M. SATHISH KUMAR
E0119052

# DESIGN & Analysis of Algorithms

## CONTINUOS ASSESSMENT - II

1. * Longest Common Sequence :

$P_1 = \alpha = (a\,b\,b\,c\,a)$

$P_2 = \beta = (b\,b\,c\,b\,a)$

* Algorithm :-

$m$ = length of $P_1$

$n$ - length of $P_2$

for $i \leftarrow 0$ to $m$ do $(len[i, 0]) = 0$

for $j \leftarrow 0$ to $n$ do $(len[0, j]) = 0$

Length (A, B).

for $i \leftarrow i$ to $m$

for $S \leftarrow 1$ to $n$ do

if $\alpha_i = \beta_j$ then

$\begin{bmatrix} len[i, j] = 1 + len[i-1, j-1] \\ prev(i, j) = \text{"}\nwarrow\text{"} \end{bmatrix}$

elseif

len $(i-1, j) \geq$ len $i, j-1)$

len $(i, j)$ = len $(i-1, j)$

prev $(i, j)$ = "$\uparrow$"

else :

len (i, j) ← len (i, j - 1)

print (i, j) = "←"

return len and prev

**Backtracking Algorithm:**

Output - LCS (A, prev, i, j)

if i = 0 or j = 0 then return

if prev (i, j) = "↖" then

[output -LCS (A, prev, i-1, j-1)]

print $a_i$

else if prev (i, j) = "↑" then

output - LCS (A, prev, i-1, j)

else Output - LCS (A, prev, i, j-1).

**Complexity for optimal substructure**

Time complexity : O(mn) ; m = 4, n = 4)

Space complexity : O(mn)

**Complexity for brute force approach:**

Time complexity : ~~O(n²)~~ O( n × $2^n$)

Space complexity : O(mn)

In brute force approach time taken is more than optimal

| | 0 | [a] 1 | [b] 2 | [b] 3 | [c] 4 | [a] 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| [b] 1 | 0 | 0 ↑ | 1 ↖ | 1 ↖ | 1 ← | 1 ← |
| [b] 2 | 0 | 0 ↑ | 1 ↖ | 2 ↖ | 2 ← | 2 ← |
| [c] 3 | 0 | 0 ↑ | 1 ↑ | 2 ↑ | 3 ↖ | 3 ← |
| [b] 4 | 0 | 0 ↑ | 1 ↖ | 2 ↖ | 3 ↑ | 3 ↑ |
| [a] 5 | 0 | 1 ↖ | 1 ↑ | 2 ↑ | 3 ↑ | 4 ↖ |

**Verification:**

a b b c a

b b c b a $\Rightarrow$ bbca

**Largest Sequence:** bbca

---

2. $k$ = JAVA

$$k = \begin{bmatrix} 2 & 14 \\ 3 & 4 \end{bmatrix}$$

$$\text{Diagraph Matrix} = \begin{bmatrix} 9 & 21 \\ 0 & 0 \end{bmatrix}$$

**Encryption:**

$$C = KP \bmod 26$$

| 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 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

**Encryption :**

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 2 & 14 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 9 & 21 \\ 0 & 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 & 14 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 9 & 21 \\ 0 & 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 & 42 \\ 27 & 63 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 & 16 \\ 1 & 11 \end{bmatrix}$$

$$C = \begin{bmatrix} S & Q \\ B & L \end{bmatrix} \Rightarrow SBQL$$

**Decryption :**

$$K^{-1} = \begin{bmatrix} 4 & -14 \\ -3 & 2 \end{bmatrix} \left( \frac{1}{-34} \right)$$

$$= -\frac{1}{34} \begin{bmatrix} 4 & -14 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 18 & 16 \\ 1 & 11 \end{bmatrix} \bmod 26$$

$$= 34^{-1} \bmod 26$$

$$= 391$$

$$P = \frac{1}{34}\begin{bmatrix} 4 & -14 \\ -3 & 2 \end{bmatrix}\begin{bmatrix} 18 \\ 1 \end{bmatrix} \bmod 26$$

$$= \frac{1}{-34}\begin{bmatrix} 58 \\ -52 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} -\frac{29}{17} \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} -66\,9 \bmod 26 \\ 59\,8 \bmod 26 \end{bmatrix}$$

$$= \begin{bmatrix} 9 \\ 0 \end{bmatrix} = \begin{bmatrix} J \\ A \end{bmatrix}$$

* multipliplication inverse of 17 is 23

$$\Rightarrow \begin{bmatrix} 45 \times 23 \\ 13 \times 23 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 21 \\ 13 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} V \\ N \end{bmatrix}$$

So after decryption $\boxed{\begin{bmatrix} J \\ A \end{bmatrix}\begin{bmatrix} V \\ N \end{bmatrix}}$

3. Base value $(g) = 5$

prime number $(q) = 23$

Secret key : $X_{Adam} = 13$

$X_{Alam} = 2$

Public key :

$Y_{Adam} = 5^{13} \bmod 23$

$= (5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5) \bmod 23$

$= (5^2 \bmod 23) \times (5^2 \bmod 23) \times (5^2 \bmod 23) \times (5^2 \bmod 23) \times (5^2 \bmod 23) \bmod 23$

$= (2 \times 2 \times \times 2 \times 2 \times 2 \times 2 \times 5) \bmod 23$

$= (32 \times 10) \bmod 23$

$= (32 \bmod 23) \times (10 \bmod 23) \bmod 23$

$= (11 \times 10) \bmod 23$

$Y_{Adam} = 18$

$Y_{Alam} = ((5^2) \bmod 23)$

$Y_{Alam} = 2$

Shared Session :

$K_{AB} \Rightarrow$ Shared Session of Alam and Adam

$$K_{AB} = g^{x_A x_B} \bmod q$$

$$K_{AB} = y_{Adam}^{x_{Alam}} \bmod q$$

$$= 18^2 \bmod 23$$

$$= (9^2 \times 2^2) \bmod 23$$

$$= ((3 \times 3)^2 \times 2^2) \bmod 23$$

$$= (3^3 \times 12) \bmod 23$$

$$= (27 \bmod 23) \times (12 \bmod 23) \bmod 23$$

$$= (4 \times 12) \bmod 23$$

$$= 2$$

$$K_{AB} : y_{Alam}^{x_{Adam}} \bmod 23$$

$$= 2^{13} \bmod 23$$

$$= (2^2 \times 2^2 \times 2^2 \times 2^2 \times 2^2 \times 2^2 \times 2) \bmod 23$$

$$= (2^6 \bmod 23) \times (2^6 \bmod 23) \times (2 \bmod 23)) \bmod 23$$

$$= (18 \times 18 \times 2) \bmod 23$$

Both Adam and Alan have

$K_{AB} = g^{X_A \cdot X_B} \bmod q$

$X_A$ = Adam
$X_B$ = Alan

$= 5^{13 \times 2} \bmod 23$

$= (5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2 \times 5^2) \bmod 23$

$= (2^2 \times 2^2 \times 2^2 \times 2^2 \times 5^2 \times 2^2 \times 2) \bmod 23$

$\boxed{= 4}$

Compared shared key of both we get 4 as $K_{AB}$.

The D-H algorithm is useful as it is assymetric with public and private secret keys and one shared session key which is secure. But sometime "man-in-the-middle attack" occurs when a third gets intercepts the keys b/w person 1 and person 2 and will be able to forward all replies between them.