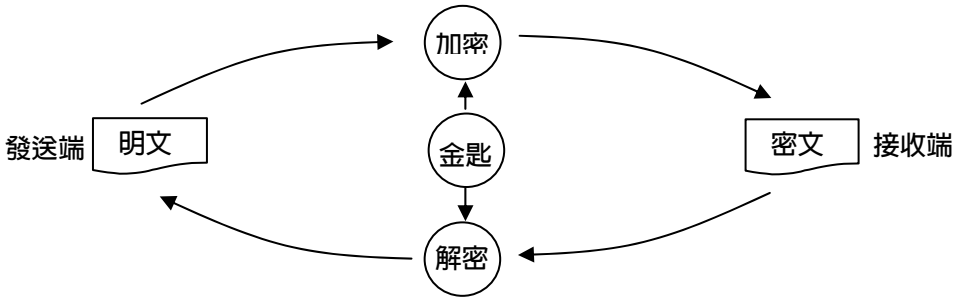
窮理致知

# Hill cipher（Hill 加密法）

楊儒民*

網路的普及，使訊息易於傳輸，但網路為公開的通道（public channel），致使傳輸中的訊息易於遭受有心人士竄改或截取，因此訊息（明文）經由加密後，轉換成密文傳輸，可確保其安全，下圖為加密及解密之架構圖：




上述金匙為傳統密碼學中，發送端及接收端皆須擁有作為加密或解密之鑰匙，下面我們介紹一個在 1930 年代由 Hill[1]發展出之加密法；首先將英文字母作如下之對應：

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

設明文為「ATTACK AT DAWN」，然後將其兩字一組拆解如下：

AT　TA　CK　AT　DA　WN

並將其轉換成對應之數值：

0 19　19 0　2 10　0 19　3 0　22 13

* 楊儒民，南台科技大學通識教育中心自然科學組副教授。

[1] L. S. Hill “Concerning certain linear transformation apparatus of cryptography”, American Mathematical Monthly, volume 38 (1931), 135-154.

南台通識電子報
2011 年 7 月 15 日出版
南台科技大學通識教育中心 發行
27期

我們將每組數值視為 2×1 之矩陣 $\begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$，

且設已知金匙為一矩陣 $K=\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}_{2\times 2}$，且設 gcd(det(k),26)＝1，

其中 det(k)表 K 之行列式，gcd 表最大公因數，上述條件確保 $K^{-1}$ 存在，

$K^{-1}K = KK^{-1} = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$。

再介紹另一運算：mod，A＝B(mod n)表 A－B 可被 n 整除，則加密過程如下：

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 5 \\ 17 \end{bmatrix}$（假設讀者知道矩陣之乘法運算）

↑金匙 ↑明文 ↑密文

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 19 \\ 0 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ 10 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 8 \\ 4 \end{bmatrix}$

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 5 \\ 17 \end{bmatrix}$

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 3 \\ 0 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 6 \\ 9 \end{bmatrix}$

$\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 22 \\ 13 \end{bmatrix}(\text{mod}26) = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$

故可得密文組數值為：

5 17　12 5　8 4　5 17　6 9　5 1

再將其轉換成對應之英文字母，則得密文如下：

FR　MF　IE　FR　GJ　FB

接收端得到此密文如還原明文呢？

在傳統密碼學中，發送及接收兩端皆須擁有金匙 $K=\begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}$，

而當接收端擁有金匙 $K=\begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}$，其可求得 $K^{-1}=\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}$，

因 $KK^{-1}=K^{-1}K=I_2 \pmod{26}$，接收端可利用金匙 $K^{-1}$ 解密還原明文如下：

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}5\\ 17\end{bmatrix}(\text{mod}26)=\begin{bmatrix}-26\\ 19\end{bmatrix}(\text{mod}26)=\begin{bmatrix}0\\ 19\end{bmatrix}$$

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}12\\ 5\end{bmatrix}(\text{mod}26)=\begin{bmatrix}45\\ -26\end{bmatrix}(\text{mod}26)=\begin{bmatrix}19\\ 0\end{bmatrix}$$

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}8\\ 4\end{bmatrix}(\text{mod}26)=\begin{bmatrix}28\\ -16\end{bmatrix}(\text{mod}26)=\begin{bmatrix}2\\ 10\end{bmatrix}$$

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}5\\ 17\end{bmatrix}(\text{mod}26)=\begin{bmatrix}-26\\ 19\end{bmatrix}(\text{mod}26)=\begin{bmatrix}0\\ 19\end{bmatrix}$$

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}6\\ 9\end{bmatrix}(\text{mod}26)=\begin{bmatrix}3\\ 0\end{bmatrix}$$

$$\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}\begin{bmatrix}5\\ 1\end{bmatrix}(\text{mod}26)=\begin{bmatrix}22\\ -13\end{bmatrix}(\text{mod}26)=\begin{bmatrix}22\\ 13\end{bmatrix}$$

故可得明文數值為：

0 19　19 0　2 10　0 19　3 0　22 13

再將數值組轉換成對應之英文字母，可得明文：

AT　TA　CK　AT　DA　WN

上面之演算流程皆按照開始之加密與解密架構圖進行。

最後，再整理上述之理論作為結語。

設 $\begin{bmatrix}P_1\\ P_2\end{bmatrix}$ 為明文，K 為金匙，則 $K\begin{bmatrix}P_1\\ P_2\end{bmatrix}=\begin{bmatrix}C_1\\ C_2\end{bmatrix}$ 為密文，此即為加密過程。

南台通識電子報
2011 年 7 月 15 日出版
南台科技大學通識教育中心 發行
27期

反之，因 $K^{-1}$ 存在，故解密過程如下：

$$K^{-1}\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = K^{-1}K\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = I_2\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$$

有興趣讀者可參考下列資料：

1. L. S. Hill “Concerning certain linear transformation apparatus of cryptography”, American Mathematical Monthly, volume 38 (1931), 135-154.
2. K. H. Rosen, “Elementary number theory and its application”, third edition, 1993.
3. D. E. Denning, “Cryptography and data Security”, 1982.
4. 賴溪松等《近代密碼學及其應用》，松崗。