

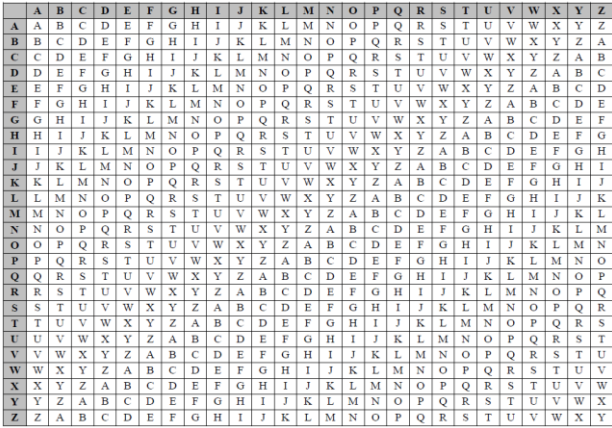


新北市 科技領域 教學示例

(一) 教案概述

單元名稱	資訊安全		
領域/科目別	科技領域/資訊科技		
教學對象	國中7年級	教學時數	共 2 節， 90 分鐘
教學資源	筆、電腦、網路、瀏覽器、偷插電的資訊科學【教師手冊】		
學習目標	1. 學生能了解資訊安全的重要 2. 學生能了解傳遞訊息被竊取的風險 3. 學生能了解網頁加密與未加密的差異 4. 學生能了解凱薩密碼與維吉尼亞密碼的編碼概念 5. 學生能透過分組合作學習完成學習單		
先備知識	1. 使用瀏覽器 2. 英文字母		
可融入之領域/議題	實質內涵	法治教育議題	
	所融入之學習重點	理解法律與法治的意義；習得法律實體與程序的基本知能；追求人權保障與公平正義的價值。	
與課程綱要的對應	核心素養	J-B2 具備善用科技、資訊與媒體以增進學習的素養，並察覺、思辨人與科技、資訊、媒體的互動關係。 J-C2 具備利他與合群的知能與態度，並培育相互合作及與人和諧互動的素養。	
	學習表現	運 a-IV -2 能了解資訊科技相關之法律、倫理及社會議題，以保護自己與尊重他人。	
	學習內容	資H-IV-3資訊安全。	
課程設計架構圖	<div><div>引起動機</div><div>生活實例探討</div><div>凱薩密碼 介紹,加密,解密</div><div>維吉尼亞密碼 介紹,加密,解密</div><div>教師總結</div></div> <div>• 第一節 45分鐘</div> <div>• 第二節 45分鐘</div>		

教學活動 (名稱)	教學內容 (含時間分配)	備註 (如學習單等、教學資源)
第一節 活動一 引起動機	<ol style="list-style-type: none"> 教師舉例資訊安全的相關新聞案例。 觀看阿里巴巴與四十大盜影片(觀看前半段)。 引導學生透過故事發現有那些資訊安全的問題? <p>(共 15分鐘)</p>	<ol style="list-style-type: none"> 個資外洩案 FB 執行長承認錯誤 受訪道歉 https://www.youtube.com/watch?v=Yki-cVi76mc 阿里巴巴與四十大盜影片 https://www.youtube.com/watch?v=A9iiuykkRcM 學習單
第一節 活動二 網頁加密安全性講解	<ol style="list-style-type: none"> 請學生觀察與討論瀏覽器網址列前方標示的安全與不安全圖示。 教師引導分組討論並分享觀察的差異，並尋找那些網站有安全性的標示。 觀看加密原理與公私鑰影片(觀看前半段)。 請同學分享心得並由教師做總結與歸納。 <p>(共 20分鐘)</p>	<ol style="list-style-type: none"> 各校學校網站、新北市校務行政系統網站加密網頁  未加密網頁  學習單 加密原理與公私鑰 影片 https://www.yxgapp.com/video/c9f80aca-fa92-440f-992d-61f22193727b.html
第一節 活動三 介紹凱薩密碼 加密與還原	<ol style="list-style-type: none"> 教師介紹凱薩密碼。 引導學生加密與還原的過程。 完成學習單。 	<ol style="list-style-type: none"> 學習單 凱薩密碼 http://ctf.ssleye.com/caesar.html

	(共 10分鐘)	
第二節 活動四 學生分 組練習	1. 進行分組練習與猜測。 2. 教師引導並討論可能遭遇的問題與限制。 (共 10分鐘)	1. 學習單 2. http://ctf.ssleye.com/caesar.html
第二節 活動五 維吉尼亞密碼 的加密 與解密	1. 教師介紹維吉尼亞密碼。 2. 教師實際舉例利用自訂的金鑰來加密。 3. 教師實際舉例利用自訂的金鑰來解密。 4. 教師引導學生分組合作練習自訂金鑰加密與解密。 5. 教師引導討論金鑰的長短與複雜度對加解密難易度之差異。 6. 教師總結資料加在資訊安全中的議題與意義。 (共 35 分鐘)	1. 學習單 2. 維吉尼亞密碼對照表 

(二) 評量活動

評量目標	1. 能完成學習單。 2. 能參與分組討論。 3. 學生能了解網頁加密與未加密的差異。 4. 學生能舉例常用的網站那些是網頁有加密。 5. 學生能實際練習凱薩密碼的加密與解密。 6. 學生能實際練習維吉尼亞密碼的加密與解密。
評量工具	學習單、口頭分享。

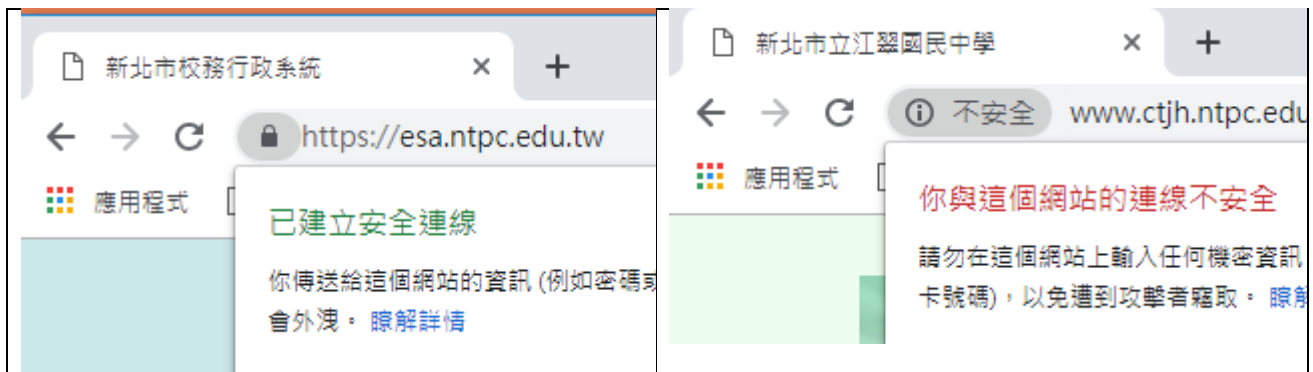
密碼與資訊安全學習單

觀看影片回答問題？

- 阿里巴巴是如何打開石洞？
- 阿里巴巴是怎麼知道密碼的？
- 阿里巴巴的哥哥在石洞內忘記密語時做了什麼事？
- 透過影片發現有那些問題並討論如何改善？

觀看網址列標示的問題？

- 觀察瀏覽器網址列中安全與不安全的標示



- 討論並分享差異？
- 尋找一下常用的網站那些有安全性的標示？

凱薩密碼 (Caesar cipher)

明文中的所有字母都在字母表上向後,按照一個固定數目進行偏移後 被替換成密文

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

基礎題

位移量是 3 的話 原文: SOS → 密文: _____

位移量是 3 的話 原文: HELLO → 密文: _____

位移量是 3 的話 密文: khos → 原文是: _____

進階題

如果收到一密文內容是 K jcxg c rgp

猜測可能的位移量: _____ (提示: 1 ~ 25)

原文是: _____

分組出題與猜測，並討論有何缺陷？

維吉尼亞密碼 (Vegenere CIPHER)

凱撒密碼：每一個字母相同的偏移量，

維吉尼亞密碼：每個字母都不同的偏移量 (參考表格)

加密

範例： 原文 HELP 金鑰 NTPC 密文 UX??	練習： 原文 face 金鑰 NTPC 密文 ??
練習： 原文 I have a dog 金鑰 N TPCN T PCN 密文 ?? 原文 Have a nice day 金鑰 taiwan 密文 ??	

解密

密文 b hire n wrmwm

金鑰

原文

分組出題與猜測

附件

維吉尼亞密碼對照表

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y