Journal of Iraqi Al-Khwarizmi Society (JIKhS) Year 2018 pages: 246-254

Volume:2 Special issue of the first international scientific conference of Iraqi Al-Khawarizmi Society 28-29 March 2018

# Using the numerical solution for partial fractional differential equation by ADI numerical method to cryptography in Hill matrixes system

Hanan Abdaljabar Assad Al-Ukaily

Department of mathematical, College of Education for Pure Science, Tikrit University

## Abstract:

Fractional calculus is the subject of evaluating derivatives and integrals of non-integer orders of a given function, fractional differential equations is the subject of studying the solution of differential equations of fractional order is considered in this paper, which contain initial conditions. The general form of a fractional differentia equation is given by:

$y^{(q)} = f(x, y), y^{(q-k)}(x_0) = y_0$

where $k = 1, 2, \ldots, n + 1$, $n < q < n + 1$, and n is an integer number. The solution of fractional differential equations has so many difficulties in their analytic solution, therefore numerical methods may be in most cases be the suitable method of solution.

Therefore, the objective of this paper is to introduce and study a numerical solution by ADI methods for solving fractional differential equations.

Finally, we used the matrix optioned from this solution as a key matrix for cryptography the plaintext and transform it to cipher text by using the method of Hill matrices system.

**Keyword**: fractional partial differential equations, ADI methods, Hill matrix, cryptography.

## 1. Introdiction:

Fractional partial differential equation is an important modern mathematical science in fractional The concept of the differentiation operator $D = \frac{d}{dx}$ is familiar to all who have studied the elementary calculus and for suitable functions f the nth derivative of f namely $D^n f(x) = \frac{d^n f(x)}{dx^n}$ is well defined provided that n is appositive integer. Fractional calculus is commonly called generalized differ-integration, which means an arbitrary order (real or complex) derivatives and integrals. The fractional differintegrations of the function of single variable and that of the functions of many variables can be unified without any trouble. That is, the classical integer order's differintegral is the special case of the fractional calculus, []. we deal with the unclassical methods in mathematics, so we use this branch to implement in cryptography science.

Let M is denote to the (clear Message) or : p (Plain text ) and C is cipher text and E is Encryption function the operations on message with the function we produce C . i.e. E(M) = C.

In cryptography, we should have three basic elements: Authentication, integrity and nonrepudiation.

## 2. Basic concept

### 2.1.Block ciphers

A bloke cipher is a function $E: \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ that takes two input, a k-bit key k and an l-bit "plaintext" M, to return an l-bit "ciphertext" $C = E(K, M)$. The key-length k and the block-length l are parameters associated to the bloke cipher and very from cipher to cipher, as of course dose the design of the algorithm itself . For each key, $K \in \{0,1\}^k$ we let $E_k:\{0,1\}^l \rightarrow \{0,1\}^l$ be the function defined by $E_k(M) = E(K,M)$. For any block cipher, and any key K, the function $E_k$ is a permutation on $\{0,1\}^n$. [ 2] [5]

### 2.2.Hill cipher:

In this method, we apply the following steps:

1-put the code for the Alphabetic letters as:

| 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 |

2- Substitute: the codes above for the plain text and in Key matrix where the Key matrix is non-singular ( i.e. $K^{-1}$ exists ).

3- Multiple K with the matrix of plaintext (M) i.e. K.M.

4- Apply Modular function (Mod 26).

5- Decode any number to letter in step 1 then we have cipher text.[2][3]

For example:

If the key Matrix or key word is (Hill) with $2 \times 2$ Matrix and the plaintext is (short example) then we have:

$$K = \begin{bmatrix} H & A \\ N & A \end{bmatrix}; P = \begin{bmatrix} f & a & t & o & a \\ r & c & i & n & l \end{bmatrix}$$

With the keyword in a matrix, we need to convert this into a key matrix. We do this by converting each letter into a number by its position in the alphabet (starting at 0). So, A = 0, B = 1, C= 2, D = 3, etc.

$$K = \begin{bmatrix} H & A \\ N & A \end{bmatrix} = \begin{bmatrix} 7 & 0 \\ 13 & 0 \end{bmatrix}$$ The key matrix (each letter of the keyword is converted to a number).

We now split the plaintext into digraphs, and write these as column vectors. That is, in the first column vector we write the first plaintext letter at the top, and the second letter at the bottom. Then we move to the next column vector,

i.e. $P = \begin{bmatrix} f & a & t & o & a \\ r & c & i & n & l \end{bmatrix} = \begin{bmatrix} 5 & 0 & 19 & 14 & 0 \\ 17 & 2 & 8 & 13 & 11 \end{bmatrix}$

To perform matrix multiplication we "combine" the top row of the key matrix with the column vector to get the top element of the resulting column vector and so on …

We use the algebraic rules $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$

We find $\begin{bmatrix} 7 & 0 \\ 13 & 0 \end{bmatrix}\begin{bmatrix} 5 \\ 17 \end{bmatrix} = \begin{bmatrix} 35 \\ 65 \end{bmatrix}$

Next we have to take each of these numbers, in our resultant column vector, modulo 26 (remember that mean divide by 26 and take the remainder).

$$\begin{bmatrix} 7 & 0 \\ 13 & 0 \end{bmatrix}\begin{bmatrix} 5 \\ 17 \end{bmatrix} = \begin{bmatrix} 35 \\ 65 \end{bmatrix} = \begin{bmatrix} 9 \\ 13 \end{bmatrix} mod26$$

Finally, we have to convert these numbers back to letters, so 9 becomes "J" and 13 becomes "N", and our first two letters of the ciphertext are "AP".

$$\begin{bmatrix} 7 & 0 \\ 13 & 0 \end{bmatrix}\begin{bmatrix} 5 \\ 17 \end{bmatrix} = \begin{bmatrix} 35 \\ 65 \end{bmatrix} = \begin{bmatrix} 9 \\ 13 \end{bmatrix} mod26 = \begin{bmatrix} J \\ N \end{bmatrix}$$

And a gain encryption process this gives us a final ciphertext "JNAADNUAAA".

**2.3.Alternating direction implicit (ADI) method:**

In mathematics, the Alternating direction implicit (ADI) method is a finite difference method for solving fractional partial differential equations .It is most not apply used to solve the problem of heat conduction or solving the fractional diffusion equations in two or more dimensions.[1]

The (ADI) method contains the following steps:

1- Applying the explicit alternating direction implicit (ADI) method for x-axis and, the implicit alternating direction implicit (ADI) method for y-axis

2- Solving the equation by the time (t).

3-from step (1) we obtain two equations, we apply the first equation on the points of rows first time and on the points of columns in second time, and iterate the some process on the second equation.

4- The equations from step (3) solved by using Tomas Algorithm Tridiagonal Matrix Algorithm (TDMA)(define bellow) or by grammar rule if the equation is more than five because it is difficult to find determined.

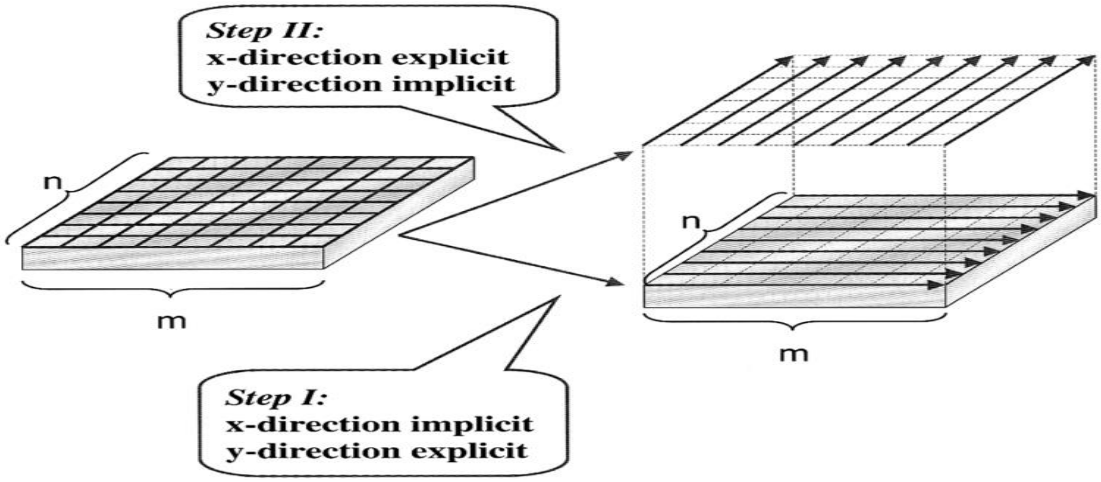


***Fig. 1. Illustration of the ADI method***

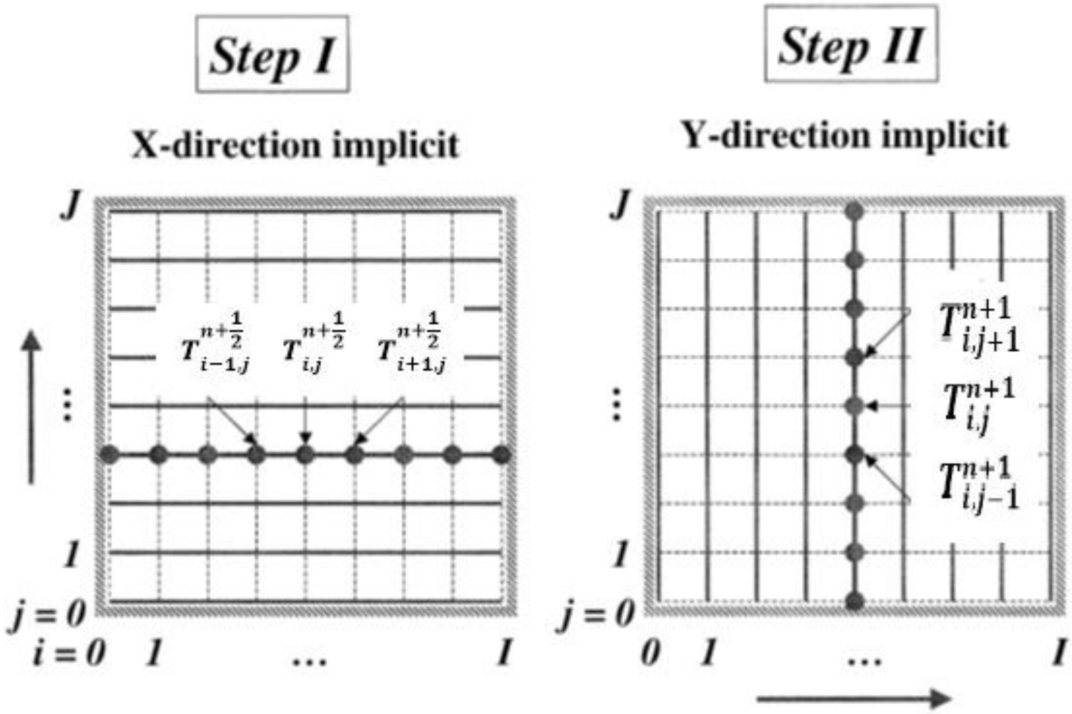
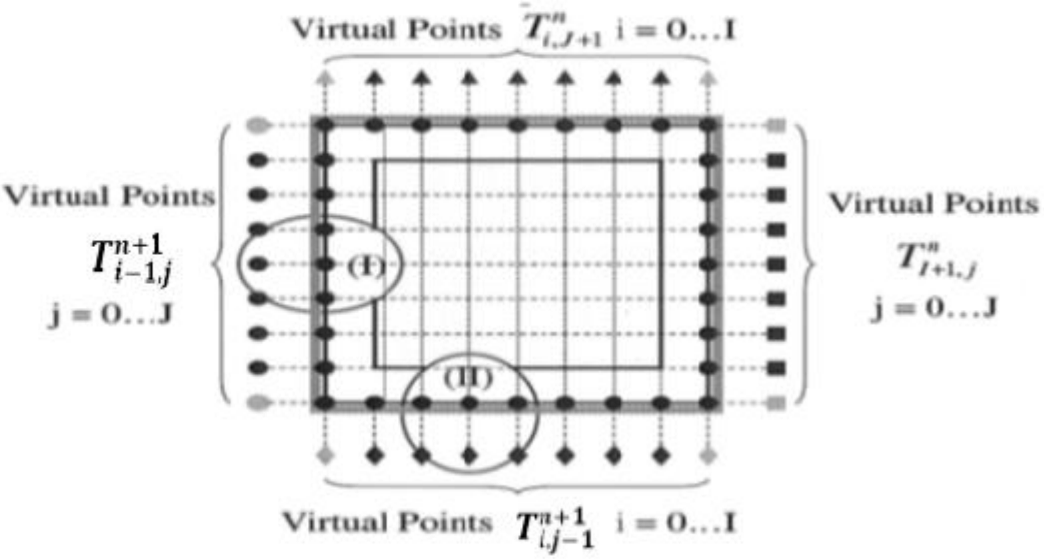


Fig. 2. For Step 1, the x-direction is implicit and the y-direction is explicit. For each j, there are I +1 equations corresponding to I +1 points. Note that each temperature point $T_{i,j}^{n+1/2}$ at value j is related to two unknowns $T_{i-1,j}^{n+1/2}$ and$T_{i+1,j}^{n+1/2}$ , which introduces a tridiagonal matrix for each j. Step 2 has a similar process to Step 1.



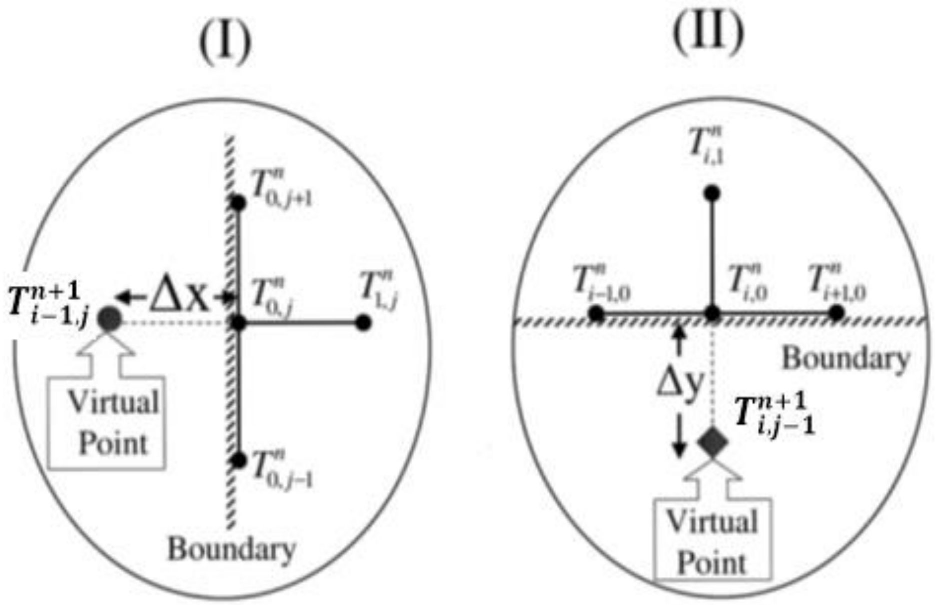


**Fig.3.Boundary conditions**

### 3. Application of ADI scheme for two-dimensional fractional diffusion for heat Flux equation:

Alternating direction implicit (ADI) method is an efficient method for the numerical solution of Fractional Parabolic Partial Differential Equations:

$$u_{i,j+1} = \mu s_{i,j_0} u_{i+1,j} + (1 - \mu s g_1) u_{i,j} + \mu s_{i,j} \sum_{k=0}^{i+1} g_k u_{i-k+1,j} \quad (1) \quad [1]$$

Here firstly we demonstrate its applicability with reference to the heat flux equation in two dimensions.[4]

$$\frac{\partial T(x,t)}{\partial t} - \alpha \frac{\partial^r T(x,t)}{\partial x^k} = 0 \quad , 0 \le r \le 1 \qquad (2)$$

together with the initial and boundary conditions:

$$T(x,0) = T_0(x) \quad \text{for } 0 \le x \le \infty$$
$$T(0,t) = 0 \quad \text{for } 0 \le t \le T$$
$$T(\infty,t) = 0 \quad \text{for } 0 \le t \le T$$

where $\frac{\partial^q u(x,t)}{\partial x^q}$ denote the left-handed partial fractional derivative of order q of the function u with respect to x and $0 < q \le 2.$

we use the explicit Alternating direction implicit (ADI) method to solve this initial-boundary value problem. To do this, we substitute t = $t_j$ ,let $\alpha = s(x,t)$ in equation (2) and replace the partial derivative $\frac{\partial u}{\partial t}$ with its approximation to get:

$$\frac{u(x,t_{j+1})-u(x,t_j)}{\Delta t}=s(x,t_j)\frac{\partial^q u(x,t)}{\partial x^q} \qquad (3)$$

where $t_j$ = jΔt, j=0,1,…, m and m is the number of subintervals of the interval [0, T].

Next, we recall the left-handed shifted Grünwald estimate to the left-handed derivative:

$$\frac{\partial^q u(x,t)}{\partial x^q}=\frac{1}{(\Delta x)^q}\sum_{k=0}^{\infty}\nu_k T(x-(k-1)\Delta x)$$

And we take n is the number of subintervals of the interval [0, $\infty$] and q is the fractional number re right up equation to came:

$$\frac{\partial^q u(x,t)}{\partial x^q}=\frac{1}{(\Delta x)^q}\sum_{k=0}^{n}\nu_k T(x-(k-1)\Delta x)$$

Therefore

$$\frac{\partial^q u(x_i,t_i)}{\partial {x_i}^q}=\frac{1}{(\Delta x)^q}\sum_{k=0}^{i+1}\nu_k u(x_i-(k-1)\Delta x,t_i)$$

Thus:

$$\frac{\partial^q u(x_i,t_i)}{\partial {x_i}^q}=\frac{1}{(\Delta x)^q}\sum_{k=0}^{i+1}\nu_k u_{i-k+1,j} \qquad (4)$$

Where $\nu_0 = 1$ and$\nu_k = (-1)k\frac{q(q-1)\ldots(q-k+1)}{k!}, k = 1,2,\ldots$ by substituting equation (4) in equation (3) one can have:

$$\frac{u_{i,j+1}-u_{i,j}}{\Delta t}=\frac{s_{i,j}}{(\Delta x)^q}\sum_{k=0}^{i+1}\nu_k u_{i-k+1,j}, i = 1,2,\ldots,n-1\ , j = 1,2,\ldots m-1$$

The resulting equation can be explicitly solved for $u_{i,j+1}$ to give:

$$u_{i,j+1}=\mu s_{i,j}\nu_0 u_{i+1,j}+(1-\mu s_{i,j}\nu_1)u_{i,j}+\mu s_{i,j}\sum_{k=0}^{i+1}\mu u_{i-k+1,j} \qquad (5)$$

Where $i = 1,2,\dots,n-1$ , $j = 1,2,\dots m-1$, $\mu = \frac{\Delta t}{(\Delta x)^q}$ , $s_{i,j} = s(x,t_j)$ and $u_{i,j}$ is the numerical solutions of equations (5) at each $(x_i, t_j), i = 1,2,\dots,n$ , $j = 1,2,\dots m$ such that $u_{1,0} = T(x_i)$ for $i = 1,2,\dots,n$ and $u_{0,j} = u_{n,j} = 0$ for $j = 1,2,\dots m.$

Now on simplifying Eq.(5) we have:

$$u_{i,j+1} = \mu s_{i,j}\nu_0 u_{i+1,j} + (1 - \mu s_{i,j}\nu_1)u_{i,j} + \mu s_{i,j}(\nu_0 u_{i+1,j} + \nu_1 u_{i,j} + \nu_2 u_{i-1,j} + \cdots + \nu_{i+1} u_{0,j})$$

$$u_{i,j+1} = 2\mu s_{i,j}\nu_0 u_{i+1,j} + u_{i,j} + \mu s_{i,j}\nu_2 u_{i-1,j} + \mu s_{i,j}\nu_3 u_{i-2,j} + \cdots + \mu s_{i,j}\nu_{i+1} u_{0,j}$$

Formula of equation (5) is also known as standard five point formula. We can rearrange formula of equation (5) in either of two ways:

$$2\mu s_{i,j}\nu_0 u_{i+1,j} + u_{i,j} + \mu s_{i,j}\nu_2 u_{i-1,j} + \mu s_{i,j}\nu_3 u_{i-2,j} + \cdots + \mu s_{i,j}\nu_{i+1} u_{0,j} = u_{i,j+1} \qquad (6)$$

$$u_{i,j+1} - u_{i,j} = 2\mu s_{i,j}\nu_0 u_{i+1,j} + \mu s_{i,j}\nu_2 u_{i-1,j} + \mu s_{i,j}\nu_3 u_{i-2,j} + \cdots + \mu s_{i,j}\nu_{i+1} u_{0,j} \qquad (7)$$

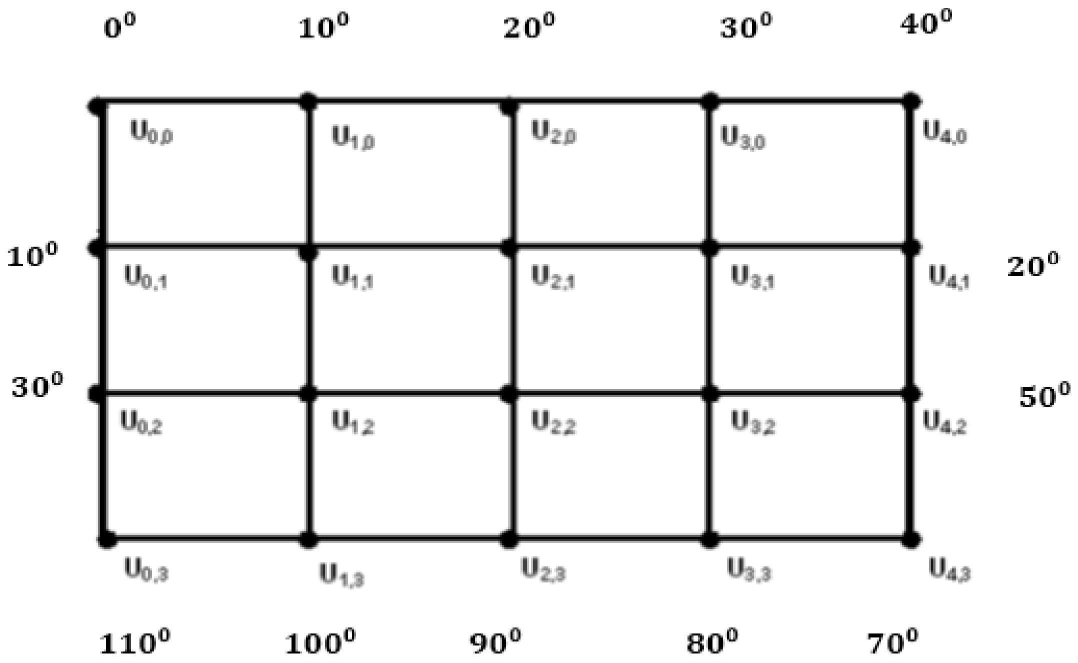
Since ADI is an iteration method, therefore formulae of equation (6) and (7) will be used as an iteration formulae:

$$2\mu s_{i,j}\nu_0 u_{i+1,j}^{(r+1)} + u_{i,j}^{(r+1)} + \mu s_{i,j}\nu_2 u_{i-1,j}^{(r+1)} + \mu s_{i,j}\nu_3 u_{i-2,j}^{(r+1)} + \cdots + \mu s_{i,j}\nu_{i+1} u_{0,j}^{(r+1)} = u_{i,j+1}^{(r)} \qquad (8)$$

$$u_{i,j+1}^{(r+2)} = 2\mu s_{i,j}\nu_0 u_{i+1,j}^{(r+1)} + u_{i,j}^{(r+2)} + \mu s_{i,j}\nu_2 u_{i-1,j}^{(r+1)} + \mu s_{i,j}\nu_3 u_{i-2,j}^{(r+1)} + \cdots + \mu s_{i,j}\nu_{i+1} u_{0,j}^{(r+1)} \qquad (9)$$

Example (2)

Consider a rectangle plate which is 16 inch wide and 12 inch high. Initially all points on the plate are at $50^0$ .The edges are suddenly brought to the temperature as shown in the Fig. (1) and held at these temperatures. Compute the heat transfer in the plate by using the Alternating Direction Implicit (ADI) method, assuming that the flux is only “X” and “Y” directions. Where $\alpha = 0.1516$ , $\Delta x = 4 = \Delta y.$



Solution

We solve above example in $[1]$ we get the solution matrix:

$$\begin{bmatrix} 0 & 10 & 20 & 30 & 40 \\ 10 & 97 & 62 & 44 & 20 \\ 30 & 109 & 83 & 61 & 50 \\ 110 & 100 & 90 & 80 & 70 \end{bmatrix}$$

Since we need a square matrix so we will take the key matrix of $(3 \times 3)$ by deleting the last two columns and last row by use concept block ciphers.

$$i.e.\, k = \begin{bmatrix} 0 & 10 & 20 \\ 10 & 97 & 62 \\ 30 & 109 & 83 \end{bmatrix} = \begin{bmatrix} 0 & 10 & 20 \\ 10 & 19 & 10 \\ 4 & 5 & 5 \end{bmatrix} mod 26.$$

Note if we need decipher we use $K^{-1}$ with the matrix of ciphertext.

## 4. Conclusion

In this paper, we find:

1- Two equation (6) and (7) is the general equation from the two equation (3.26) (3.27) from to $[1]$ it is used to find the numerical solution of partial fractional differential equation in two-dimensional fractional diffusion for heat Flux equation.

2- We used above two equation to solve the problem of diffusion the heat in finite pleat and we used the matrix solution as a key matrix to cipher the text and massage.

3- we use the fractional equation as a key matrix to cipher in first time state of ordinary equation .

## 5. Recommendation

We recommend another case in any fractional equation and we recommend to find the invers of key matrix to solve the code to return the basic text.

## 7. References

[1] Al-Ukaily,Hanan A., "Using (ADI) method to find a numerical solution of fractional partial differential equation" un published M.S.C. Tikrit University 2015.

[2] Bruce Schneier, John Wiley, and Sons, Inc. Applied cryptography, second Edition, ISBN.0471128457 Pub Data : 1/1/1996.

[3] G.B.AGNEW,"Random sources for cryptographic systems" Advances in cryptographic . EURO CRXPT 87 (LNCS 304) ,77-81, 1988.

[4] J.M .Angulo, M.D .Ruiz-Medina ,U.V.Anh,W Grecksch,Fractional diffusion and fractional heat equation, Adv.Appl.prob.32(2000) 1077-1099.

[5] M. Bellaro,J.Kilian,and P.Rogaway.the security of the cipher block chaining message authentication code. Journal of computer and system sciences, 61(3):362-399, December 2000.

[6] M.Abu Hammad, R.Khalil.conformable fractional heat differential equation,international Journal of pure and applied mathematics, valume 94, No.2,2014,215-221.