

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(十一)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(十一)

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 22 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	非對稱式加密	黃俊嘉	高英耀
14:40-15:30	非對稱式加密弱點與攻擊實作	黃俊嘉	高英耀
15:40-16:30	數位簽章簡介	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：

- ✧ 非對稱加密（英語：Asymmetric cryptography）也稱為公開金鑰加密（英語：Public-key cryptography），是密碼學的一種演算法，它需要兩個金鑰，一個是公開金鑰，另一個是私有金鑰：一般而言用公開金鑰加密、私密金鑰解密。
- ✧ 數位簽章英文為 Digital Signature，也常稱數位簽名，是將電子文件使用演算法、私密金鑰和加密技術，來進行數位資訊鑑別的方法。數位簽章具備真實性、完整性與不可否認性。

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：4228173。
- 二、報名時間：即日起至 113 年 3 月 20 日(星期三)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。

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。

- (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。



-

研習地點：

