一個應用近代加密技術實現的安全聊天軟體

專題生: 電機四 4108054117 余元正

一、介紹

不論是在 Facebook、Line、微信、Twitter、QQ... 等通訊軟體中，我們都可以跟好友或是好友們進行私聊。不論是閒談亦或是機密，我們都不希望訊息有其他人知道，是否能保障使用者的安全通訊(Secure Communication)，是日漸重要的課題。

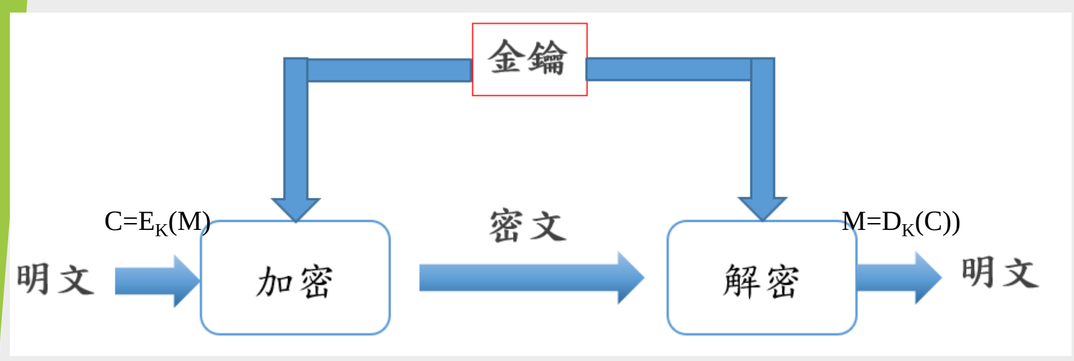
為了防止他人隨意擷取電腦傳送出的訊息就能直接輕易得知信息內容，我們必須將訊息經過加密技術加密後再傳送。

二、基礎機制

加密算法是密碼學的核心，常見的方式是在寄送訊息端將訊息(明文)表述為不
具可讀性的方式(密文)，此謂之加密。接收端再以一種秘密數學演算法將訊息恢復
回來，此謂之解密。
加密算法千萬種，其基本組成通常都包含四個部分:

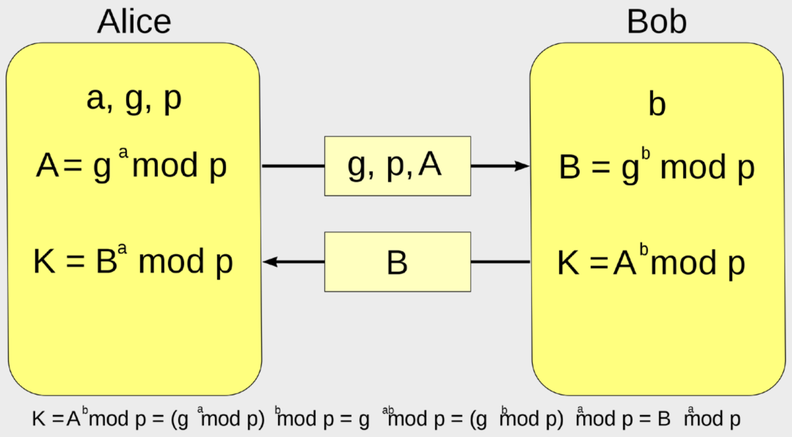
1. 需要被加密的初始訊息，即明文 M。
2. 用於加密或解密的鑰匙，即金鑰 K。
3. 加密算法 E 或是解密算法 D。
4. 明文被加密後得到的密文 C。

加解密過程示意圖



在手機版與電腦版的程式中，為了能在公共信息道中建立一個安全信息通道，我們需要進行金鑰協商(Key Agreement)來使雙方能協議出一個共享秘密(Shared Secret)，並使用此共享秘密作為此次通訊的會議金鑰(Session Key)，並使用會議金鑰對通訊中傳送/接收的訊息進行加密/解密。
在程式中可以使用:**CRYSTALS-Kyber KEM(電腦版)、ECDH、DH等**算法來協商出對稱密鑰，來加密訊息。

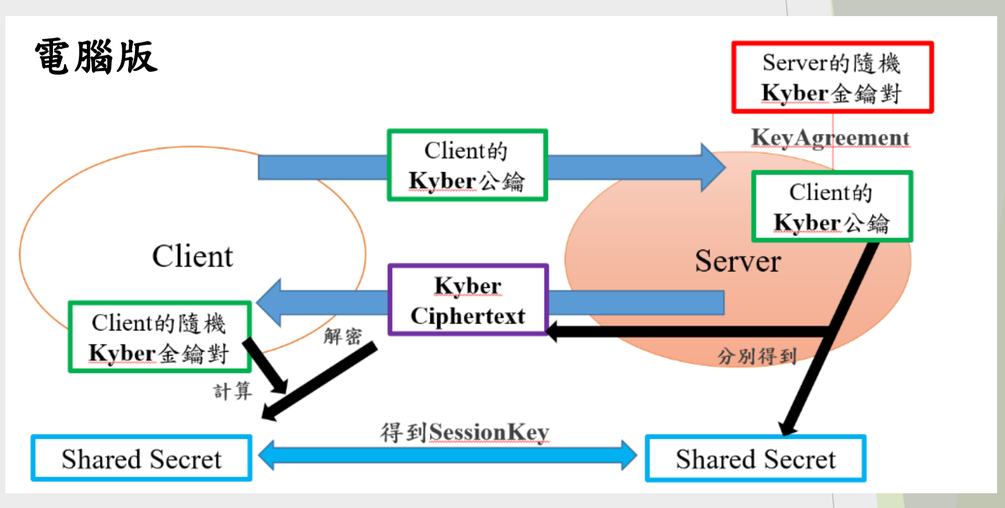
Diffie-Hellman原理:



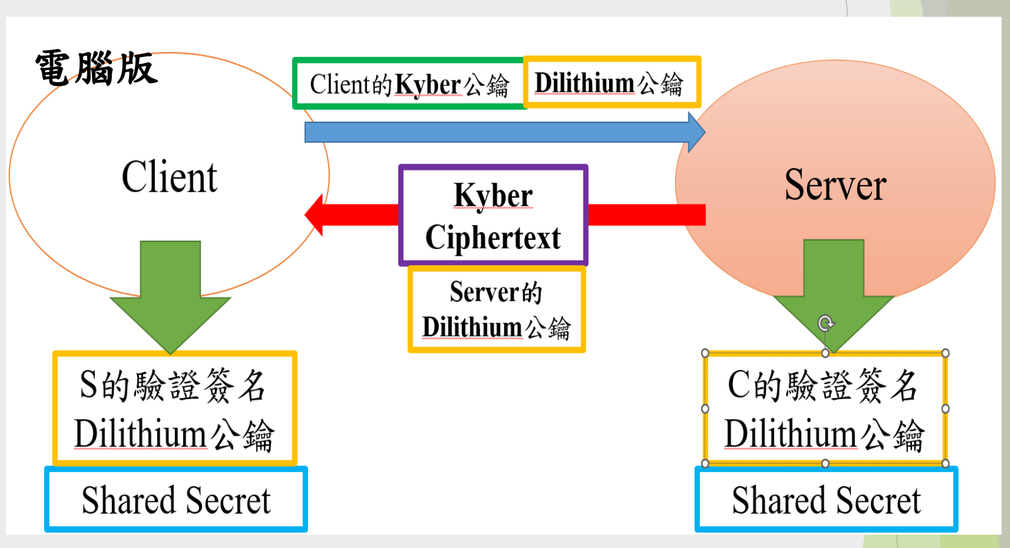
如上圖中，Alice產生a,g,p，其中a保密，計算A後將g,p,A傳送給Bob，Bob收到後計算回傳B給Alice。
至此，雙方皆計算出共享秘密K。

Alice		Bob		Eve	
knows	doesn't know	knows	doesn't know	knows	doesn't know
p = 23	b = 15	p = 23	a = 6	p = 23	a = 6
base g = 5		base g = 5		base g = 5	b = 15
a = 6		b = 15			s = 2
$A = 5^a \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$		$A = 5^a \bmod 23 = 8$	
$B = 5^b \bmod 23 = 19$		$A = 5^a \bmod 23 = 8$		$B = 5^b \bmod 23 = 19$	
$s = 19^b \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$		$s = 19^a \bmod 23$	
$s = 8^b \bmod 23 = 2$		$s = 19^a \bmod 23 = 2$		$s = 8^b \bmod 23$	
$s = 19^b \bmod 23 = 8^b \bmod 23$		$s = 8^{15} \bmod 23 = 19^a \bmod 23$		$s = 19^a \bmod 23 = 8^b \bmod 23$	
s = 2		s = 2			

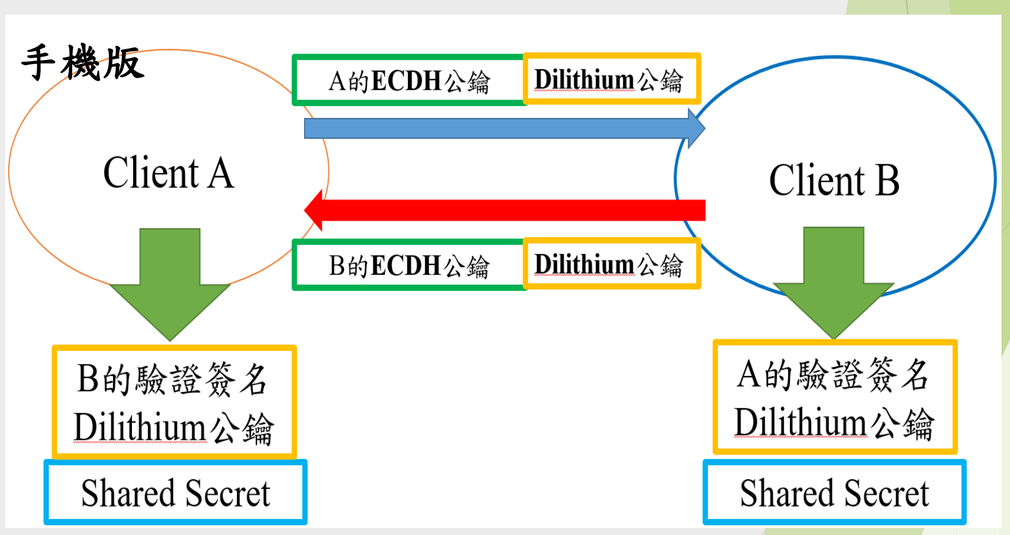
三、系統架構



Server端與Client端的密鑰協商



加入CRYSTALS-Dilithium簽名簡化後的密鑰協商



ECDH+CRYSTALS-Dilithium簽名簡化後的密鑰協商

四、結論

透過對訊息的加解密，終於使我們的聊天室變的安全多了。

未來希望能在電腦版提供離線訊息的功能以及資料庫的運用。手機版希望能提供好友群聊等功能，讓這個軟體更加方便，這些都是接下來可以繼續努力的目標。