International Journal of Trend in Scientific Research and Development (IJTSRD)
Conference Issue | March 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Fostering Innovation, Integration and Inclusion Through Interdisciplinary Practices in Management

A Model for Encryption of a Text Phrase using Genetic Algorithm

Dr. Poornima G. Naik[1], Mr. Pandurang M. More[2], Dr. Girish R. Naik[3]

[1]Professor, [2]Research Student
[1]Department of Computer Studies, [3]Production Department
[1,2]Chhatrapati Shahu Institute of Business Education and Research, Kolhapur, Maharashtra, India
[3]KIT's College of Engineering Gokul Shirgaon, Kolhapur, Maharashtra, India

Organised By:
Management Department, Chhatrapati Shahu Institute of Business Education and Research, Kolhapur, Maharashtra

An Autonomous Institute Under UGC & Shivaji University College with Potential for Excellence (CPE) - III Phase.

How to cite this paper: Dr. Poornima G. Naik | Mr. Pandurang M. More | Dr. Girish R. Naik
Cite this article : Dr. Poornima G. Naik | Mr. Pandurang M. More | Dr. Girish R. Naik "A Model for Encryption of a Text Phrase using Genetic Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Special Issue | Fostering Innovation, Integration and Inclusion Through Interdisciplinary Practices in Management , March 2019, pp.53-58, URL: https://www.ijtsrd.com/papers/ijtsrd23063.pdf

IJTSRD23063

ABSTRACT

In any organization it is an essential task to protect the data from unauthorized users. Information Systems hardware, software, networks, and data resources need to be protected and secured to ensure quality, performance, and integrity. Security management deals with the accuracy, integrity, and safety of information resources. When effective security measures are in place, they can reduce errors, fraud, and losses. In the current work, the authors have proposed a model for encryption of a text phrase employing genetic algorithm. The entropy inherently available in genetic algorithm is exploited for introducing chaos in a text phrase thereby rendering it unreadable. The no of cross-over points and mutation points decides the strength of the algorithm. The prototype of the model is implemented for testing the operational feasibility of the model and the few test cases are presented

KEYWORDS: *Activity, Cross-over Points, Integrity, Mutation, Security, Vulnerability*

1. INTRODUCTION

In any organization it is an essential task to protect the data from unauthorized users. Information Systems hardware, software, networks, and data resources need to be protected and secured to ensure quality, performance, and integrity. Security management deals with the accuracy, integrity, and safety of information resources. When effective security measures are in place, they can reduce errors, fraud, and losses. The Internet is invaluable resource provider which at the same time increases the vulnerability of information systems and networks so that they can be used to facilitate attacks by criminals, unauthorized users and hackers. So, in order to overcome that problem the current research focuses on providing a solution in the form of some activity based authentication in distributed environments organization by suggesting and implementing few soft computing techniques.

In traditional organizations the manual systems enable access to the organizations private data by unauthorized users, hackers and crackers. The traditional system has many disadvantages since it is associated with high administrative responsibilities that has high possibilities of misuse of organizations important data with very low data security.

The distributed application designed with the help of soft computing techniques will help to provide high level security within particular organization. Another layer of security is added by a distributed environment. In the current research, a model for activity-based authentication is proposed. The model can be employed by any organization interested in protecting its confidential data. The model addresses all the issues pertaining to security from low security level to high security level. It protects information & transaction within organization against unauthorized users and it is only accessible to authorized users and due to that approach information remains secure. As authentication data is dynamic, time dependent and is frequently changing, it is extremely difficult for an intruder to gain an unauthorized access to the system. Soft computing techniques can increase accuracy, integrity, and safety of information resources.

Tools and Techniques Employed For Implementation of the Model:-

- Visual Basic Runtime Environment.
- JDK 1.5 and Java Runtime Environment.
- Extensible Markup Language (XML) with Document Type Definition (DTD) for implementation of generic framework.
- MS-Access for strong activity-based authentication data.
- ActiveX DLLs and OCX Custom controls for XML parsing and networking.
- 32-bit Data Source names for implementing business logic in middle-tier of 3-tier architecture using JDBC drivers for communication between data-tier and business-logic tier.

2. Literature Review

1. Method for biometric-based authentication in wireless communication for access control

A. Rudolf Maarten Bolle
B. Nalini Kant Ratha
C. Sharathchandra Pankanti

This research paper deals with storing of biometric data (on a database) over a network, poses addressing security issues that in extreme instances can be compromised. Significant security can be achieved if the biometric templates are stored locally in a portable device. A user can use the portable device to either transmit wirelessly the stored biometric data for authentication purposes, or a user can locally measure a biometric data using the portable device and match it against a biometric data which is also stored locally (in the portable device).

2. A Pattern Matching Model for Misuse Intrusion Detection

A. Sandeep Kumar
B. Eugene H. Spafford

This research paper describes a generic model of pattern matching that can be usefully applied to misuse of intrusion detection. The model is based on Colored Petri Nets. Guards define the context in which signatures are matched. The notion of start and final states, and paths between them define the set of event sequences matched by the net. Partial order matching can also be specified in this model. The main benefit of the model is its generality, portability and flexibility.

3. Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method.

A. Asaf Shabtai
B. Uri Kanonov
C. Yuval Elovici

In this paper, a new approach for detecting previously un-encountered malware targeting mobile device is proposed. In the proposed approach, time-stamped security data is continuously monitored within the target mobile device (i.e., smart phones, PDAs) and then processed by the Knowledge-Based Temporal Abstraction (KBTA) methodology. Using KBTA, continuously measured data (e.g., the number of sent SMSs) and events (e.g., software installation) are integrated with a mobile device security domain knowledge-base (i.e., an ontology for abstracting meaningful patterns from raw, time-oriented security data), to create higher level, time-oriented concepts and patterns, also known as temporal abstractions.

4. Soft-computing techniques and ARMA model for time series prediction

A. F.Rojas
B. A.Guillen
C. L.J.Herrera

In this research paper the challenge of predicting future values of a time series covering a variety of disciplines is dealt with. The fundamental problem of selecting the order and identifying the time varying parameters of an Auto Regressive Moving Average model (ARMA) concerns many important fields of interest such as linear prediction, system identification and spectral analysis. Recent research activities in forecasting with Artificial Neural Networks (ANNs) suggest that ANNs can be a promising alternative to the traditional ARMA structure. These linear models and ANNs are often compared with mixed conclusions in terms of the superiority in forecasting performance. This study was designed: (a) to investigate a hybrid methodology that combines ANN and ARMA models; (b) to resolve one of the most important problems in time series using ARMA structure and Box–Jenkins methodology: the identification of the model. In their paper, the authors have presented a new procedure to predict time series using paradigms such as: fuzzy systems, neural networks and evolutionary algorithms with a goal to obtain an expert system based on paradigms of artificial intelligence, so that the linear model can be identified automatically, without the need of human expert participation. The obtained linear model is combined with ANN, making up an hybrid system that could outperform the forecasting result.

5. A survey of intrusion detection techniques in Cloud

A. Chirag Modi
B. Dhiren Patel
C. Bhavesh Borisonia

In this paper, the authors have surveyed different intrusions affecting availability, confidentiality and integrity of cloud resources and services. Proposals incorporating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in cloud are examined. The authors recommend IDS/IPS positioning in cloud environment to achieve desired security in the next generation networks.

6. Soft Computing Applications in Infrastructure Management

A. Gerado W. Flintsch
B. Chen Chen

This research paper deals with infrastructure management decisions, such as condition assessment, performance prediction, needs analysis, prioritization, and optimization are often based on data that is uncertain, ambiguous, and incomplete and incorporate engineering judgment and expert opinion. Soft computing techniques are particularly appropriate to support these types of decisions because these techniques are very efficient at handling imprecise, uncertain, ambiguous, incomplete, and subjective data. This paper presents a review of the application of soft computing techniques in infrastructure management. The three most used soft computing constituents, artificial neural networks,

fuzzy systems, and genetic algorithms are reviewed, and the most promising techniques for the different infrastructure management functions are identified. Based on the applications reviewed, it can be concluded that soft computing techniques provide appealing alternatives for supporting many infrastructure management functions. Although the soft computing constituents have several advantages when used individually, the development of practical and efficient intelligent tools is expected to require a synergistic integration of complementary techniques into hybrid models.

Conceptual Model

An activity-based authentication model is conceptualized for the generic framework in the following phases.

Phase1 : Defining the structure and grammar for storing activity information in XML format.

Phase2 : Designing Application Architecture for Authentication in 2-tier and 3-tier model with and without Cryptography.

The layered application architecture employed in the implementation of the security model with and without encryption and decryption techniques is depicted in Figure 1 and Figure 2, respectively with the corresponding activity authentication levels shown in Figure 3.

Without Cryptography - 2-Tier Architecture-

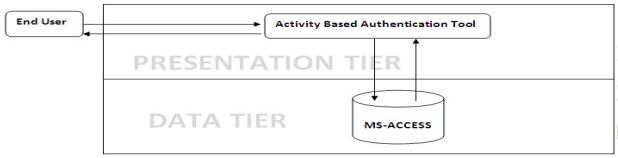


Figure1. Application Architecture without Cryptography

With Cryptography – 3- Tier Architecture-

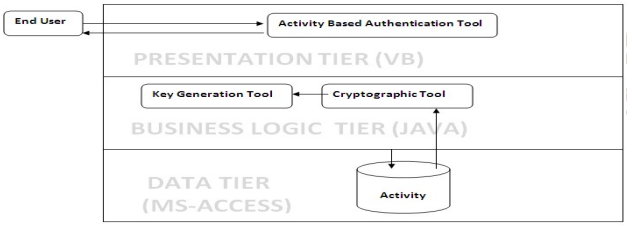


Figure2. Application Architecture with Cryptography

Activity Authentication Levels-

4	Pattern Generation Activity
3	Mix Color Activity
2	Move Image Activity
1	Time Activity

Figure3. Activity-based Authentication Levels

Theoretical Model proposed is further implemented and tested in windows10 environment.

Phase3: Designing Encryption/Decryption Algorithms Employing Genetic Algorithm

Proposed Cryptographic Algorithm Employing Genetic Algorithm-

Encryption of a Text Phrase-

Step 1: Extract two 8-byte blocks from the text phrase to be encrypted.

Let the two blocks be represented by

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7

c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7

where each b_i and c_i is a character in a textual phrase.

Step 2: Perform crossover operation.

Generate two random numbers in the range [0-7]. Let the two random numbers generated be 1 and 6.

Hence, Crossover Point1 = 1

Crossover Point2 = 6

Perform the crossover between two crossover points generated above.

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7

c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7

The blocks after performing crossover operation are

b_0	b_1	c_2	c_3	c_4	c_5	c_6	b_7

c_0	c_1	b_2	b_3	b_4	b_5	b_6	c_7

Step 3: Perform mutation operation.

Generate two random numbers in the range 0 to 7. Let the two random numbers generated be 3 and 4.

Hence, Mutation Point1 = 3

Mutation Point2 = 4

Perform mutation operation on two blocks obtained in Step 2.

b_0	b_1	c_2	128-c_3	128-c_4	c_5	c_6	b_7

c_0	c_1	b_2	128-b_3	128-b_4	b_5	b_6	c_7

Step 4: Generate a random key based on crossover points, mutation points and crossover factor generated above.

Hence the symmetric key in an octal form is

1	6	3	4

Each octal digit in a symmetric key can be represented using 3 bits. Hence a symmetric key in a binary format is given by

3 * (c + m)

In the above example, c = m = 2.

Hence Key Length = 12.

In the case of 2 cross over points and 3 mutation points the length of the key is 15 bits which depends on the number of crossover points and mutation points. The length of the symmetric key can be computed using a general formula

3 * (c + m)

Results and Discussions

The model for activity authentication tool presented is implemented in VB with MS-Access as backend for storing authentication related information. The structure of the database employed for the purpose is shown in the Figure 4. Winsock control is used for remote connection. The reference to the same is added using components dialog as

depicted in Figure 5. The authentication information is distributed on multiple servers by employing vertical fragmentation. The user can implement the database on multiple machines and select the machine for both storing the authentication information and for performing end user authentication.

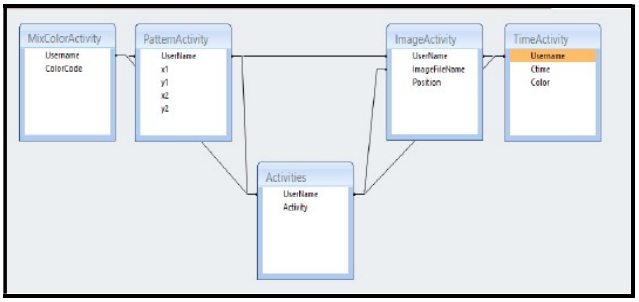


Figure4. Structure of Database for Storing Activity-based Authentication Information

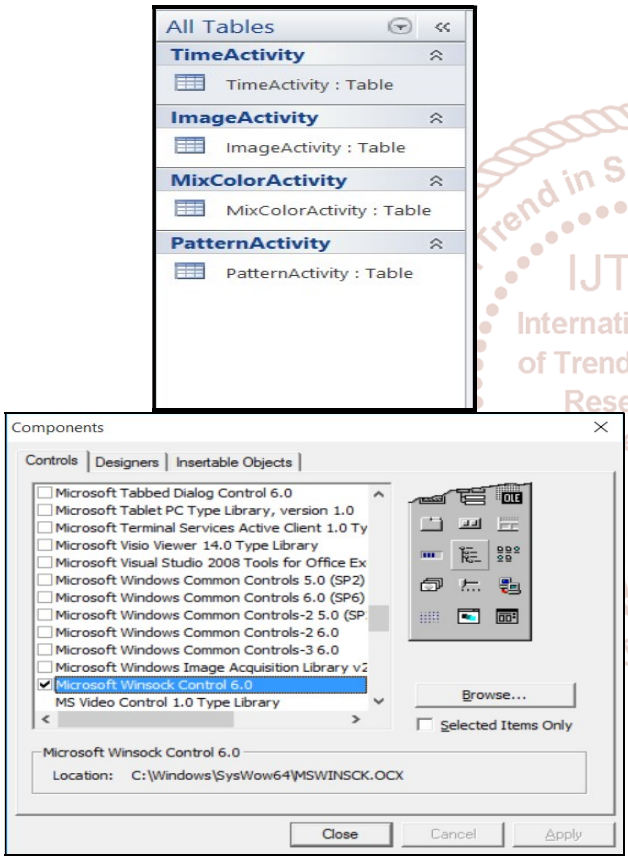


Figure 5. Adding Reference to Microsoft Winsock Control 6.0

System Requirements

1. Reference to Microsoft Winsock Control 6.0 hosted in MSwinsock.ocx Activex Control is added to the project as shown in fig.4.4.
2. Reference to Microsoft XML Parser.
3. Reference to Microsoft MS-Flex Grid control.

Executable batch files are generated for setting required environment variables. The structure of the executable batch files is shown below-

run.bat

```
set path=%path%;C:\Program Files\Java\jdk1.7.0\bin
set class path=C:\Program Files\Java\jdk1.7.0\bin
java Generate Key test
Pause
```

run1.bat

```
set path=%path%;C:\Program Files\Java\jdk1.7.0\bin
set class path=C:\Program Files\Java\jdk1.7.0\bin
java Encrypt all
Pause
```

32-bit ODBC DSN is created for accessing the Access database in a middle tier hosting a java application.

DSN Name	Access Database
activity	Sactivity.mdb
encactivity	encactivity.accdb

The user interface for the startup application screen are depicted in Figure 5(a) and Figure 5(b), respectively.

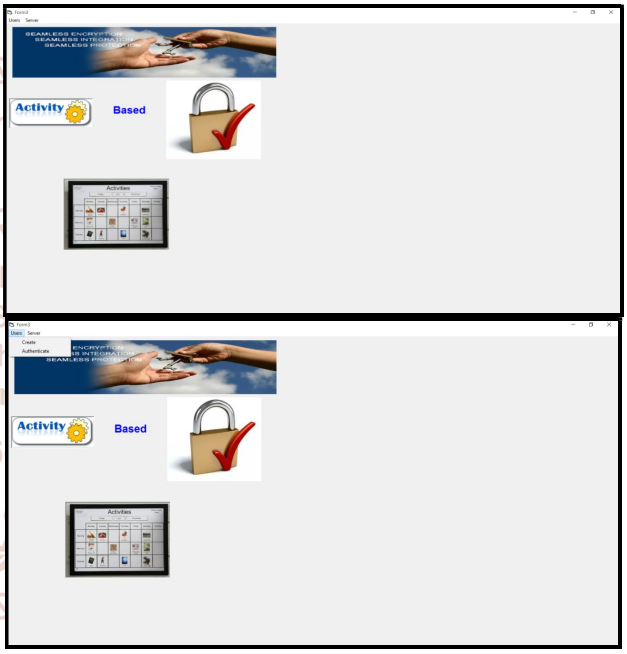


Figure 5(a)-5(b) Startup Screen for Activity Based Authentication Tool

Experimental Results

A key-pair is generated and stored in a key store database.

Contents of KeyStore.mdb file

RSA algorithm is employed for generating a key pair. The contents of Key table is depicted in Figure 6.

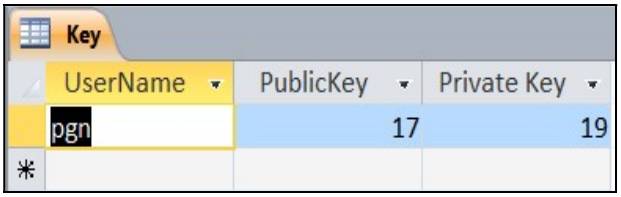


Figure6. Contents of Key table

The tool developed was tested for 50 different test cases, a few of which are presented here:

Test Cases:-

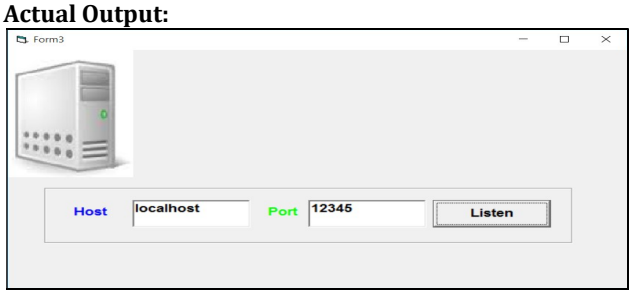
Test Case 1-

Select Start->Server option from the main menu.

Expected Output-

GUI for accepting host name and port of the server should appear and on clicking the "Listen" command button, the server should be up and running listening to the incoming requests at the specified port. The window should automatically get minimized.

Actual Output:



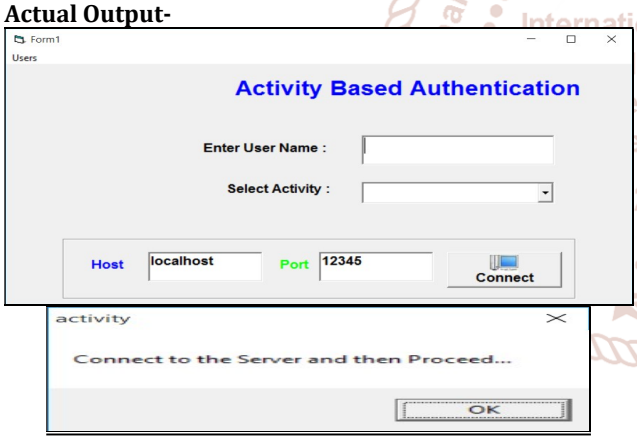
Test Case 2-

Select Users -> Create option from the main menu and enter user name.

Expected Output-

GUI for accepting user name should appear and the message "Connect to the Server and Proceed" should appear.

Actual Output-



Test Case 2.a-Click on the "Connect Button".

Expected Output-The message "Accepted Connection from 127.0.0.1" should appear.

Actual Output:

Test Case 3-

Connect to the server, enter username and press Enter key. Storing Time Activity data on machine MCA10 and requesting data across port 5000

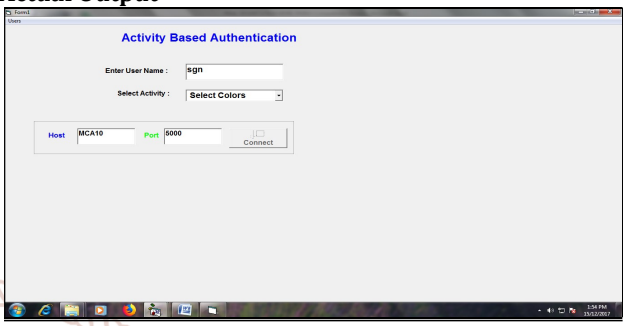
Expected Output-

If the username already exists in the database, only the activities not selected by the user should appear in "Select Activity" drop-down list.

If the username does not exist in the database, new username must be inserted into the database and all the activities should be displayed in the "Select Activity" drop-down list.

The dropdown list should display all the activities so far not selected by the current active user.

Actual Output-



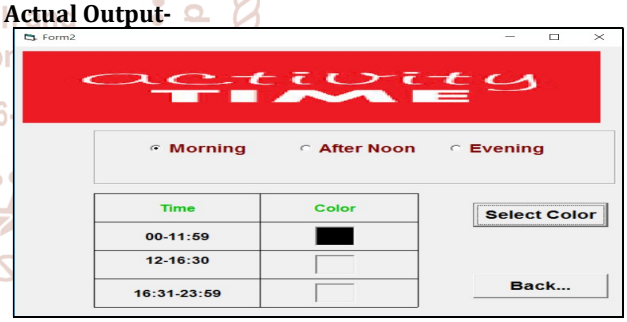
Test Case 4-

Connect to the server, enter username and select "Time Activity" option from the dropdown list.

Expected Output-

Time Activity form should be displayed.

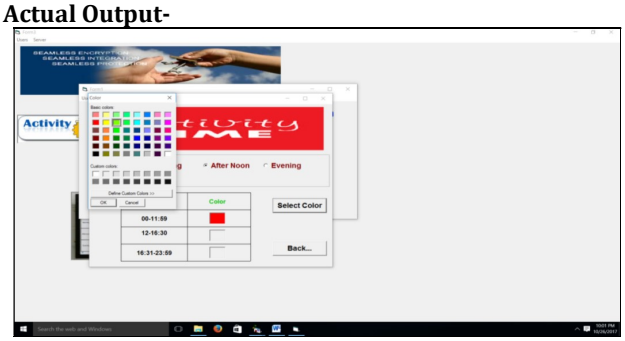
Actual Output-

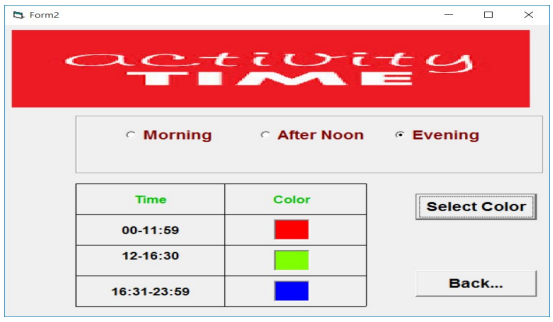


Test Case 4.a:

Select 1..3 different colors in 3 different time slots by selecting the appropriate option button and click on the "Back" button.

Actual Output-



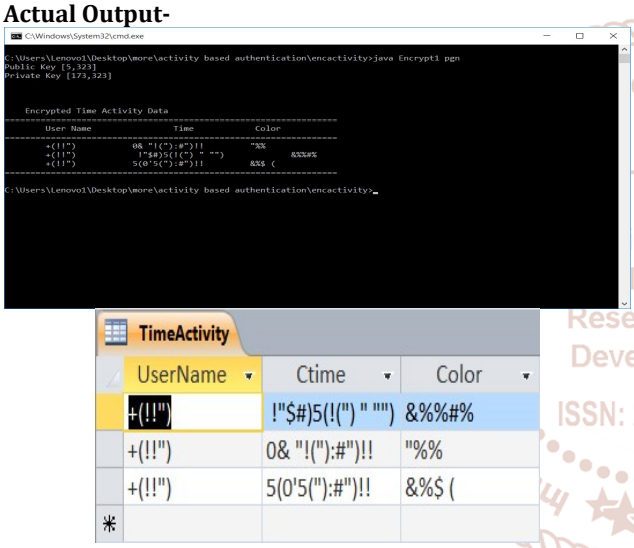


Test Case 5-
Enter the following command from command window

```
javac Encrypt1.java
java Encrypt1 pgn
```

Expected output-
The Time Activity data should be retrieved from the activity.mdb database and encrypted using hybrid RSA and GA algorithm and encrypted data should be stored in Time Activity table of encactivity.accdb database.

Actual Output-

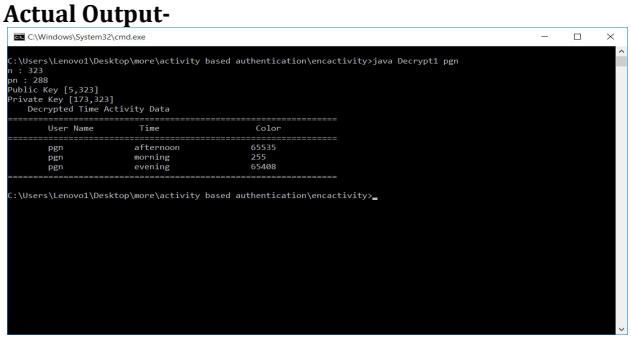


Test Case 6-
Enter the following command from command window

```
javac Decrypt1.java
java Decrypt1 pgn
```

Expected output-
The Time Activity data should be retrieved from the encactivity.accdb database and decrypted using hybrid RSA and GA algorithm and decrypted data should be stored in Time Activity table of activity.mdb database temporarily for authentication.

Actual Output-



Conclusion and Scope for the Future Work:
This section summarizes phase-wise conclusions drawn from research work carried out pertaining to activity based authentication, design and implementation phases. The model is designed and implemented in two different application architectures. The first model is based on plain textual authentication model which employs two-tier architecture where the end user interacts with the presentation tier which employs data tier for data persistence. The second model employs cryptography for data protection and employs three-tier architecture by separating out the application's business logic in a middle tier. The logical tiers are mapped to the corresponding physical tiers on one-to-one basis. Both the models are implemented employing Visual Basic in presentation tier, Java in middle tier and MS-Access in data tier. The algorithm is implemented in Java and applied for the encryption and decryption of an activity-based password of employees in a hypothetical organization. Based on security needs of the organization the user can select between 1 to 4 different levels of authentication.

References:

[1] Rudolf Maarten Bolle, Sharon Louise Nunes, Sharathchandra Pankanti, Nalini Kanta Ratha, Barton Allen Smith, Thomas Guthrie Zimmerman, Weniger, " Method for biometric-based authentication in wireless communication for access control , US6819219 B1, International Business Machines Corporation, BiBTeX, EndNote, RefMan, 16 Nov 2004.

[2] Sandeep Kumar, Eugene H. Spafford, " A Pattern Matching Model for Misuse Intrusion Detection", The COAST Project, Department of computer Sciences, Purdue University, West Lafayette-47907-1398, CSD·TR-94-071, October 1994

[3] Asaf Shabtai, Uri Kanonov, Yuval Elovici, "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method." Journal of Systems and Software, Volume 83 Issue 8, August, 2010, Pages 1524-1537

[4] F. Rojas, H. Pomares," Soft-computing techniques for time series forecasting", ESANN'2004 proceedings - European Symposium on Artificial Neural Networks, Bruges (Belgium), 28-30 April 2004, d-side publi., ISBN 2-930307-04-8, pp. 93-102

[5] Chirag Modi , Dhiren Patel , Bhavesh Borisaniya , Hiren Patel , Avi Patel , Muttukrishnan Rajarajan," A survey of intrusion detection techniques in Cloud", Journal of Network and Computer Applications 36 (2013) 42–57

[6] Gerado W. Flintsch, Chen Chen," Soft Computing Applications in Infrastructure Management", June 7th 2007,Blacksburg-Virginia