CHAPTER FOUR

CRYPTANALYSIS OF TRANSPOSITION CIPHER PROBLEMS USING COMBINATORIAL OPTIMIZATION PROBLEMS TECHNIQUES

4.6 Applying Exact Methods with SR to Solve TCP

4.6.1 Applying CEM with SR to Solve TCP

Notice from table (4.15) that if $m \le 9$ we can apply CEM to solve TCP with n=11,…,17, to obtain exact solution in reasonable time. To find ADK for each n mentioned in table (4.15) we have to apply CEM for $m \le 9$. The CEM applied for σ of n-sequences consists of m-subsequence to obtain π of m-sequences where some subsequence is multi digits, then we called it **multi digits CEM** (**MDCEM**). Now we can propose a subalgorithm MDCEM:

Subalgorithm MDCEM

READ n, m, k=1,…,m, (SL_k, S_k).

MDCEM=CEM(m, SL_k, S_k).

Table (4.16) shows the results of applying MDCEM with SR using table (4.15) for n=11,…,17, and L=1000, RT(m) and ERT(n) are the required and expected required time in seconds respectively.

Table (4.16): The results of applying MDCEM with SR for n=11,…,17.

N	m	m!	ADK, SOF(ADK)≈1.72	MDCEM	
				RT(m)	ERT(n)
11	3	6	(2-11-7-9, 4-1-10 ,6-3-8-5)	0.02	10991≈3h
12	4	24	(2-12-7, 9-5, 1-10-6, 3-8-4-11)	0.04	34638≈10h
13	5	120	(2-13, 7-10-5-1, 11-6-3, 9-4-12, 8)	0.16	91940≈25h
14	6	720	(2-14-8, 11-5, 1-12, 7, 3-10-4, 13-9-6)	1.41	215228≈60h
15	7	5040	(3-15, 9, 11-6, 1-13-8, 4-10, 5-14, 12-2-7)	9.69	------
16	8	40320	(3, 16-9-12, 6-1, 14-8, 4, 11-5-15, 13-2, 7-10)	76.09	------
17	9	362880	(3-17-9, 13, 6-1,15-8, 4-11-5, 16, 14-2, 7,10-12)	658.8	------

4.6.2 Applying New BAB with SR to Solve TCP

As well known, each arc in classical search tree of BAB method represents by single digit of n-sequence, and then branching from a node. We can exploit the SR to decrease the number of levels in BAB's search tree and solve a TCP with m-1 levels instead of n-1 levels by obtaining sequences π of m-sequence. To make this happen we have to consider each arc as a string S_k of digits with length SL_k.

Now we want to exploit the SR to construct a new style of BAB search tree. Each arc of BAB search tree may represents a subsequence of the main sequence. In section (4.3.2) we propose a new BAB method and called it MBAB, this method will be applied to find sequences π of m-sequence with elements S_k. We call the new BAB method by **multi digits BAB** (MDBAB) method, which is shown below.

Algorithm (4.5): Multi Digits BAB (MDBAB) algorithm

STEP(1): **INPUT** CT, L, m;

LB=1.0,ℓ=0,sπ=(S_1,S_2,…,S_m),ND=m,(**FOR** k=1,…,m SEQ(k)=k);

STEP(2): ℓ= ℓ+1, j=0;

FOR k=1,…,ND

Branching from node last string ℓ in SEQ;

UNSEQ= sπ without SEQ;

π = concatenate(SEQ,UNSEQ);

Calculate UB_k= SOF(π) {*in level* –ℓ }

IF $UB_k \geq$ LB **THEN**

j = j + 1;

LIST(j , :) = σ; SUB(j) = UB_k;

END;

END;

STEP(3): LB=mean {SUB};

BestFit = $\max_{1\leq i\leq j}\{SUB\}$, BestDK= LIST(i);

SEQ=cut from LIST first ℓ strings, LIST=Φ, SUB=Φ; ND=j;

IF ℓ=j-1 **STOP ELSE GOTO STEP(2)**;

IF BestFit ≥ 1.68 **STOP**;

STEP(4): **OUTPUT** BestFit, BestDK;

Example (4.3): Let n=6, (for any L) with σ of 6-sequence has SR with the following subsequencs:S_1=(1),S_2=(4), S_3=(3,5), S_4=(6,2), with lengths 1,1,2,2 respectively this mean m=4 and π=(S_1,S_2,S_3,S_4)=(1,4,3-5,6-2). First, set initial LB (ILB)=1.0.

For level 1: $UB_{\{1\}}$((1,4,3-5,6-2))=1.3513 (≥ILB), $UB_{\{4\}}$((4,1,3-5,6-2)) =1.2717,$UB_{\{3-5\}}$ ((3-5,1,4,6-2))=1.2281, $UB_{\{6-2\}}$((6-2,1,4,3-5))=1.3302, so we branch from the nodes with good UB's, the new LB_1=mean($UB_{\{1\}}$) =$UB_{\{1\}}$=1.3513.

For level 2: from node with $UB_{\{1\}}$, $UB_{\{4\}}$((1,4,3-5,6-2))=1.3513 (≥LB_1), $UB_{\{3-5\}}$ ((1,3-5,4,6-2))=1.2312, $UB_{\{6-2\}}$((1,6-2,4,3-5))=1.7187 (≥LB_1), so we branch from the nodes with $UB_{\{4\}}$=1.3513 and $UB_{\{6-2\}}$=1.7178, the new LB_2=mean($UB_{\{1\}}$,$UB_{\{6-2\}}$)=1.5350.

For level 3: from the node with $UB_{\{4\}}$, $UB_{\{3-5\}}$((1,4,3-5,6-2)) =1.3513 and $UB_{\{6-2\}}$((1,4,6-2,3-5))=1.3251. From node with $UB_{\{6-2\}}$, $UB_{\{4\}}$((1,6-2,4,3-5))=1.7187 ($\geq LB_2$) and $UB_{\{3-5\}}$((1,6-2,3-5,4))=1.3547 so the only $UB \geq LB_2$ is the one at node with $UB_{\{4\}}$ to obtain the best fitness = 1.7187 hence the sequence π=(1,6-2,4,3-5) is the ADK (see figure (4.5)).

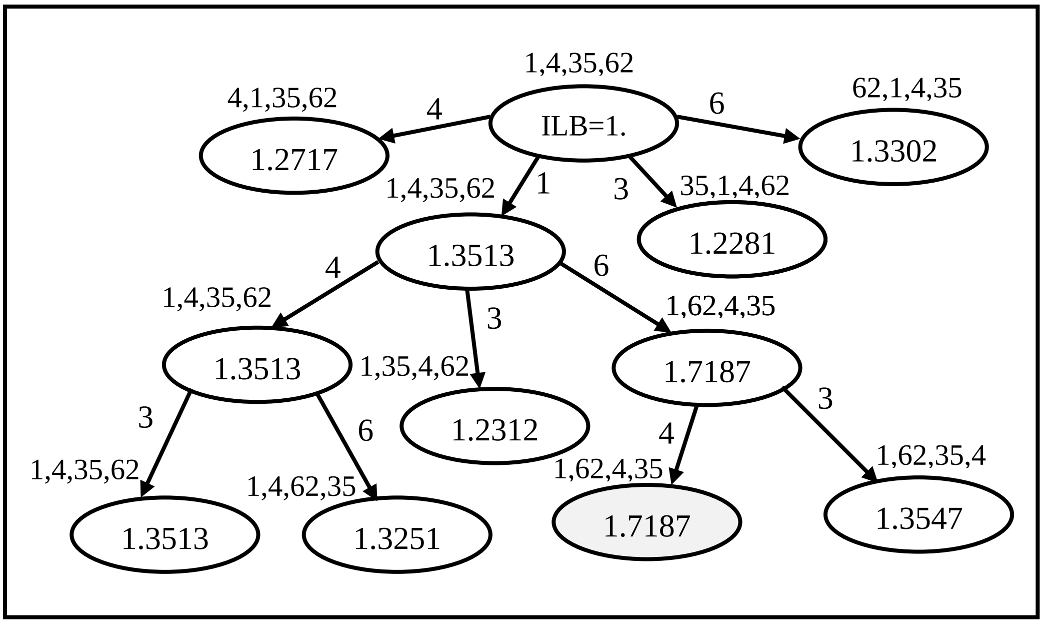

Figure (4.5): Applying of MDBAB for n=6.

From figure (4.5), the optimal solution is σ=(1,6,2,4,3,5), with SOF(6,σ)=1.7187. Since m=4, then the MDBAB search tree has 3 levels. The shaded node is the optimal solution.

Remark (4.3): For m≤9, if the current value of the upper bound $UB_k(\pi)\approx 1.7$ (which is the fitness of text using ADK) is obtained in any level k≤m when applying MDBAB we can stop the process and no need for more branching.

Now we can propose a subalgorithm MDBAB:

The RT(m) signed with * is the expected time which is interpolated by using Lagrange interpolation. Now we can propose a subalgorithm MDBAB:

Subalgorithm MDBAB

READ n,m,SL_k,S_k, k=1,…,m.

MDBAB=MBAB(m,SL_k,S_k)

4.7 The Construction of Cryptanalysis System for TCP

In this section, we will suggest a new cryptanalysis system for TCP using all the exact and local search methods mentioned above.

Now to apply MDCEM, we check if m less or equal to a reasonable number can be manipulated by MDCEM ($m \le 8$). While if ($8 < m \le 12$) we can applied MDBAB. From example (4.4), for key#8, m=4, so TCP can be solved by MDCEM in 4! (=24) states. Otherwise for (m>13), we reapplied SRKBA to solve TCP or to obtain more new ASR. These procedures are repeated until the TCP is solved.

We introduce subalgorithm **FIND_SR** to obtain the SR by applying CBA.

Subalgorithm FIND_SR

FOR i=1 : ss

  FOR j=1:n-1

    $n_1=Key_{i,j}$; $n_2=Key_{i,j+1}$;

    $N(n_1,n_2)+1$;

END {i,j};

Calculate $P(n_1,n_2)= N(n_1,n_2)/(ss*NG)$;

IF $P(n_1,n_2) \ge T_1$ **THEN FIND** (m,S_k), k=1,…,m;