

ENCRYTION OF DATABASE

**PBL Report for DATA STRUCTURE AND ALGORITH (CSE102) Course**

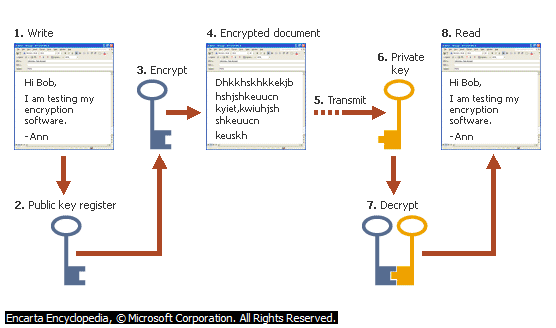
**Faculty: M JAYASUDHA**

**Slot: D1**

**TEAM MEMBERS**

1. **PURUSHOTTAM - 14BEC1043**
2. **ROHIT KUMAR PANDEY - 14BEC1022**

***PROBLEM UNDERTAKEN***



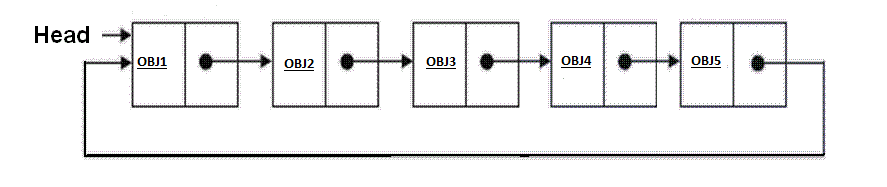
* ENCRYPTION, PROCESS OF CONVERTING MESSAGES OR DATA INTO A FORM THAT CANNOT BE READ WITHOUT DECRYPTING OR DECIPHERING IT**.**
* TO HIDE THE INTEGRITY OF DATABASE
* TO ENCRYPT DATABASE
* A SCENARIO IN WHICH A COMPANY WANTS TO HIDE THE TRUE IDENTITY OF ITS EMPLOYEES. WE ARE MAKING A PROGRAM THAT HELPS TO ACHIEVE THIS GOAL

***OUR APPROACH***

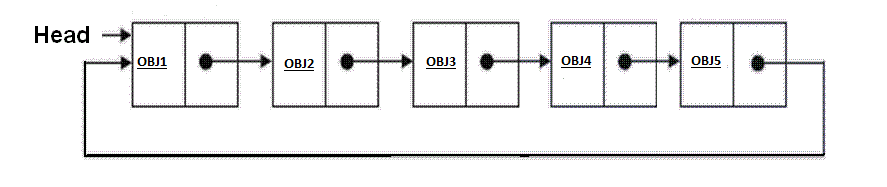
* LANGUAGE USED:C
* LARGER DATABASES HAVE BECOME INCREASINGLY IMPORTANT IN BUSINESS LIFE
* WE WILL BE SECURING THE COMPANY DATABASE USING

ENCRYPTED DATA STRUCTURE.

***HOW THE CODE WILL WORK***



* WE WILL CREATE A CIRCULAR SINGLE LINKED LIST
* THE DATA FIELD OF LINKED LIST WILL CONTAIN A STUCTURE
* EACH STRUCTURE ENTITY WILL HAVE DATA FIELDS LIKE EMPLYEE ID, DOB , NAME ,DESIGNATION , DEPARTMENT ETC
* NOW, WE WILL EXTRACT DATA FROM STRUCTURE LIKE EMPLOYEE ID.
* THIS EMPLOYEE ID WILL BE ENCRYPTED FURTHER.



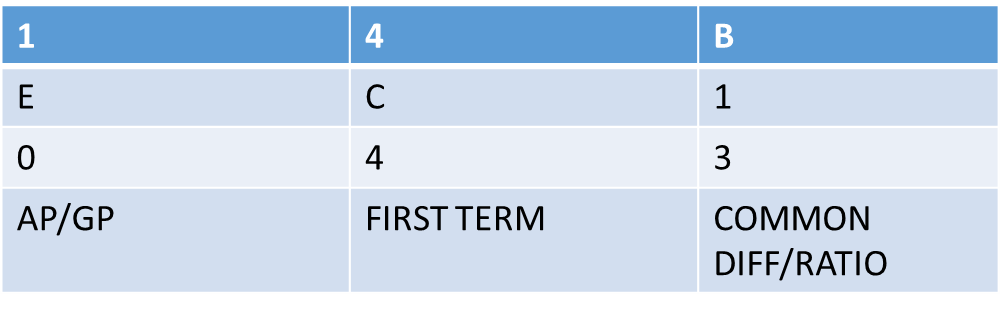
***14BEC1043***

Extracting DATA like EMPLOYEE ID

***14BEC1043***

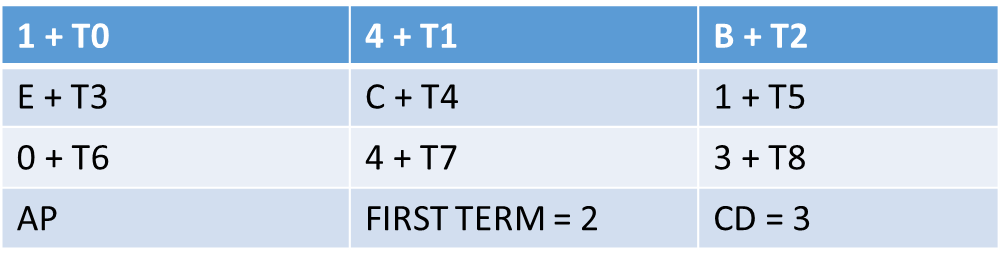
***OBJ1***

***DATA STRUCTURING***



RESERVED

* THE DATA WILL BE STRUCTURED IN AN ARRAY OF 4\*SIZE(VARIABLE) MATRIX.
* THE 4TH COLUMN WILL BE RESERVED FOR ENCODING DATA
* THE TABLE WILL CONTAIN ASCII VALUE OF DATA ENTERED



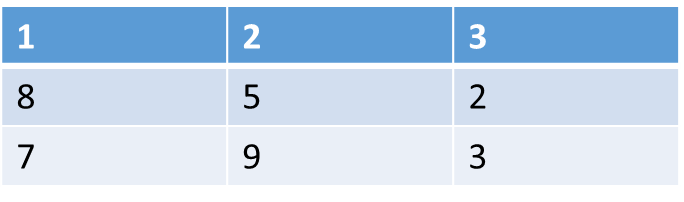
RESERVEDDDD

* ONCE THE DATA IS ENTERED IN ASCII FORM , WE WILL ASK FOR ENCODING OPTION : AP OR GP
* WE WILL ASK USER TO INPUT COMMON RATIO/DIFFERENCE AND THE FIRST TERM
* THEN ADD THE GENERAL TERM TO EACH CHARACTER IN THE MATRIX ARRAY

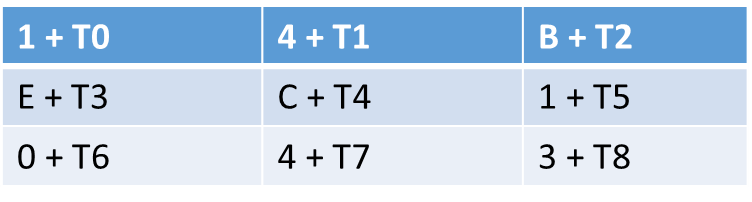
***ENCRYPTING DATA***

* ASK FOR PUBLIC KEY MATRIX (3\*3) FROM THE USER
* MULTIPLY THAT PUBLIC KEY MATRIX TO THE STRUCTURED DATA USING MATIX MULTIPLICATION
* THE 4TH COLUMN WILL REMAIN INERT

PUBLIC SECRET KEY

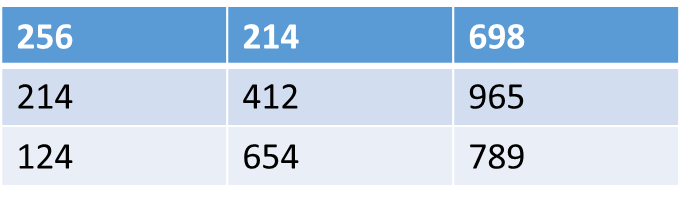


SECRET MESSAGE



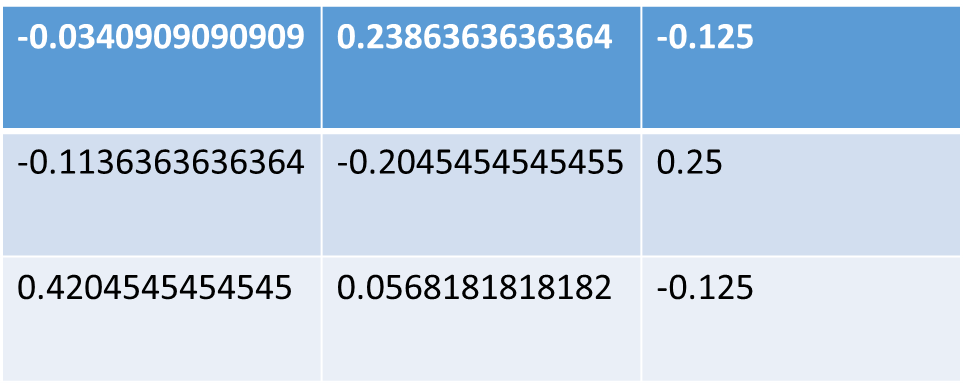
\*

* THUS WE GET THE ENCRPTED MESSAGE



ENCRYPTED MESSAGE

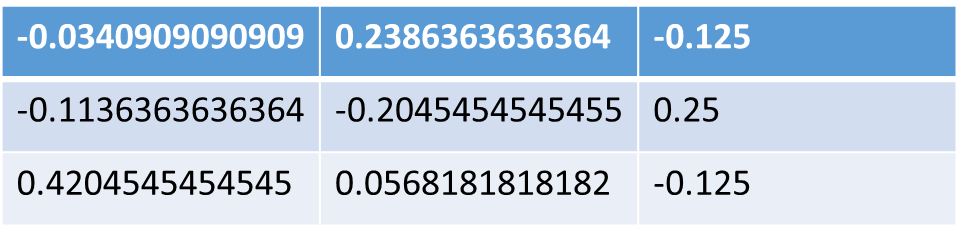
* NOW DISPLAY THE PRIVATE SECRET KEY TO THE USER
* THE PRIVATE SECRET KEY IS THE “**INVERSE**” OF THE PUBLIC SECRET KEY.
* ONLY THIS KEY CAN HELP TO DECRYPT THE MESSAGE



PRIVATE SECRET KEY OR INVERSE MATRIX

***DECRYPTING MESSAGE***

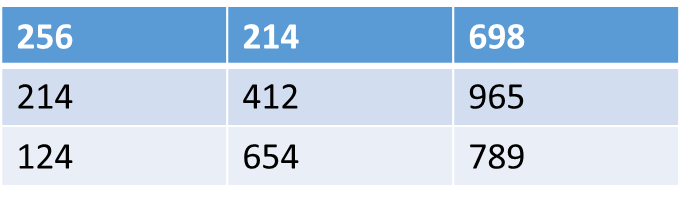
* TO DECRYPT THE MESSAGE WE NEED TO HAVE THE PRIVATE KEY
* INPUT THE PRIVATE KEY FROM THE USER
* MULTIPLY THE PRIVATE KEY TO THE SECRET MESSAGE
* THIS WILL GIVE THE ORIGINAL MATRIX

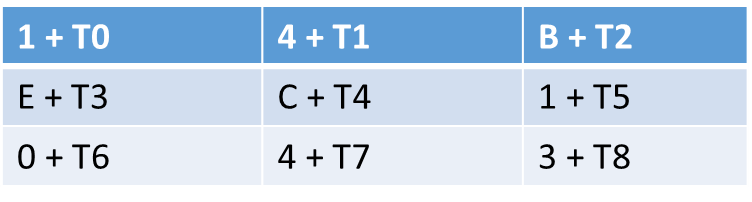
******

PRIVATE SECRET KEY OR INVERSE MATRIX

\*

ENCRYPTED MESSAGE

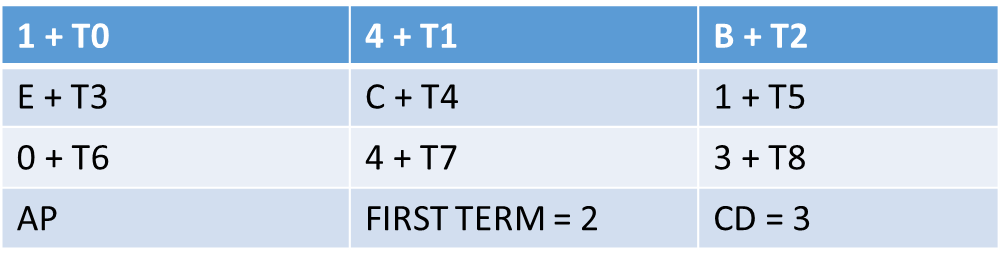




SECRET MESSAGE

=

* ONCE WE GET THE DECRYPED MSSG WE NEED TO DECODE THE MSSG BACK TO ORIGINAL FORM
* TO DO THAT WE NEED TO READ THE 4TH RESERVED COLUMN AND SUBTRACT THE COMMAN DIFFERNCE OR RATIO FROM EACH TERM IN THE MATRIX.



RESERVED

=

GENERAL TERM

-

|  |  |  |
| --- | --- | --- |
| **1** | **4** | **B** |
| E | C | 1 |
| 0 | 4 | 3 |

* THIS WILL GIVE BACK THE “**ORIGINAL DATA**”.

**14BEC1043**