r.json(); });
35 const b64 = pem.split("\n").filter(l => l && !l.startsWith("-----")).join("");
36 const der = Uint8Array.from(atob(b64), c => c.charCodeAt(0)).buffer;
37
38 const rsaKey = await crypto.subtle.importKey(
39   "spki",
40   der,
41   { name: "RSA-OAEP", hash: "SHA-256" },
42   false,
43   ["encrypt"]
44 );
```

Demo - KMS

使用RSA公鑰加密AES金鑰

```
45     const encryptedDEK = new Uint8Array(  
46         await crypto.subtle.encrypt(  
47             { name: "RSA-OAEP" },  
48             rsaKey,  
49             rawKey  
50         )  
51     );
```


Demo - 後台情形


 Google Cloud

My crypto Project

Search (/) for resources, docs, products, and more


Search



 Welcome, 劉廷


You've activated your **full account**


Use any remaining credits, then pay as you go.




\$3 out of \$9,741 credits used

Expires August 19, 2025

You're working on project [My crypto Project](#) 

Number: 390472387796  ID: quantum-boulder-460412-q3




[Add people to your project](#)

[Set up budget alerts](#)

[Review product spend](#)

[See all credit usage](#)

Try Gemini 2.0 Flash

Try Gemini 

Demo - 後台情形

←

→

↺

console.cloud.google.com/storage/browser/my-secure-files-bucket;tab=objects?forceOnBucketsSortingFiltering=true&inv=1&inv=AbyF...

🔍

☆

📄

🔴

⋮

🗄️

📄 臺北市學生學習歷程...

📘 Facebook - 登入或註冊

📺 (247) 信號與系統 Sig...

🗣️ ChatGPT

🔥 Claude

📄 臺北市立建國高級中...

📍 國立陽明交通大學 校...

🌐 Ling-Chieh's Course...

»

📁 所有書籤

☰

Google Cloud

🔗 My crypto Project

🔍 Search (/) for resources, docs, products, and more

🔍 Search

🌟

📄

2

?

⋮

🔴 延

☰

Cloud Storage

📌

←

Bucket details

🔗 Go to path

🔄 Refresh

🗄️ Overview

📁 Buckets

📈 Monitoring

⚙️ Settings

Storage Intelligence

🗄️ Insights datasets

⚙️ Configuration

🛒 Marketplace

📄 Release Notes

📁 Overview

📁 Buckets

📈 Monitoring

⚙️ Settings

Storage Intelligence

🗄️ Insights datasets

⚙️ Configuration

🛒 Marketplace

📄 Release Notes

📁 Objects

🔧 Configuration

👤 Permissions

🛡️ Protection

🕒 Lifecycle

📊 Observability

New

📋 Inventory Reports

⚙️ Operations

📁 Folder browser

📁 my-secure-files-bucket

Buckets > my-secure-files-bucket

Create folder Upload Transfer data Other services

Filter by name prefix only Filter Filter objects and folders Show Live objects only

<input type="checkbox"/>	Name	Size	Type	Created	
<input type="checkbox"/>	642b229ee26fe323482c4e25fa6a...	26.7 KB	text/plain	May 22, 2024	📄 ⋮
<input type="checkbox"/>	642b229ee26fe323482c4e25fa6a...	40 B	text/plain	May 22, 2024	📄 ⋮
<input type="checkbox"/>	aa2931c3c88d473f1e0fbcfed077...	26.7 KB	text/plain	May 22, 2024	📄 ⋮
<input type="checkbox"/>	aa2931c3c88d473f1e0fbcfed077...	40 B	text/plain	May 22, 2024	📄 ⋮
<input type="checkbox"/>	c5b206a25573d9ab5c997428f61...	26.7 KB	text/plain	May 21, 2024	📄 ⋮
<input type="checkbox"/>	c5b206a25573d9ab5c997428f61...	40 B	text/plain	May 21, 2024	📄 ⋮

Demo - 後台情形(.bin)

```
l|??j"韓梅稟s竣0?gu 銛k □5?? 輻□□@?瞬P麼N` □??`.表 ? My&f? e?k +-+菰u □?# ??XZG?
想n?7p?機卡 □i□kdufq□銡k?□□饨暖j(2M?
u□ .纖:p? P? □ 鉛□ V 扁=□誦5o9:N+CWx? □剉蠟庖Vz鐳??說 e "? ? 軀?&□
□R4驛□ 1? 讀 4? 咖E□m?m?少?y?斯k 迂|熾J?□4 q? 瑄鷄S(i?0f□3□: ?穰+m3!善?曾N
??H ?|AK 1*朝賊m?p□? 屹n?壤?齏?o\標?
=?捲? i?□懸N□ 盧?U爛p鳴 ?p嚙? J?颯??
□u
淺YEx??~py 鄭?櫟葦陝 4□??R譏啄XiH ? ?□? N莖<未%0??3,?G背□ □ 艘□1調^?BF?□□h?
□z□膝裂? \胸秘□ZZq 蟻齏□S>??□停/:?穎+□室 斫l+AW?5 )?8誦?曠e?R?? ? zi??(鯉 ?H???疆
□?` cz□唱X□???僑矯 ?n 嶺| ?m
?裏.□lu ?
□T鵬qAlg?= 殢 ? ?SI-□8?□ 8 ??? h?□睽? 廊 ?&
廊伉俦 $
氏格 z霍>?鄆?征耿??xE?=?缺M?苗S孳□□□嗉稿m稊詢0 g Z豎 |<□R?~?爻?6^鋤趁?:w? ?廬 ?
[f?淮, ? 8? Fzt f?c' ?$d距闊?:?v) 遯>Z鯨
□M 霄?1 ?
□w趨|苑 %??i 綬? ■ 掩□□?□Ak鐔□?9?'o?B 荷 ???2□P肝 H摠□袒 玆?□
?i□ 缺□o??嬌□??&&:
腊? □~@□?擣挂 /囑??? CUW i?7□ u?
"?合? :>ir??蹠□E象 .□??捷@.B@c|)?□??塌o?/ 杜eb?軔? ? 3□zN` }囑□怒?□? ?F ? 欽??沂
?□軔??捺??#豈囀9青3?"f- ?次??叢? ?x ? □?H豨?? /1 ?勉氣 k'碧b?紉?:8m | i 8俄 ?孳
r2 □f?杓 薏&倍?1 Eet?

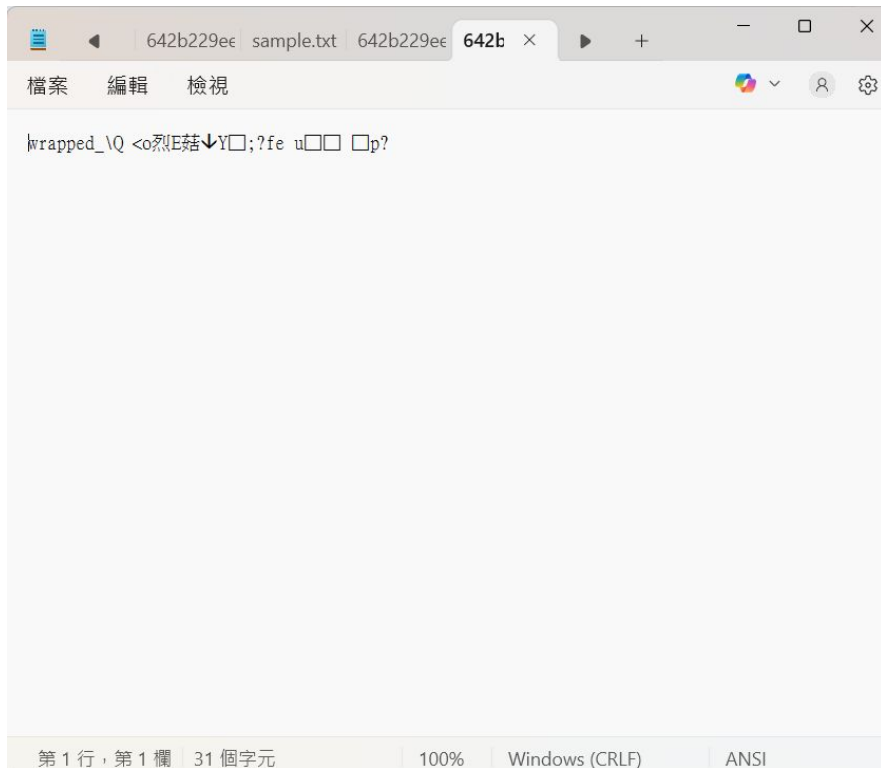
a援F?
LX□?桉+A1?s'??B份E饒lg 傳j□{l? 鏽翊=)? □%W□MD@?□ 如?-□8??{ #Zx□??q - 5D c?榘俞
□>?CS?W `SZ|1?搥 賊友□??dp豈駢???( 遍)@D□WY:舢 F □□立 ?輒□時綜?O-V絞証遐$$.□E?
B?V ㄣz? ?嫻?6(姬x,渠□?乖?喃g諸| ?尾 贊%諺b裕-b8□'?薏r劊□)□?□(功w)NK?□踞詒
攀揉.
?□U\?□□c ?? C ??? □?杯罇@ Y ? 俚?/-檣O? □呼v uo□□? s鶉 咀f培?筌 0??能□$??bZf
謬??f椅~i?10$? .□演誦 ??洽搗Ll 鍾□(q|?? ?? ? o(??桃幻攢e$□\閨3@Q ? 租Tv讀b膝
"註v祝靚. 7腕鈔鈞□iow?$?k? ??番2□?1綺I ?W狙韃O格/1 ? .?ts#K沅杓 □?+??-w? ?鮓
j???'XvⅢ??物?kg?□?維?0鰭O□ 煥E@?鮮 0□昌賴彈?□抱=啖"?G□ 0?E I 颯6
Y□Tz 8(? 1櫟a6?T???:□□5'??徙 =方:□點趕B□?闊& 谿=:# ? 1 菁C /?w□ ??
j x?壽□ ??□鼎??zm娣鑿砥脣[ ?n?;坦袞□S□z6楸?0a孽躉 QAD煖□ \?鋪稍?1魅W鵠? 甌R 峽
皛%4 ?□ 齏 環k擗齏□??關|lsQ4ei?7?OT始鉗 ???e ?N?□l|li+?h俛鑄延□ 葵|TovHM編 1動 ?
```

第 1 行, 第 1 欄 17,886 個字元

100% Macintosh (CR)

ANSI

Demo - 後台情形(.key)



The screenshot shows a text editor window with a single tab titled "642b229ee sample.txt". The editor contains the following text:

```
wrapped_\Q <o烈E菇↓Y□;?fe u□□ □p?
```

The status bar at the bottom indicates the cursor is at "第 1 行, 第 1 欄" (Line 1, Column 1), the file contains "31 個字元" (31 characters), the zoom is "100%", the line ending is "Windows (CRLF)", and the encoding is "ANSI".

Thank you for your listening

Q&A