18DCE115

Date
Page 1

10/06/'20

CE246 - DATABASE MANAGEMENT SYSTEM

KASHYAP SHAH
4CE2 => B-BATCH
COMPUTER ENGINEERING
9408718809

ANSWERS

Q1 P = 17
q = 13
e = 5
M = 7

RSA algorithm : It is used to implement
Assignment cryptography.

$n = P \times q$
$= 17 \times 13$
$= 221$

$\phi(n) = (P-1)(q-1)$
$= 16 \times 12$
$= 192$

public key (e) = 5

$$de = 1 + k\phi(n)$$

$$d = \frac{1 + k\phi(n)}{e}$$

Let $k = 0$, $d = \frac{1+0}{5} = \frac{1}{5}$ → not proper

$k = 1$, $d = \frac{1+193}{5} = \frac{193}{5} = 38.6$ (not proper)

$k = 2$, $d = \frac{1+2(192)}{5} = \frac{1+384}{5} = \frac{385}{5} = 77$

∴ plain text = 7

For cipher Text = E(M) cipher = $M^e \pmod n$

$= 7^5 \bmod 221$

$= 16807 \bmod 221$

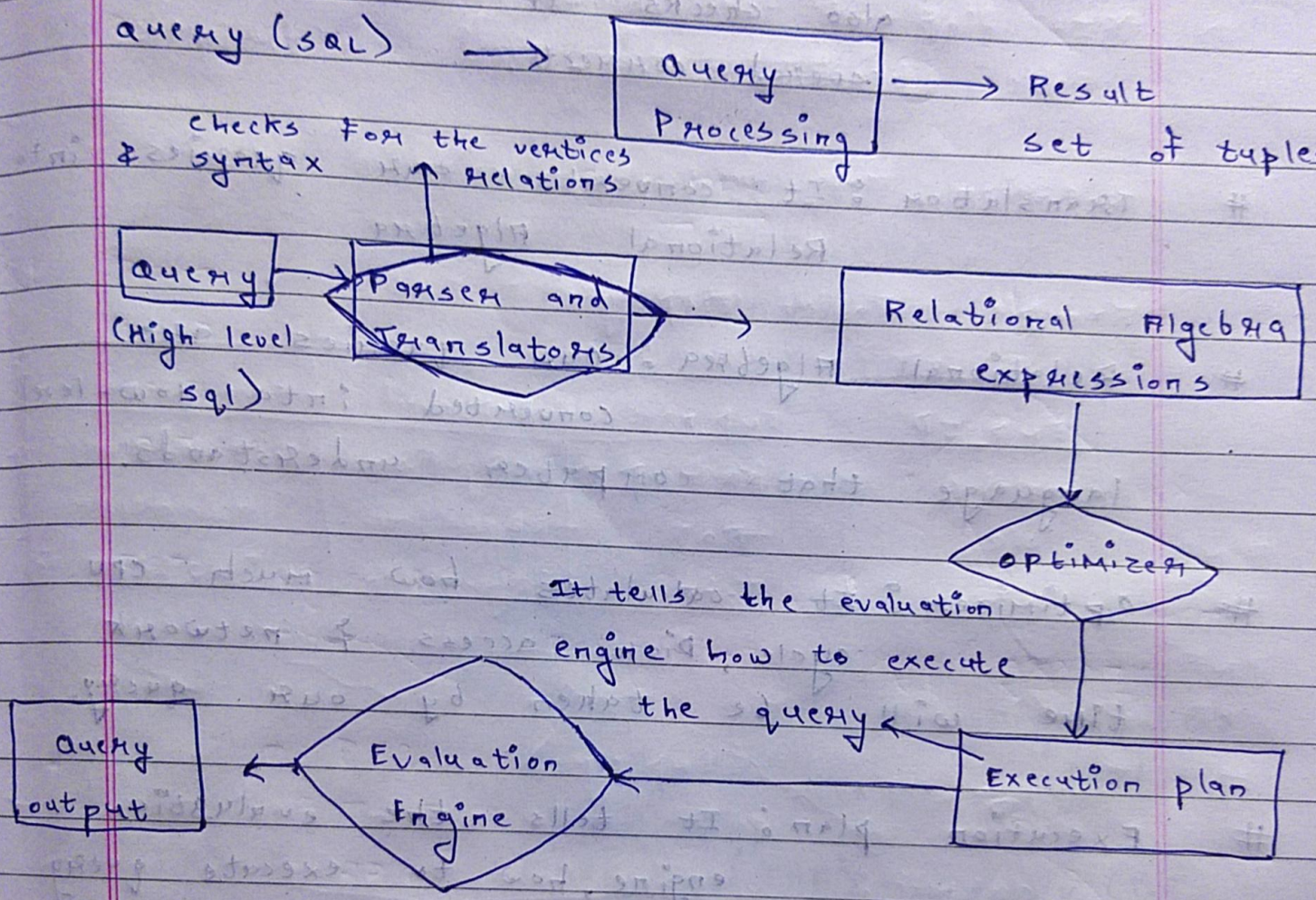
$= 11$

$D(c)\,pt = c^9 \pmod n$

$= 11^{77} \pmod{221}$

Decryption = 7

Q9 Query Processing : Range of activities involved in extracting data from a database to process the query and generate result.



query : Commands that a user waits (select * from the table name)

Parser : It checks syntax of query and also checks if the relation is ~~covered~~ correct.

Translator : It converts our queries into Relational Algebra.

Relational Algebra : Our queries are converted into low-level language that computer understands.

Optimizer : It calculates how much CPU cycle, Disk access & network time will be taken by our query.

Execution plan : It tells the evaluation engine, how to execute query.

Evaluation Engine : It evaluates our query and displays the output.

Q7 1) For all v (is_unk(v.Gender) & is_unk (v.Surname) & is_unk (v.Firstname) & is_unk (v.occupation) & is_unk (v.Birthdate) & is_unk (v.city) & is_unk (v.cast)

=> For all → True (T)

T ∩ ((F∩F∩F∩F∩F∩F∩F) ∧ (F∩F∩F∩T∩F∩F∩F) ∩ (F∩F∩F∩F∩F∩F∩F) ∧ (F∩F∩F∩T∩F∩F∩F))

= T ∧ (F∩F∩F∩F)

= T ∧ F

= T

2) Exists v (v.gender = 'F' & v.Birthdate > '1/6/1990')

=> F v ((F∩T)) v (T∩F) v (T∩T) v (T∩T))

= F v (F∨F∨T∨T)

= F∨T

= T

Q8 Projection Operator: (π) is a unary operator in relational algebra that performs a projection operation.

⇒ It displays the column of a relational or table based on specified attributes.

Notation : π_{name} (table name)

Example Table Employee

Emp_ID	Emp_name	Emp_email	Emp_phone
101	Kashyap	K@gmail.com	9408712809
102	Raj	R@gmail.com	9406918100
103	John	j@gmail.com	9426817890

$\pi_{EMP\text{-}ID, emp\_name}$ (Employee)

output :

Emp_ID	Emp_name
101	Kashyap
102	Raj
103	John

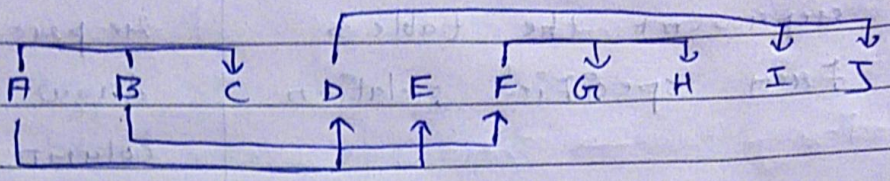
Tuple Relational Calculus | Domain Relational

Tuple Relational Calculus	Domain Relational
1) In TRS, the variable represent the tables from specified relation	1) In DRS, the variables represent the value draw from specified column.
2) In this filtering variables uses type of relation.	2) In this filtering is done based on the domain of attributes.
3) A tuple is a single element in database term, it is a row	3) A domain is equivalent to column data type & any constraints on value of data.
4) Example : {T | employee(T) and T.Dept_ID=10}	Example : {< EMPLOYEE > DEPT_ID=10}

Q5 $R = \{A, B, C, D, E, F, G, H, I, J\}$

$F = \{AB \rightarrow C, A \rightarrow DE, B \rightarrow F, F \rightarrow GH, D \rightarrow IJ\}$

b) $R = \{$ A B C D E F G H I J



Here A, B are the essential attributes

Closure of $(AB)^+ = ABCDEFGHIJ$

∴ AB is the candidate key

	$AB \rightarrow C$	$A \rightarrow DE$	$B \rightarrow F$	$F \rightarrow GH$	$D \rightarrow IJ$
BCNF	✓	—	—	—	—
3NF	✓	×	×	×	×
2NF	✓	×	×	×	×
1NF	✓	✓	✓	✓	✓

Here, the relation is in 1NF

There is a partial dependency $A \rightarrow DE$

Transitive dependency

$B \rightarrow F$

$F \rightarrow GH$

and also of all the dependancy does not have A as a super key

- Decomposition:

R_1 (A B)

R_2 (A D E I J)

↳ R_{21} (D I J)

R_{22} (A D E)

R_3 (B F G H)

↳ R_{31} (B F)

R_{32} (F G H)

Then for the above tables are in BCNF.

There are 5 tables => R_1, R_{21}, R_{22}, R_{31} & R_{32}