**​​​​​​​​​​​ A**

**Synopsis ​​Report On**

**Implementation​​ of​​ Graph ​​Algorithm**

Submitted​​ to ​​the ​​department ​​of

**Computer​​ Science ​​and​​ Engineering**

In ​​partial ​​fulfilment​​ of​​ the ​​requirements

For ​​the ​​degree ​​of

**BACHELOR​​​ OF​​ TECHNOLOGY**

**In​​**

**Computer​​ Science ​​and​​ Engineering**

Under ​​​the​​guidance ​​of Mr​. Randhir Kumar Singh (Assistant ​​​Professor)​​​

**Submitted ​​By**

AnshDeep Kaur 1416410061

Vaibhav Verma 1416410280

Neha Singh 1416410162

Pranveer Singh Institute of Technology, Kanpur

Dr. A P J A K Technical University, Lucknow

**PROBLEM STATEMENT**

Exam Timetabling problems in universities begin with the integration of examination data and processes from various departments, centres, faculties and branches. It is a complex problem during number of exams that needs to be scheduled. This software make sure that there is no clashing between subjects and students can be fit in the specific room. In addition to scheduling this project also includes data security i.e. all the entered data will be stored in encrypted form.

The exam timetabling problem consists of planning different exams in six days with different capacities. Furthermore, each day there are only two slots available which are morning session and evening session. The main objective of this project is to guarantee data security and all the exams are schedule and student can sit in all the exams that they are applied for.

**Why we have chosen this problem?**

Every ​​exam​​ scheduling ​​is ​​a​​ challenging​​task ​​that ​​Universities ​​and​​ colleges ​​face​​several​​ times every​​ year. ​The ​​challenge ​​is​​ to​​ schedule​​ so ​​many ​​exams ​​of ​​forces​​in​​ a ​​limited ,​​ and ​​usually short ​​period​​ of​​ time.​​​ An ​​exam​​ schedule​​ should ​​avoid ​​conflicts,​​ in​​ the​​ sense​​ that​​ no​​ two ​​or more ​​exams ​​for​​ the ​​same ​​student ​​ ​​schedule​​ at ​​the ​​same ​​time.​​​ Part​​ of ​​the ​​challenge ​​is ​​to achieve fairness​​ for the ​​students.​​​A fair​​ schedule ​​does ​​not​​ schedule​​ more ​​than​​ 2​​ exams,​​​ for example ​​for​​ a​​ student ​​​on ​​one ​​day. ​​​In ​​the ​​meantime ​​schedule ​​does​​ not leave ​​a ​​big ​​gap between​​ exams​​for ​​the ​​students.​​​ The​​ exam​​ scheduling ​​problem​​ is ​​defined ​​as ​​follows:

​​“​​we first ​​represent ​​the​​ courses​​ by​​​ nodes​​ of​​ a ​​graph​​where ​​two​​ nodes ​​are​​ adjacent​​ if ​​the ​​two corresponding​​ courses​​ are ​​registered​​ by​​ at​​ least ​​one​​ student.​​​Then ​​it ​​is ​​required ​​to ​​assign ​​each course ​​represented ​​by ​​a ​​node ​​a​​t time​ ​slot​​, ​​in​​condition​​ that ​​a ​​set ​​of ​​constraints imposed​ ​on ​​the ​​problem ​​are ​​also ​​met​​.” ​​We​​solve​​ this ​​problem ​​by ​​using ​​node ​​graph ​​colouring technique.

**OBJECTIVE AND SCOPE**

The objective of this project is to presents a graph-coloring-based algorithm for the exam scheduling application which achieves the objectives of fairness, accuracy, security and optimal exam time period.

This application can be used in educational institutions as well as in corporate world. This can be used anywhere any time as it is a windows based application(user location doesn't matter).

It fulfils all an office application automatically with minimal overhead.

**METHODOLOGY**

In​ ​undirected​ ​graph ​​G ​​is ​​an ​​ordered ​​​pair(V,E) ​​​where​​V ​​is ​​a ​​set ​​of ​​nodes ​​and ​ ​E is ​​a​​ set​​ of​​ number of ​​directed ​​edges ​​between​​ nodes.​ ​​Two ​​nodes ​​are​​ said ​​to​​ be ​​adjacent if ​​there​​ is​​ an​​ edge ​​between ​​them. ​​​The​​ graph​​ coloring ​​is ​​a​​ well-known ​​problem . ​​​Node ​​coloring ​​assign ​​colors ​​to ​​the ​​nodes​​ of​​ the ​​graph ​​such​​that no ​​two ​​adjacent ​​nodes ​​have ​​the​​ same ​​color.​​​ Two​​ edges ​​are ​​said​​ to ​​be​​adjacent if ​​they ​​both​​ share ​​a ​​node ​​in ​​common.

We​​ first ​​represent​​ the ​​courses ​​by​​ nodes ​​of ​​a​​ graph,​​ where two ​​nodes​​ are adjacent ​​if​​ the ​​two ​​corresponding​​ courses​​ are​​ registered ​​by​​ at​​least ​​one​​ student. then, ​​​it ​​is ​​required ​​to ​​assign​​ each ​​course​​ represented ​​by ​​a​​ node ​​at​​ time​​slot, such ​​that ​​no ​​two​​ adjacent​​ nodes​​ have​​ the ​​same​​ slot,​​​ in​​ condition​​ that ​​a​​ set​​ of constraint ​​impose​​ on​​ the ​​problem ​​are ​​also ​​met.​​​ We ​​solve ​​this ​​problem​​ by ​​using graph ​​coloring ​​algorithm​​ technique.

We ​​use ​​RSA ​​algorithm​​ to ​​make ​​our ​​system​​ more ​​secured. We store all the data in database in encrypted format .

RSA​​ is ​​a​​public​​ key ​​cryptosystem​​ developed​​ by​​ 3​​MIT​​professor,​​​ Ronald​​l rivest,​​​Adi​​Shamir,​​ and​​​ Leonard​​M​​Adleman,​​​ in​​ 1977 ​​in​​ an ​​effort​​ to ​​help ensure​​ Internet​​security.​​​ Crypto system​​ is​​ simply​​ an​​ algorithm ​​that ​​can​​ convert input​​ data ​​into​​something​​ unrecognisable(​​encryption),​​​ and​​ convert ​​the unrecognisable ​​data​​back​​ to ​​its​​ original​​ form(​​decryption).

The​​​ RSA​​ algorithm ​​assume​​ that ​​each​​ computer ​​user​​ has​​ a ​​triplet​​ of integers ​​(E,​​D,​​N), ​​​in ​​which ​​E ​​and ​​N​​ are​​ open​​ for ​​all​​ to​​ see,​​​ but ​​D ​​​is ​​known only​​ to ​​the​​user.​​​ The ​​pair​​(E,N)​​​ is​​ called ​​the ​​public​​ key​​ and​​ (D,​​N) ​​is ​​called​​ the private​​ key.

Public​​ key​​ Cryptography ​​generate ​​public ​​key ​​and​​ private ​​key ​​by​​ using​​ the following​​steps:

1.Choose ​​two ​​large prime​​ numbers p​​ and q. ​​​Generally,​​​ p​​ and​​ q​​ are ​​100​digits long.

2.Compute ​​the ​​value ​​of​​ module ​​N​​​ as: ​​N=p\*q.

3. Choose ​​an​​ integer ​​E​​​ that ​​is ​​relatively​​ Prime ​​to ​​(p-1)​​\*​​(q-1) ​​i.e., ​​E​​​ does not ​​divide ​​​(p-1)​​\*​​(q-1)​​​ evenly.

4.Choose ​​an ​​integer ​​D ​​​such ​​that ​​E\*D = ​​1​​mod​​(p-1)​​\*​​(q-1). ​​​In​​ other words,​​E​​\*​​D​​-1 ​​​is​​ evenly​​ divisible​​ by​​ (p-1)​​\*​​(q-1).

5.The ​​public​​ key ​​is​​ the ​​pair​​(E,N). ​​​This​​ is​​ used​​ to ​​encrypt​​ messages.

6.The ​​private ​​key​​ is ​​the​​ pair(D,​​N). ​​​This​​ is​​ used ​​to ​​decrypt ​​encrypted messages ​​and​​ reveal ​​the ​​original message.

Give​​ a ​​message ​​M​​(​​​represented​​as​​a​​long​​sequence​​of​​digits), ​​​The ​​encrypted message​​ C ​​​is ​​created ​​by ​​C =​​ M​​​E​mod​​N.

Given​​ an ​​​encrypted​​ message ​​C,​​​ the​​ original ​​message ​​M ​​is ​​recovered ​​by ​​​**​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​**M=​​​C​D​​mod​​N.

**HARDWARE AND SOFTWARE USED**

**Hardware-**

* 2GHz x86 Processor.
* 1Gb of system memory(RAM).
* 15GB of hard-drive space.
* Monitor to display output.
* Keyboard /Mouse for data input.

**Software -**

**Front End -**

* **J2EE:**  Java 2 Enterprise Edition is a programming platform- put of the java platform for developing and running distributed multi tier architecture java, application, based largely on modular software components running on an application server.
* **HTTP:** Hypertext transfer protocol is a transaction or oriented client/server protocol between web browser and web Server.
* **APACHE TOMCAT:**Web Server for running j2ee application over network.

* **HTML:** It provides a means to create structured documents including images, lists and other item.

**Back End:-**

* **MS-ACCESS:** It is relatively compatible with SQL. Query can be viewed graphically or edited as SQL statement

**REFERENCES**

1. E.Cheng, R. Kleinberg, S. Kurk , W. Lindsey , AND D.Steffy. A strictly combinatorial approach to a university exam scheduling problem , practice and theory of automated Timetable.

2.Y.YANG , R. Paranjape and L. Benedicenti, an agent based general solution model for the course timetabling problem , ACM May 8-1-2016.

3.Diffie, Hellman , M.E., New directions in cryptography, IEEE Transactions on Information Theory 22(1976), 644-654.

4. Rivest , Shamir, Adleman , An method for obtaining digital signatures and public key cryptosystems, communications of the ACM 21(1978), 120-126.