網路安全

Diffie-Hellman金鑰交換技術

Diffie-Hellman金鑰交換技術

- 金鑰交換是指兩個或多個成員在開放網路環境下，透過相互間訊息的交換，彼此能夠共享一個秘密的資訊。
- 由 Diffie 與 Hellman 於 1976 年提出，也引出了公開金鑰的概念來建立一個秘密交換資訊的管道 – 最早提出的公開金鑰架構
- 但James Ellis（UK CESG）已於1970年時不為人知地 已提出此概念
- 主要目的在於讓網路上未曾見面的雙方，可以透過計算模指數（modulo）運算，而使得雙方可以獲得相同的 交談金鑰（session key）。
- 是一個可以實際用於公開交換秘密金鑰的方法及商用產品。

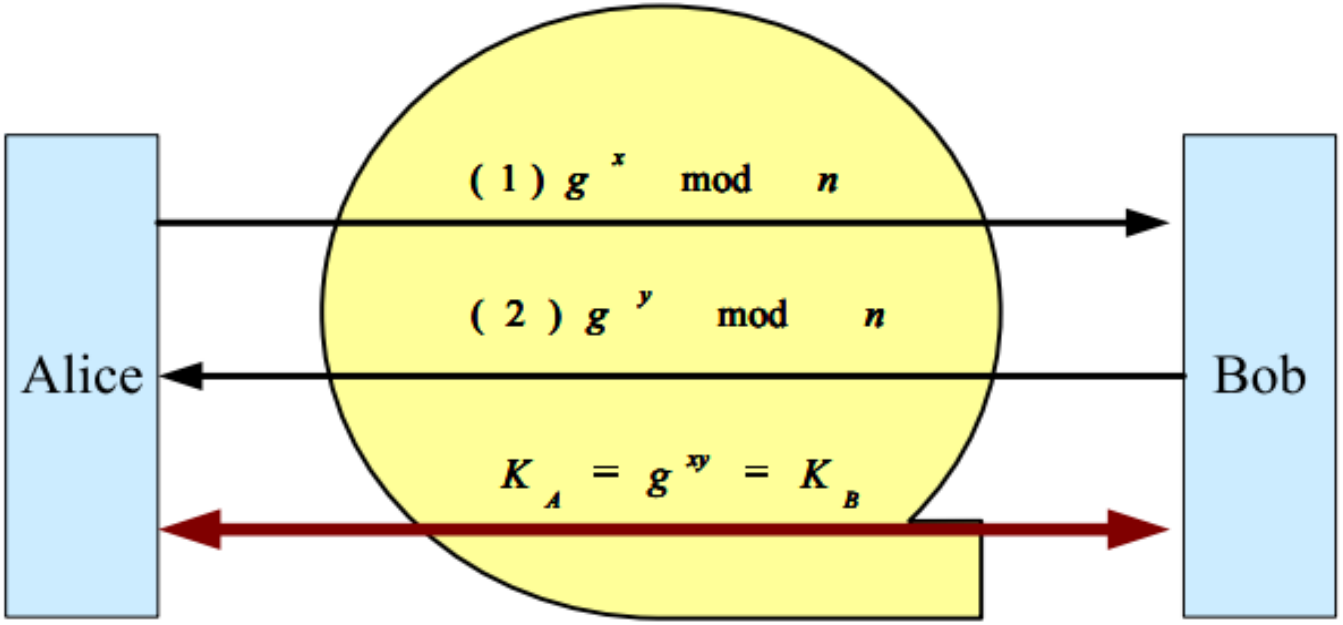
Diffie-Hellman金鑰交換技術

- 一個利用公開金鑰的分送機制，其特色為
  - 可以用來產生一把通訊雙方共用的金鑰
  - 只有通訊雙方知道此把共用金鑰
  - 金鑰的內容由通訊雙方來決定
  - 以有限體(Galois)的指數運算為基礎(取某質數或多項式的同餘)
- 此金鑰交換系統安全性一般認為是植基於解離散對數(discrete logarithm)的困難度，以目前演算法的安全分析來說，到目前為止還是很安全 的。

Diffie-Hellman金鑰交換技術

- 金鑰交換過程缺乏提供溝通雙方相互身份認證的功能，任何人都可以假冒成對方跟其他使用 者作秘密通訊，無法有效抵擋中間人攻擊（man-in-the-middle attack）

原型



(3) $K_A = (g^y \bmod n)^x$

$= g^{xy} \bmod n$

(4) $K_B = (g^x \bmod n)^y$

$= g^{xy} \bmod n$

$K_A=(g^y)^x$

$K_B=(g^x)^y$

範例

- 範例:Alice與Bob欲利用Diffie-Hellman演算法產生秘密通訊的金鑰。
  - 計算金鑰的公式為$k = g^{xy} \bmod n$
  - g,n為公開，分別為g=3，n=19
  - Alice選定x=4
  - Bob選定y=5
  - 請計算雙方共同決定的秘密通訊金鑰 k=?

ANS:

Alice計算$g^x \bmod n = 3^4 \bmod 19=5$ → (傳送給Bob)

Bob 計算$g^y \bmod n = 3^5 \bmod 19=15$ → (傳送給Alice)

Alice收到15,然後計算$15^4 \bmod 19=9$

Bob 收到5, 然後計算$5^5 \bmod 19=9$

先不考慮mod（變型）最後mod一次

假定基底為：3

二人第一次各自計算：

Alice 隨機自選一個數字假定為4

Alice計算 3^4 =81 → （傳送給Bob）

Bob 也隨機自選一個數字假定為5

Bob 計算 3^5 =243 → （傳送給Alice）

二人收到對方送來的值，進行第二次的計算：

Alice收到243，然後計算243^4 =3,486,784,401

$(3^5)^4$

Bob 收到81， 然後計算81^5 =3,486,784,401

$(3^4)^5$

範例 cont.

先不考慮 mod

ANS:

【Phase-1 】

Alice計算$g^x \bmod n = 3^4 = 81$ → (傳送給Bob)

Bob 計算$g^y \bmod n = 3^5 = 243$ → (傳送給Alice)

【Phase-2】

Alice收到243, 然後計算$243^4 \bmod 19 = 9$

Bob 收到81, 然後計算$5^5 \bmod 19 = 9$

隨堂練習

- **答題方式請參考第 7 & 8頁（變型）**

- 練習：同上g=3, n=17, Alice選定x=2, Bob選定y=4
  請計算雙方共同決定的秘密通訊金鑰 k=?

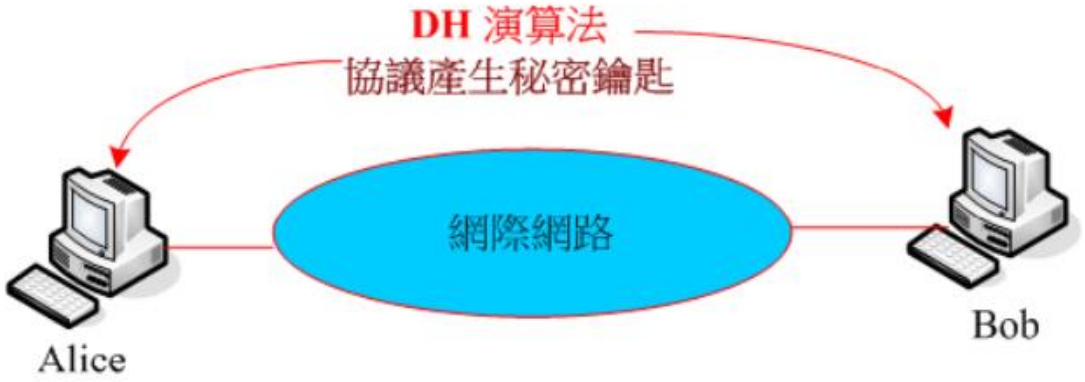
Diffie-Hellman 安全性

- 如果某人監聽線上的流量時，他們或許會得知g、n、g^x和g^y，但是x 和y依舊安全無虞。
- 這個系統的安全性主要是依據即使得知 $g^x \bmod n$ 也很難找到 x。
- 這個問題稱為離散對數問題，因而數字越大也就越難算出結果（也就是說以現今的電腦能力也很難算出結果）。
- 必須非常小心選擇x和y(夠大)。

網路參考資料 1/3

Diffie-Hellman 鑰匙交換

- DH 演算法目的－產生秘密鑰匙



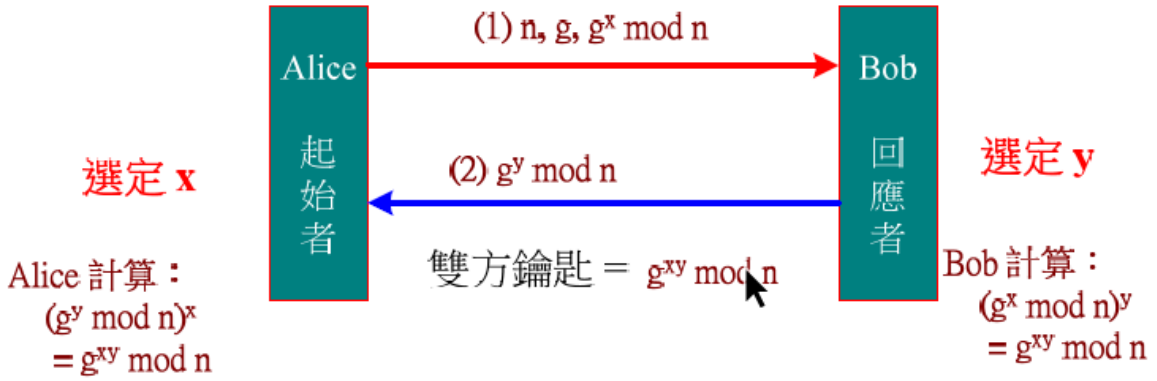
註:http://www.tsnien.idv.tw/Security_WebBook/security_PDF/chap3/3-6-1%20Diffie-Hellman%20%E6%BC%94%E7%AE%97%E6%B3%95%E6%8E%A8%E8%AB%96.pdf

網路參考資料 2/3

Diffie-Hellman 鑰匙交換

mod：模數運算

- 鑰匙交換的運作程序
  - n 與 g 為公開值
  - 雙方各選一個較大的數值 x 與 y
  - 參數 g 與 n 可以由發起端(x) 或憑證內註明
  - 計算出『秘密鑰匙』：$g^{xy} \bmod n$



網路參考資料 3/3

DH 演算法推論

- 驗證 Diffie-Hellman 演算法
  - Alice 選定：n = 47, g =3, x=8, 計算出：

    $g^x \bmod n = 3^8 \bmod 47 = 28 \bmod 47$

    訊息 (1) = {47, 3, 28}
  - Bob 選定：y =10 , 計算出：

    $g^y \bmod n = 3^{10} \bmod 47 = 17 \bmod 47$

    訊息 (2) = {17}
- Alice 計算會議鑰匙：

  $(g^x \bmod n)^y = g^{xy} \bmod n = 28^{10} \bmod 47 = 4 \bmod 47$
- Bob 計算會議鑰匙：

  $(g^y \bmod n)^x = g^{xy} \bmod n = 17^8 \bmod 47 = 4 \bmod 47$
- 會議鑰匙 k= 4

參考資料

- ftp://163.25.117.117/clhsu/ISMT/%B8%EA%A6w%B9%EA%B0%C8%C5%E9%C5%E7%BDg%20v1.6/pdf/12.pdf