美國國家資料加密標準(Data Encryption Standard, DES)

一、傳統式加密：

自 1976 年提出公開金匙的觀念以後，公開金匙的發展便迅速蓬勃發展起來，而到了現在已經幾乎是現代密碼學的主流了。但公開金匙密碼系統面臨著高運算量的問題，使得在實際運用時面臨著速度的問題。所以傳統密碼系統由於其加解密的速度比公開金匙密碼系統的速度快了許多，在現代密碼學中仍然有著非常重要的地位，其中美國國家資料加密標準（Data Encryption standard, DES）密碼系統就是傳統密碼系統的一個典型代表。

傳統式密碼系統主要由兩個動作所組成，一是換位(Transposition)，一是代換(Substitution)。不論多麼複雜的傳統密碼系統絕對脫離不了這兩個基本的`動作。

二、**換位式加密法** (Transposition)：

換位式加密法基本精神是依照某個特定的規則來重新排列明文。也就是擾亂明文間的順序。

例如：

STRIKE WHILE THE IRON IS HOT

經過一個簡單的換位後可得

TOH SI NORI EHT ELIHW EKIRTS

其中的關聯就是將明文以相反的順序重寫而已。

三、**替換式加密法** (Substitution)：

替換式加密法的基本精神和換位式加密法完全不同，對於明文的每一個字母並不去改變它的位置，只是將它以其他的符號代替。

例如：

原字母 ：ABCDEFGHIJKLMNOPQRSTUVWXYZ

替代字母：ZYXWVUTSRQPONMLKJIHGFEDCBA

所以若明文為

FAITH CAN MOVE MOUNTAINS

密文則為

UZRGS XZM NLEV NLFMGZRMH

四、美國國家資料加密標準 (DES)

美國國家資料加密標準（Data Encryption standard, DES）為 1970 年由 IBM 公司所發展出來，且在 1977 年被美國政府用作為全國資訊保密標準的一個密碼系統，也是乘積式密碼系統最有名的一個代表系統。直到今日，儘管 DES 已經經歷了二十個年頭，在已知的公開文獻中，仍是無法完全的、徹底的把 DES 給破解掉。所以這套密碼系統仍是被公認安全的。

DES 系統為一區塊式的密碼系統，而**區塊式加密系統**就是對一定大小的明文或密文來

加密或解密。所以在 DES 的系統中將明文分為許多 64 位元之區塊，每個區塊再經由密碼系統作加解密處理；所以 DES 密碼系統沒有密文擴充的問題，就一般資料而言，無論明文或密文大都大於 64 位元，所以只要將明文(或密文)中每 64 個位元加以切割，對每一個區塊加密或解密就可以了。

當最後一個切割區塊小於 64 位元時則在使區塊之後加上'0'位元，直到此區塊的大小滿足 64 位元為止。

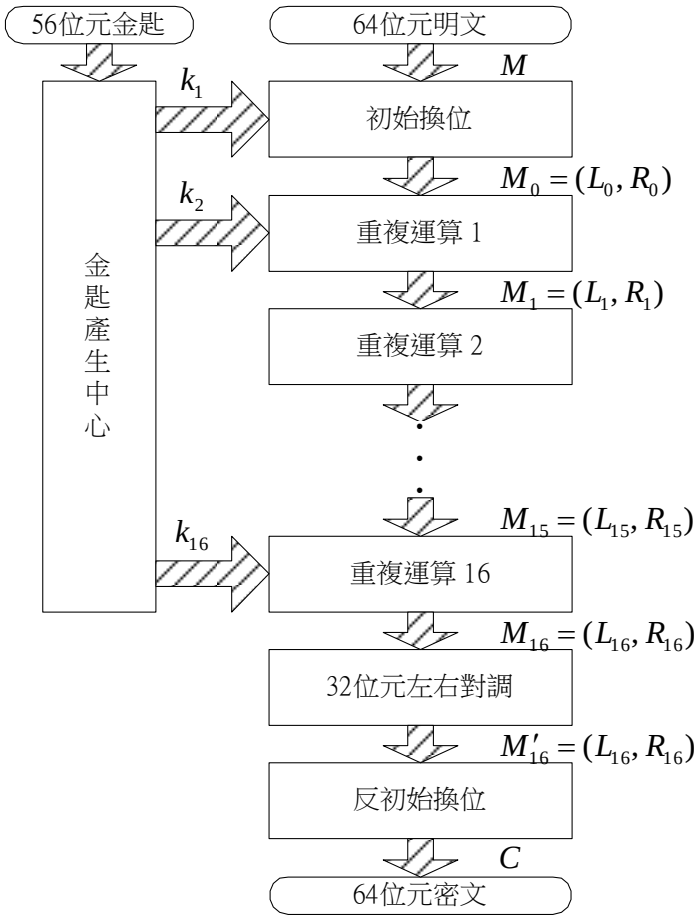
DES 所用的加密或解密的金匙(Key)也是 64 位元，但其中有 8 位元用來做錯誤更正(Error Correction)，所以 64 位元中真正有效的位元只有 56 位元。

DES 密碼系統包含了三個部分：

1. 一個 56 位元金匙轉換為 16 個 48 位元金匙的金匙產生中心。
2. 一組換位系統—初始換位（Initial permutation, IP）與反初始換位(Inverse permutation, IP^{-1})。
3. 以及 16 個金匙所做的 16 次重複運算。

五、DES 演算法：

下圖是 DES 的加／解密架構圖：



DES 系統主要架構

其最上方的 64 位元輸入區塊可能是密文也有可能是明文，端看使用者要加密或是解密而定。而加解密的不同只在於圖右邊的 16 個子金匙的使用順序不同而已。

六、初始換位與反初始換位

DES 密碼系統在最開始有一個初始換位用來將明文的 64 個位元來做換位，最後也有一個對應的反初始換位，原始 DES 系統換位的方法如表一：

表一：

58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25
初始換位	反初始換位

上圖將 64 個位元由左而右由上而下表示，每個數字代表將要移到的目標。換句話說，對整個系統而言，此一部份可以獨立出來設成其他不同的換位方式。換句話說，初始換位及反初始換位可以是不同的排列表。

七、金匙產生中心

金匙產生中心負責將密碼系統之 56 位元金匙轉換成 16 個 48 位元表示的金匙供系統之 16 個不同的重複運算所使用。

在金匙產生的過程中，56 位元之系統金匙經由換位選擇運算，如表二金匙排列 A 的換位後產生一 56 位元之 LK_0，再經由 16 個不同的移位運算來分別產生 16 個 56 位元運算的 LK1、LK_2….LK_{16} 等，而 LK_1、LK_2….LK_{16} 再經由換位選擇運算，如表二金匙排列 B 的換位與縮減後變成 16 個供重複運算使用的 48 位金匙，k_1、k_2….k_{16}；16 個移位運算 LS 之左移次數均各有不同可以參考左旋函數(表三)。

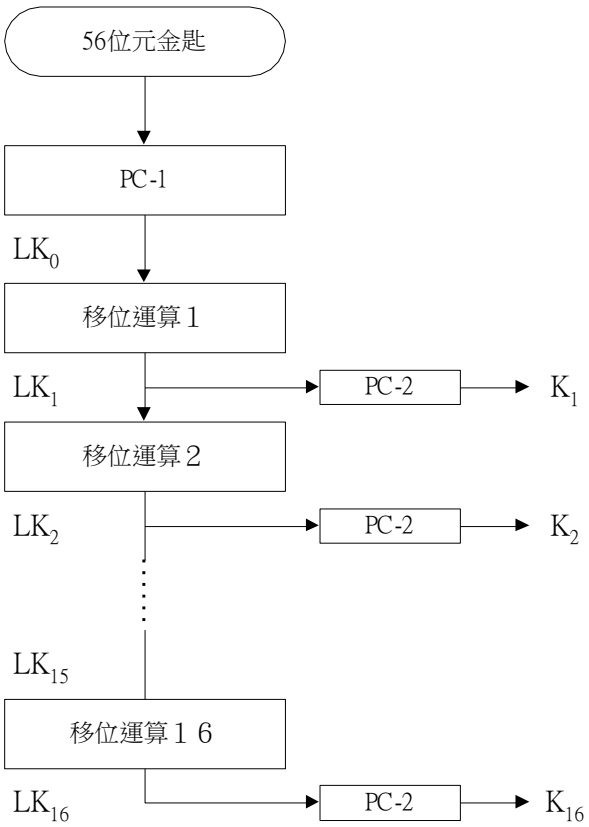
表二：

金匙排列 A	金匙排列 B
57 49 41 33 25 17 09	14 17 11 24 01 05
01 58 50 42 34 26 18	03 28 15 06 21 10
10 02 59 51 43 35 27	23 19 12 04 26 07
19 11 03 60 52 44 36	16 07 27 20 13 02
63 55 47 39 31 23 15	41 52 31 37 47 55
07 62 54 46 .8 30 22	30 40 51 45 33 48
14 06 61 53 45 37 29	44 49 39 56 34 53
21 13 05 28 20 12 04	46 42 50 36 29 32

表三：

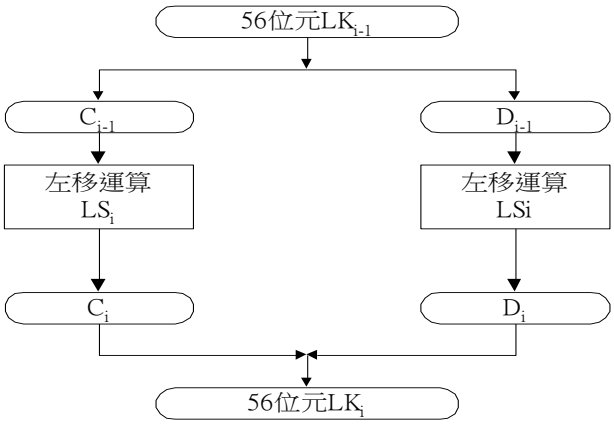
左移函數							
回數	左旋位數	回數	左旋位數	回數	左旋位數	回數	左旋位數
1	1	5	2	9	1	13	2
2	1	6	2	10	2	14	2
3	2	7	2	11	2	15	2
4	2	8	2	12	2	16	1

金匙產生的過程中的輸入，為使用者所持有的 64 位元母金匙。而加密或解密時，使用者先將母金匙輸入子金匙的產生流程中即可。



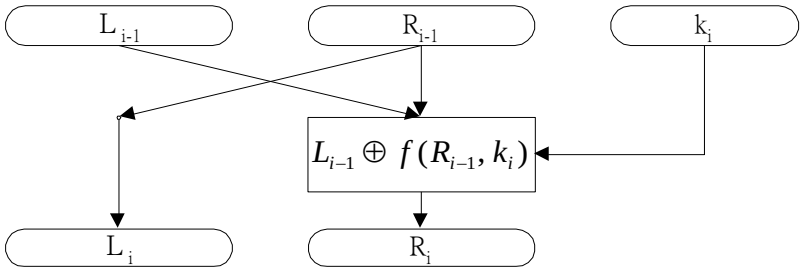
金匙產生之主架構

八、DES 密碼系統主體——16 次重複運算



移位運算 i

DES 密碼系統的主體為 16 次使用不同金匙的重複運算，這些重複運算的內容如下：



$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

重複運算 i之內部功能

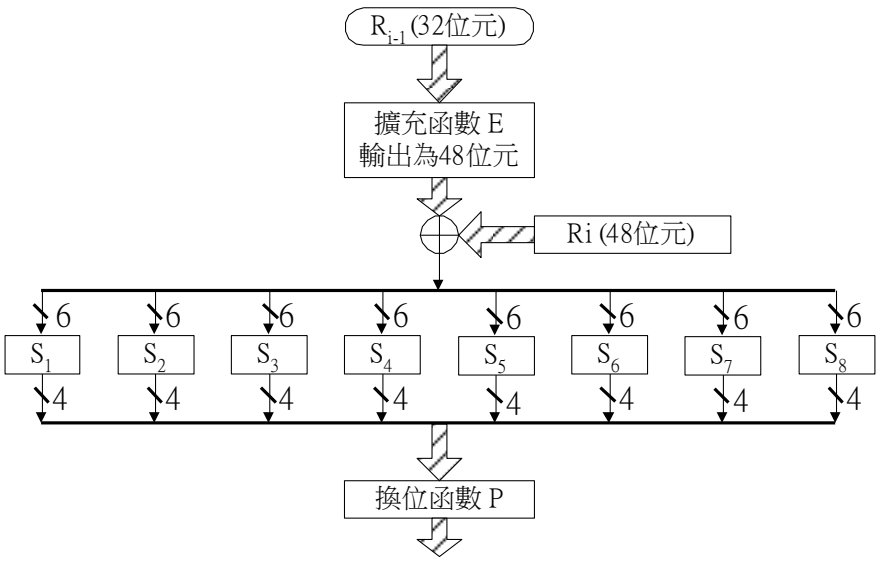
上圖表示將上次運算之 64 位元運算結果分為左右兩部分，右半部分移作下次,重複運算之左半部，此外將右半部分再與由金匙中心所產生之 48 位元金匙經 $f(R_{i-1}, k_i)$ 運算後，再與左半部作互斥運算後做為下次重複運算之右半部分。

九、 f 函數：

f 函數是整各 DES 密碼系統中最重要的部分，而其中的重點又在替換盒(Substitution Boxes)，下圖為 f 函數的計算過程架構。 f 函數有兩個輸入資料：一個為 32 位元的中間密文 R，另一個為 48 位元的金匙 K。

函數 $f(R_{i-1}, k_i)$ 主要是將 32 位元的中間密文 R 右半部份經由擴充換位函數 E(如表四)轉換成為 48 位元。

接著，再與另一輸入資料，及 48 位元金匙做互斥或(XOR)運算後分成八個 6 位元的替換盒 S_1、S_2….S_8 輸入資料。然後經由替換盒，S_1、S_2….S_8 轉換成八個 4 位元的輸出，$4 \times 8 = 32$ 個位元，即又變成 32 位元，最後經由換位函數 P(如表四)縮減為 32 位元的結果，這就是 f 函數。



$f(R_{i-1}, k_i)$結果,輸出為32位元

表四：

擴增排列 E
32 01 02 03 04 05
04 05 06 07 08 09
08 09 10 11 12 13
12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 01

換位函數 P
16 07 20 21
29 12 28 17
01 15 23 26
05 18 31 10
02 08 24 14
32 27 03 09
19 13 30 06
22 11 04 25

九、解密說明：

DES 密碼系統在 16 個重複運算後有一個將左右兩部分對調的動作，最主要的原因是為了了解使解密也能使用同樣的演算法。換句話說，解密的步驟和加密的步驟相同；亦即我們需將密文先做初始換位，再經過 16 次重複運算步驟而這 16 次重複運算所使用的金匙依序須為 k_{16}、k_{15}….k_1，最後將左右兩部分對調後再做反初始換位運算即可得到原來知明文。這樣才是真正加密的反運算。

十、DES 的安全性

1. 弱金匙(Weak Key)：

所謂的弱金匙是指所有可能的金匙中，有幾個特別的金匙會降低 DES 的安全性，所以使用者要避免使用這幾個弱金匙。而弱金匙的產生原因是由於子金匙產生過程的設計不當所引起的。

弱金匙的特性：

I. 為某個母金匙經過金匙排列後會產生 16 一模一樣的子金匙。如此一來將會大大的降低 DES 的安全性。如下表五：

表五：

DES 的 4 個弱金匙	
1	0101 0101 0101 0101
2	FEFE FEFE FEFE FEFE
3	1F1F 1F1F 1F1F 1F1F
4	E0E0 E0E0 E0E0 E0E0

II. 對弱金匙而言，其加密解密的過程是完全一樣的。我們知道 DES 的加密與解密的過程中，唯一不同的是子金匙的使用順序是完全相反的。然而對弱金匙而言，因為衍生的 16 個金匙是玩相同的，故金匙之間就毫無順序而言了。

2. 半弱金匙(Semi-Weak Key)

弱母金匙所產生的子金匙恰好之有兩種，而每一種可能的子金匙剛好各出現八次，則此種金匙則稱為半弱金匙。如表六：

表六：

DES 所有的半弱金匙			
01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FE1F	FE1F	FE0E	FE0E
1F01	1F01	0E01	0E01
FEE0	FEE0	FEF1	FEF1

3. DES 的互補性(Complement)

在 DES 的明文 m，密文 C 與金匙 K 之中存在著互補的特性。簡單的說：

若 $E_K(M)=C$ 則 $E_T(m)=E_{\bar{K}}(\bar{m})$

這個性質使得破解者 A 欲破解使用 B 的金匙 K，而 A 有擁有 B 使用金匙 K 對明文 m 及 $\bar{m}$ 加密的密文 $E_K(m)$ 及 $E_K(\bar{m})$，則 a 可以利用 DES 的互補性來找出金匙 K。此比完全搜尋(Exhaustive Search)破解少花了一半的時間(共時間複雜 2^{55})，下列為 A 如何找出金匙 K 的破解法：

a. A 先將所有的金匙每兩個歸為一對，其中同一對的兩個金匙互為 1 的補數，如此共有 2^{55} 對。

b. A 從尚未測試的金匙對中，挑出一個金匙 T，並對明文 m 加密，得到密文 $E_T(m)$。

c. 若 $E_T(m)=E_K(m)$，則 $T=K$；否則 $E_T(m)=E_{\bar{K}}(\bar{m})$，$\bar{T}=K$

d. 若 c 的兩個狀況都不成立，則表示 $T\neq K$ 且 $\bar{T}\neq K$，那麼就回到 b 重新測試。

4. 替換盒的設計原則

a. 對任一個替換盒而言，沒有任何線性方程式能等價(Equivalence)於此一替換盒的輸出入關係。也就是說替換盒為非線性函數。

b. 改變替換盒的任一位元的輸入，則至少有兩個以上的輸出位元會有所改變。

c. 當某一固定位元的輸入時，我們希望替換盒的四個輸出位元之間的 0 與 1 個數之差別愈小愈好。

5. DES 的 16 個回合

1990 年 Eli Biham 及 Adi Shamir 公開了一種極具破壞力的破解法—差分密碼分析(Differential Cryptanalysis)。他們能證明任何少於 16 回合的 DES 版本，差分分析法的時間複雜度都小於完全搜尋的時間複雜度。

6. 差分攻擊法

差分攻擊法基本上屬於明文攻擊法，在某些特定的情形下也可以用於已知明文的攻

擊。簡單的說，分析特殊明文配對(Plaintext Pair)的差值對於其所對應的密文配對(Ciphertext Pair)之差值所產生的影響。

差值所指的是兩個明文(或密文)之間所做的互斥或(XOR)所得到的值。例如：

$A=10011111_2$

$B=10110001_2$

則 A 與 B 的差值為 00101110_2

而某些特殊的差值會有很高的機率出現在密文配對上，我們稱此為特徵值(Characteristic)。差分密碼分析法就是選擇許多擁有相同特徵的明文配對，加密後得到相應的密文配對，再藉著特徵值與這些密文配對推導出一些可能的金匙，並賦予可能的機率，最後再選出最有可能者。

十一、結論：

DES 密碼系統可說是傳統密碼系統非常典型的一個代表作，許多專家學者對其保密度提出質疑，由於沒有提出確切的破密方法，加上無論以軟、硬體來設計都有非常快的速度，所以如果所保密文件的保密度不是非常要求嚴苛的話，DES 密碼系統為一可行的系統。