112 學年度十二年國民基本教育課程綱要普通型數位前導學校計畫
資訊安全與數理邏輯跨領域實作工作坊(九)實施計畫

壹、 研習講題：資訊安全與數理邏輯跨領域實作工作坊(九)

貳、承辦單位：國立臺南第一高級中學

參、研習時間與地點：

一、研習時間：113 年 3 月 1 日(星期五)13 時 30 分~17 時 30 分 (13 時 30 分~13 時 40 分為報到時間)

二、研習地點：國立臺南第一高級中學 藝術教育大樓二樓 201 電腦教室

肆、研習議程：

時間	主題	講者	講座助理
13:30-13:40	報到		
13:40-14:30	編碼、Hash 與加密	黃俊嘉	高英耀
14:40-15:30	古典密碼學	黃俊嘉	高英耀
15:40-16:30	Stream Cipher	黃俊嘉	高英耀
16:40-17:30	Q&A 及實作	全體與會人員	

伍、活動對象：教師 40 名，採先報名先錄取方式

陸、研習大綱：

- ✧ 編碼是資訊從一種形式轉換為另一種形式的過程，轉換過程為約定好的處理方式，因此編碼後的資料視同為明文；解碼則是編碼的逆過程。
- ✧ 雜湊是電腦科學中一種對資料的處理方法，通過雜湊函式將資料與索引（雜湊值）關聯起來，生成一種便於搜尋的雜湊表。它也常用作一種資訊安全的實作方法，由一串資料中經過雜湊演算法計算出來的資料指紋，經常用來識別檔案與資料是否有被竄改，以保證檔案與資料確實是由原創者所提供。
- ✧ 加密指將資料明文與金鑰（Key）進行特殊計算，產生不可辨識的密文。
- ✧ 古典密碼學是指在電腦發明以前人類的資料以文字書寫，為免遭到竊取，所以針對文字進行加密，通常分為替換式密碼與轉置式密碼兩大類。
- ✧ Stream cipher 是一種對稱加密演算法，加密和解密雙方使用相同偽隨機加密資料流作為金鑰，明文資料每次與金鑰資料流順次對應加密，得到密文資料流。實踐中資料通常是一個位元 xor 操作加密。

柒、 報名方式：

一、全國教師在職進修資訊網(https://www1.inservice.edu.tw/)，課程代碼： **4215603**。

二、報名時間：即日起至 113 年 2 月 27 日(星期二)止。

捌、經費來源：

一、本案所需經費由承辦單位之前導學校計畫及數位學習精進方案相關經費項下支應。

二、參加人員請服務學校(單位)惠予公(差)假登記，往返差旅費由原服務單位依規定報支。

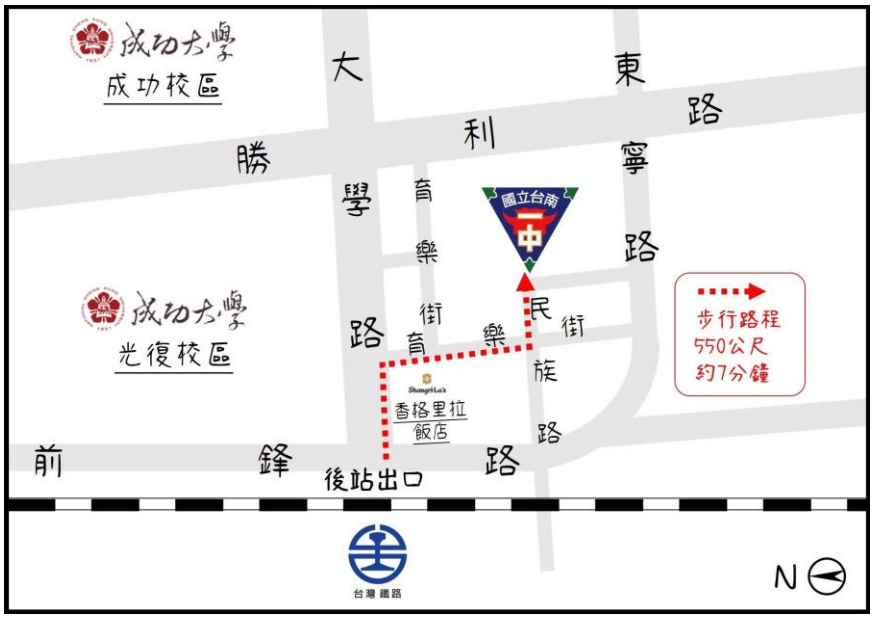
玖、交通方式：

本次研習不另提供接駁服務，敬請與會師長多搭乘大眾運輸交通工具，造成不便，敬請見諒。

一、高鐵&臺鐵：

(1) 高鐵：高鐵臺南站，請轉乘臺鐵沙崙線至臺鐵臺南站，由後站出站，步行約 7 分鐘。

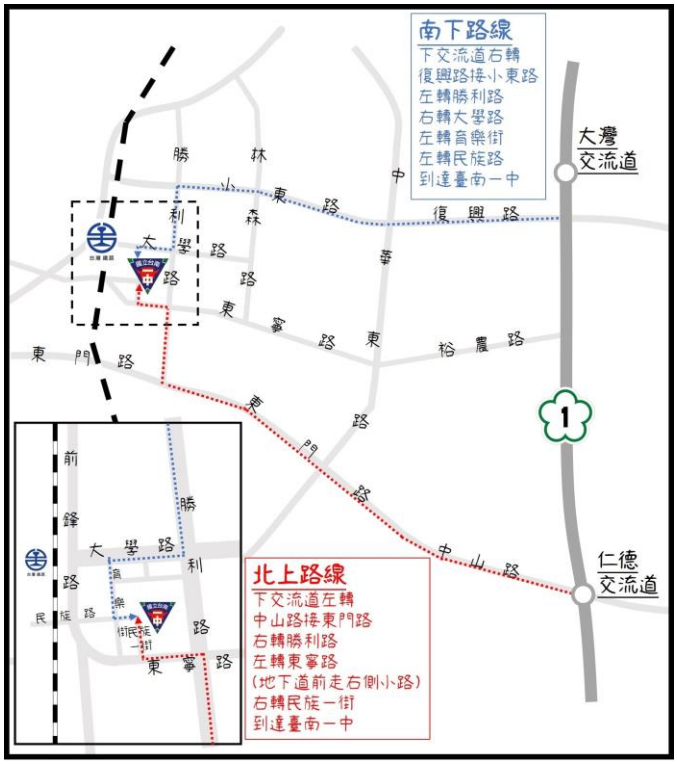
(2) 臺鐵：臺鐵臺南站，請從後站出站，步行約 7 分鐘。



二、自行開車：

(1) 高速公路(北上)：仁德交流道→左轉中山路接東門路→右轉勝利路→左轉東寧路(地下道前走右側小路)→右轉民族一街。

(2) 高速公路(南下)：大灣交流道→右轉復興路接小東路→左轉勝利路→右轉大學路→左轉育樂街→左轉民族路。



研習地點：


臺南一中地圖
MAP OF ZHUYUANGANG
特色課程展示廳
民族一街 Minzu 1st St.
傳達室
民族路 Minzu Rd.
學生車棚
紅樓
科學教育大樓
小禮堂
至善樓
新民樓
綜合教育大樓
藝術教育大樓
合作社
大榕樹
垃圾場
明德樓
人文教育大樓
群英堂
操場
東寧路
勝利路
地下道
Shengli Rd.
研習地點
停車位置
體育館
排球場
游泳池
Dongning Rd.
司令臺
足球場
學生宿舍
網球場
籃球場
排球場
跳遠場地
N
圖例
公車臺南一中站
中華郵政ATM
全家臺南一中店