# Aegis基本介紹(不重要)

1. 利用**AES-256-GCM**加密，可以用password或生物辨識的方式解鎖
2. 允許/拒絕 螢幕截圖
3. 與Google Authenicator相容
4. 支持[**HOTP**](#bookmark=id.gjdgxs)和[**TOTP**](#bookmark=id.30j0zll)兩種演算法
5. 匯出：支持導出到本地端，格式支援**.JSON、.TXT**
6. 匯入：支援部分app(Authy、FreeOTP、FreeOTP+、Google Authenicator、Microsoft Authenicator、Steam、TOTP Authenicator)匯入資料，但需要root權限 / 從本地端匯入資料

**參考介紹網址：**<https://f-droid.org/zh_Hant/packages/com.beemdevelopment.aegis/>

**AES :** 進階加密標準（英語：Advanced Encryption Standard）:一種對稱金鑰加密

AES的區塊長度固定為128位元，金鑰長度則可以是128，192或256位元

**對稱金鑰加密 :** 加密和解密時使用相同的密鑰

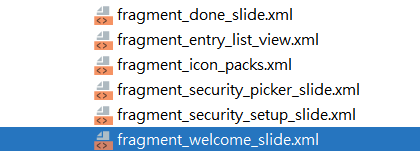
**GCM ( Galois/Counter Mode)：**指的是該對稱加密採用Counter模式，並帶有GMAC消息認證碼。

**HOTP (HMAC-based One-Time Password):** 基於HMAC算法加密的一次性密碼。是事件同步，通過某一特定的事件次序及相同的種子值作為輸入，通過HASH算法運算出一致的密碼。

**TOTP :** TOTP 是Time-based One-Time Password的簡寫，表示基於時間戳算法的一次性密碼。

# Aegis資料夾說明

* **src/main/res/layout/fragment\_XXXX**負責修改最初app打開的起始介面(welcome介面、設定密碼界面等等)



* **src/main/res/mipmap** 可以設定icon，至於as使用的是debug模式，所以出現的icon會是紅色的，而手機安裝的icon則是藍色的

ic\_launcher\_foreground跟ic\_launcher\_background是一組

其他為debug模式下的icon

尺寸分別有：

108x108

162x162

216x216

324x324

432x432

**模擬機預設dpi規格為下：**



所以是**xxhdpi** 1080p（1920\*1080 ）

要改的是**src/main/res/mipmap-xxhdpi/ic\_launcher\_debug\_foreground.png**

改這邊的icon，setting那邊的icon會跟著變動



若要更動UI介面的icon，則是修改

**src/main/res/mipmap-xxxhdpi/ic\_launcher\_debug\_foreground.png**這個檔案



* **src/main/res/layout/dialog\_add\_entry.xml** 到這裡新增button

這裡很難，icon引入我寫的drawable底下一個叫做ic\_url\_check.xml的向量icon

另為TextString要引入string資料夾裡面的item

所以要在string那邊右鍵，Open Translate Editor來做key的新增和value的設定

* Override 指的是「改寫、覆寫」，主要是用來讓**繼承的 class 改寫掉從 base class 繼承到的*行為***。
* **src/main/java/com/beemdevelopment/aegis/ui/MainActivity.java** 控制活動項，有listener，監聽onClick的動作
* **C:\Users\USER\Desktop\senior project\OTP\old\大學部\111級\fyduOTP\app\src\main\java\org\shadowice\flocke\andotp\Activities\MainActivity.java** 學長新增的程式碼寫在這裡面

# URL比對原理

可以先安裝fyduotp(學長的)跟原本的andotp做比較

會發現學長的一開始多了一個新的頁面，可以選擇URL比對的地方，關掉就會是一般andotp的樣子。

Aegis是掃描QR code，會自動填入發行商、ID、和金鑰 (以臉書的2FA為例子)

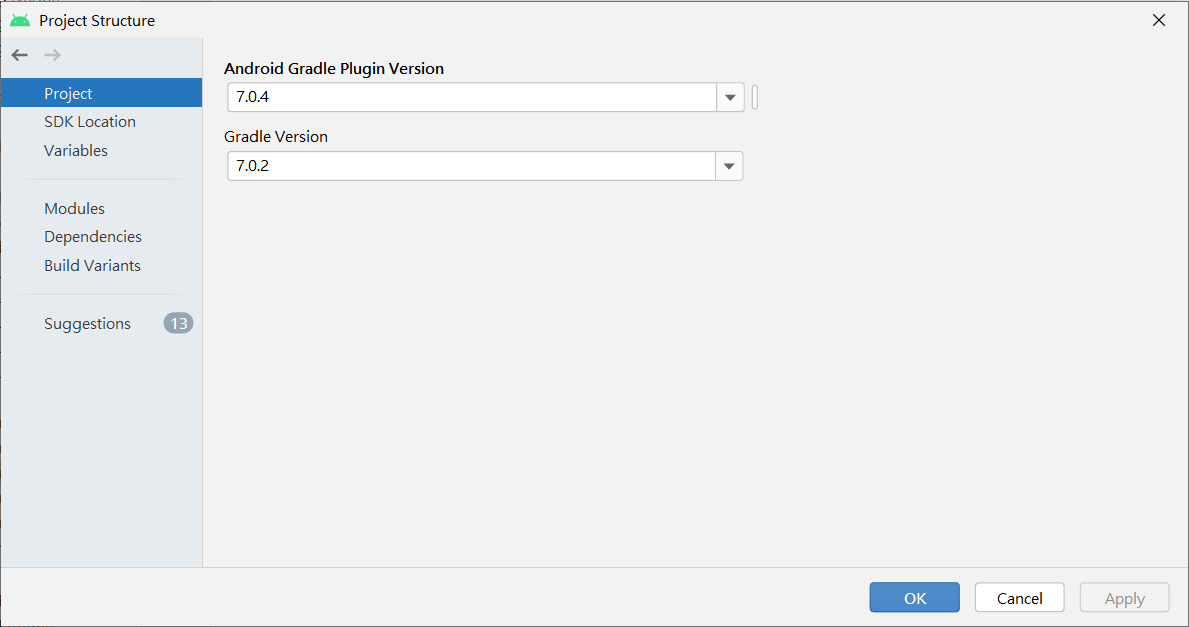


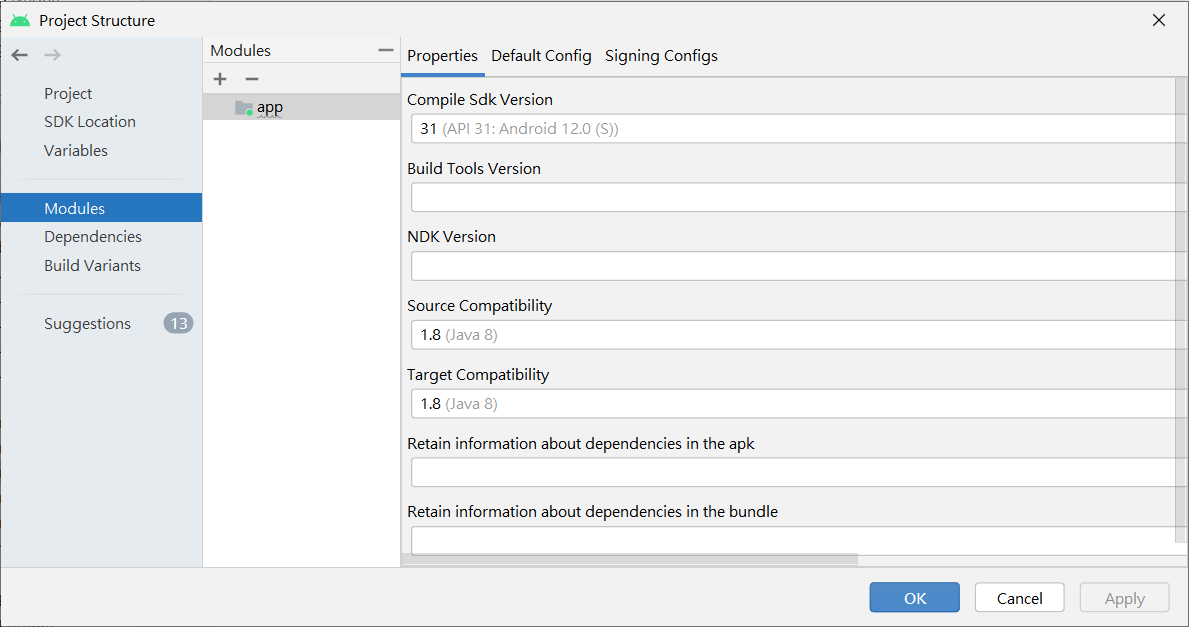
掃描出來會自動填入金鑰

而比對URL功能是主要在登入時，**所以應該要在進入頁面新增一個「登入前判斷URL網址是否安全頁面」來掃描URL是否安全再進行登入(可能判定安全就打開該URL)**

所以老師才會說要結合PM功能

# Project Structure參數





# Gradle是甚麼

<https://codertw.com/ios/69804/> [參考網址]

所以最初 Google 還是希望 Android 能在 Eclipse 上進行開發，為了滿足這個需求，Google 開發了一個叫 ADT （Android Developer Tools）的東西，相信以前從 Eclipse 時代過來的對 ADT 應該都不陌生，正是因為有了 ADT ，從此我們只需要碼好程式碼，然後直接在 Eclipse 上進行編譯、執行、簽名、打包等一系列流程，而這背後的工作都是 ADT 的功勞。某種意義上 ADT 就是我們的構建工具。

Google 推出 Android Studio 以來，就宣佈預設使用 Gradle 來作為構建工具

Gradle 採用的是一種叫做 Groovy 的語言

現在預設新建一個專案，然後點選 AS 上的執行，預設就會直接幫你安裝 Gradle ，我們不需要額外的安裝 Gradle 了，但是其實這個 Gradle 不是真正的 Gradle ，他叫 Gradle Wrapper ，意為 Gradle 的包裝，什麼意思呢？假設我們本地有多個專案，一個是比較老的專案，還用著 Gradle 1.0 的版本，一個是比較新的專案用了 Gradle 2.0 的版本，但是你兩個專案肯定都想要同時執行的，如果你只裝了 Gradle 1.0 的話那肯定不行，所以為了解決這個問題，Google 推出了 Gradle Wrapper 的概念，就是他在你每個專案都配置了一個指定版本的 Gradle ，**可以理解為每個 Android 專案本地都有一個小型的 Gradle ，通過這個每個專案你可以支援用不同的 Gradle 版本來構建專案**