实验原理

## 一．单表置换密码

单表置换密码也是一种传统的代替密码算法，在算法中维护着一个置换表，这个置换表记录了明文和密文的对照关系。当没有发生加密（即没有发生置换）之前，其置换表如5-2-1所示。

表5-2-1　置换表

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

在单表置换算法中，密钥是由一组英文字符和空格组成的，称之为密钥词组，例如当输入密钥词组：I LOVE MY COUNTRY后，对应的置换表如表5-2-2所示。

表5-2-2　置换表

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | L | O | V | E | M | Y | C | U | N | T | R | A |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| B | D | F | G | H | J | K | P | Q | S | W | X | Z |

在表5-2-2中 ILOVEMYCUNTR是密钥词组I LOVE MY COUNTRY略去前面已出现过的字符O和Y依次写下的。后面ABD……WXZ则是密钥词组中未出现的字母按照英文字母表顺序排列成的，密钥词组可作为密码的标志，记住这个密钥词组就能掌握字母加密置换的全过程。

这样对于明文：data security has evolved rapidly，按照表5-2-2的置换关系，就可以得到密文：VIKI JEOPHUKX CIJ EQDRQEV HIFUVRX。