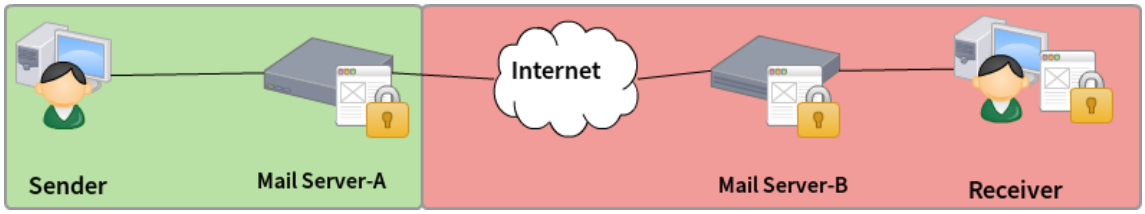
郵件加密！

電子郵件的應用並沒有因為即時通訊軟體，如 LINE、Whatsapp 興起而被取代相反的因為郵件格式是通用格式，任何作業系統或是網路環境都可以輕易的閱讀，但是如何確保郵件傳輸時的安全及隱密性，卻又是另一個嚴肅的考驗。郵件加密並不是一個新的技術，但傳統複雜的 PGP 、S/MIME 及 PKI 加密技術，讓傳送及接收雙方都要付出額外的處理程序才能傳送或是看到郵件，讓郵件加密的優點因為不方便操作而被放棄。

簡易的加密及解密程序，就是讓郵件加密普及的最重要因素，因此， ShareTech 的郵件伺服器利用加密的 ZIP 或是 PDF 等形式傳送郵件，讓雙方原本的發送及接收習慣改變最小，但又可以確保郵件的保密性。基本上 ZIP 跟 PDF 都是常見的檔案格式，一般的電腦甚至是手機、平板電腦等要開啟這類型的檔案，並不需要安裝額外的軟體，只要寄件者利用適當的管道將加密的密碼告知收信者或是雙方約定好的密碼，收信者就能順利的解開檔案。

郵件加密運作原理

每封郵件都是由內文或是附加檔案組合，採用 ZIP 加密的方式時，郵件伺服器會把附加的檔案以 ZIP 方式加密，再加密過程給予一個加密的密碼，重新組合郵件內文及加密後的 ZIP 檔案，再傳送給收信者，至於內文則保留原來的格式，當郵件在傳遞過程或是儲存在使用者的電腦中遭駭客入侵，駭客們只看到一個需要密碼解鎖的 ZIP 檔，如果沒有密碼並沒辦法看到完整的檔案，示意圖如下：



眾至資訊股份有限公司

台中總公司
04-27050888
台北分公司
02-25011185
高雄分公司
07-2298788
免付費專線
0800-666188

另一種傳遞加密郵件的是採用 PDF 加密的方式，郵件伺服器會將內文跟附加檔案，整個打包成 PDF 格式，當收信者收到郵件時是看到一封需要密碼解密的 PDF 檔案，輸入傳送者給的密碼後，才能看到原始郵件的內文及附檔，如下圖：

加密的 PDF 裡面如果有附加檔案，需要使用 PDF 閱讀軟體才能看到檔案，使用瀏覽器的 PDF 則只能看到內文。

從整個加密過程可以理解，加密郵件出了寄件者的郵件伺服器後，全變成由密碼保護的加密形式，不論是 ZIP 或是 PDF 格式，沒有密碼，將無法看到郵件內容，確保這一封郵件只有寄件者認定的收件者才有辦法看到原始內容。

密碼很重要，如何管理 ？

郵件服務器加密時使用的密碼可以採用隨機密碼或固定密碼 2 種，固定密碼的方式比較簡單，特定的收件者使用特定的密碼，例如：銀行寄信用卡帳單都會使用收信者的身份證字號當作預設密碼。

但是動態的隨機密碼就比較傷腦筋，每封郵件的加密密碼都不一樣，不過郵件服務設想周到，採用 2 種方式，克服這個問題，一種是寄出密碼通知信，每次加密郵件寄出，延遲數分鐘後再寄出一封密碼通知信給雙方，註明此次加密的密碼。另一種是讓收信者登入郵件伺服器查詢加密的密碼，對於收件者來說，在經過授權後也可以進入郵件伺服器查詢密碼。

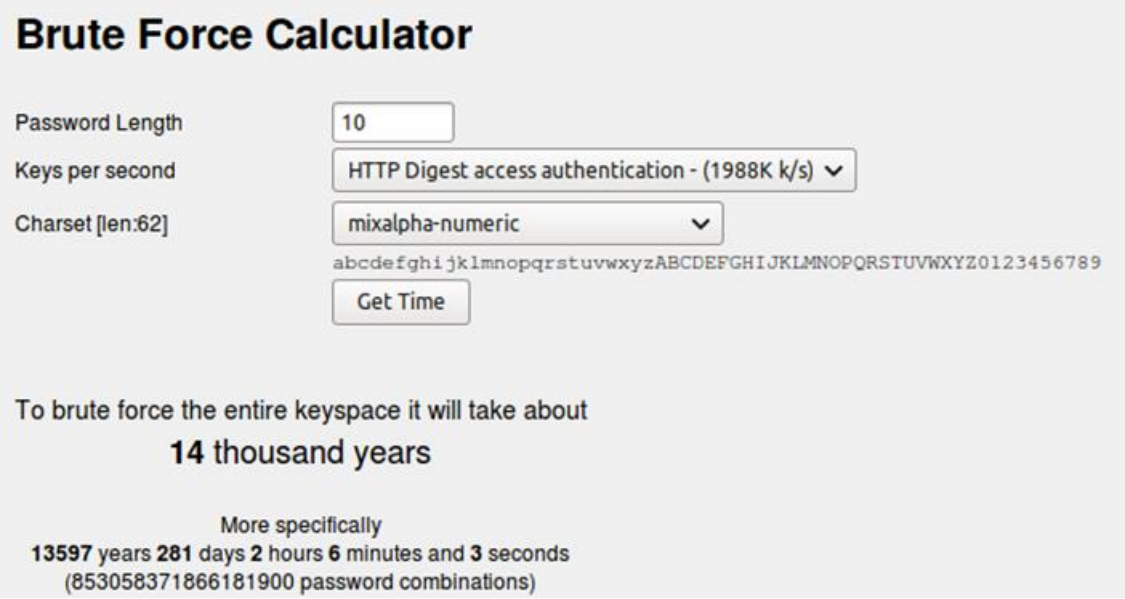
眾至資訊股份有限公司

台中總公司
04-27050888
台北分公司
02-25011185
高雄分公司
07-2298788
免付費專線
0800-666188

只有密碼保護夠安全 ？

有別於傳統使用公鑰跟私鑰的郵件加密模式，單用密碼保護的強度感覺上似乎有點薄弱，理論上使用密碼保護的資料，如果使用暴力破解的方式在『特定的時間』內一定能被破解。換個方向想，如果這個『特定的時間』比郵件的生命週期更長，那就達成保護郵件內容的目的，例如，設定的密碼被暴力破解需要 20 年的 CPU 運算時間，如果這個時間比郵件內容的生命週期更長，間接就保護資料的安全。

因此使用郵件加密時的密碼組合跟強度就非常重要，密碼組合方式就牽涉到被暴力破解的時間，以 http://calc.opensecurityresearch.com/ 這個網站的時間估算，如果採取英文大小寫跟數字的組合，在密碼長度為 10 個字元下，暴力破解密碼需要 140 年，參考下圖：



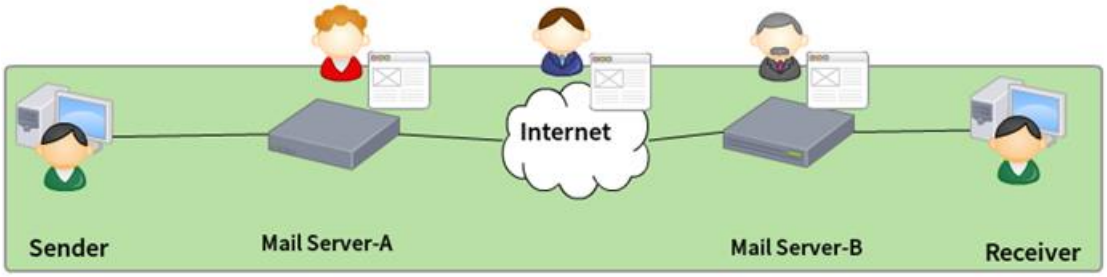
140 年的破解時間遠比此封郵件的生命週期更長，因此使用密碼保護的郵件內容可以在特定的時間內確保他的資料完整性跟安全性。

眾至資訊股份有限公司

台中總公司
04-27050888
台北分公司
02-25011185
高雄分公司
07-2298788
免付費專線
0800-666188

不做加密會怎樣？

一般郵件的溝通是用 SMTP 協定，這個協定沒有任何加密的機制，有心人士只要側錄網路封包就可以將傳遞的郵件擷取，就算採用新的 SMTPS 加密技術傳輸，一樣可以透過 Man-In-Middle 的方式，從網路上將信件還原成原來的狀態，就算採用嚴謹的 VPN 或是數據專線保護了傳輸端的傳遞機制，Mail Server 還有 MIS 或是管理人員可以看到完整的郵件內容，整封郵件的資料就是『天知、地知、你知、我知、大家都知』，如下圖：



透過簡單的郵件加密機制，不僅可以保障郵件在傳輸過程不被人竊取，就算存在個人的電腦或是手機上，也不必擔心機密資料外洩，因為只有收件者才有解密的密碼，駭客侵入網路或是個人電腦後，拿到的是一堆加密過的亂碼，就算要用暴力破解，也要等到 140 年後，更方便的是，這樣的加密機制比使用 PGP、PKI 等技術更不會造成傳送及接收端的困擾及使用習慣，在方便性跟安全性取得一個平衡點。

眾至資訊股份有限公司

台中總公司
04-27050888
台北分公司
02-25011185
高雄分公司
07-2298788
免付費專線
0800-666188