Q1) describe all sdlc model with suitable diagram and example?

=> software development life cycle => structure development comparies and different phases.

phases work in top to down impying that the phase that input from the porious phase end. regrate to as intamdiates product work product availabde

1) priminary Investigation =>

* prelinary semestation vergia the problem and undertempt the and the requiral syestem.

- It consider whenever the peracde will be

cat effetysa from buisness point of virue and with it can devolope from within existi clardi considered
* The output whether we new system should be devolope or not

2) Software Analyase
This phase studies the problem are requirments of software in dectail. the requrment or regnyged during the nature development
- After analysing the requirments of the user analysis the user analysing the requirements of the user a requirment known as rottra requirment specification (SRS) is developed. it includes dereloping plans that direction the activites to be predermed. during the project and as for torros configuration managment plans pegat and reheduling and the quality assurans plans.

3) Software edign:
In this phase the requirment are given a define from
delign can delign are a prev of efficency and the required junction

and the quality requirments of a syestem
- rataare delign are a ~~proce~~ blue print ton the implecutation and requirments in the software syesteam
- fach element as the anlysis provides information that is requirment to crate dectign model.
- The requirment specification at rofure together with data function and behaviour models provide a platform to the design tase to mut required fonctional re quality requirment of a syuteam

4] software coding
- This phase can be defined as a prourt of aranlating the software requirment into a programming language tools that are available
- coriting athrough knowledge of programing language be its tale
- Therefore it is important to chete the appropriate programming languages according to user requirment
- A paradase program code is effiement it makes optimal of retours and conits minimum eartare

5) software testing →
- This testing is performed to assure that software is the from. assure
- Efficient testing improves
- to archive this software testing requires to a through analysis of the software systematic manner
- Test plan is created to test software in a planned and systematic
- In a addition software testing is pepare to ensure that sofware produce the correct output
- the implies that output produced should be according to user requirment

6) software maintainance:-
- In these phase conepitred of sect of soultage engineering artites that a yes after software in delived to the.
- the object of software maintance is to make software operational according to user requirment
- The need of software maintenance is to provide community of revive This malise that software maintance fear an fixing error encovering for

or in comphability of roadcoare a software.
- In addition it facilities future and maintanace work to provide comunity of revive.
- This malise that software maintance foar on fixing error recovering for fative. such as harade. future on in comphibillity of redcoore or softwoare.
- In addition it facilies future and maintance work by modifying the software code and database used in the software
- After the software is devolope it may require changes
- To make changes in software syesteam. software and implement changes can also be
- Note that changes can also be foraed on the software. syesteam because of changes in goverment equation or changes in potiars of the organisation various kinds of prgass models coe are moret for waterfall model. repieral model

- waterfall mode ⇒

in waterfall moded coro known as cyde moded) the dereolopment of software pro- weals tienarly and sequentially teom require analysis to daign coding testing integration implamaintation. and maintance there. this moded. is are known as linear sequncial

model

1. waterfall model ?

In waterfall model also known as cycler model the development of software product linearly and sequencially from requirment analysis to digin, coding testing, integration implemantation and maintanance thre. this model is also known as linear sequntial model

A) syesteam ai Information ⇒
engeeniring modering ⇒ Estabished the extream for the syntax known as compression bare syesteam
- Hend it is essencial to that syesteam.
- A subsect a requirment is allocate to the software. interact with hardor
- syesteam engeniring individuls collecting requirments at the syesteam level the enfend are collect at a level whare all devisis.

regarding buisnes rentegies are taken

B) Requirment analysis ⇒
fowres on the requirment of software which is to developed
it determine the prosses that are incorporated driving the development of software
- The phass ideveds intraction. thes phase involed interaction betaen user and struare engineering and produs a document known as Software-requirment specification (SRS)

Design =>

Determine the dellid pass of are analyed

* it will ler software requirment defined by the use and trangats they into a software sequincial.
* in this phase the employer it on fieding a solution to the problem defined in the requirment analysed phede
* The software engeneer in the pase is mainly comand with the data scoate algorithm and intage xpasetabiane

c] coding =>

* emphalies on transation of design into a programming language this coding tyle and guideline
* The problem credit should be eay early to read and understand
* All the present written documented according to the speulcation.

d] Testing =>

* ensure that the produce is devoloped according to the requirment of the aser
* Testing is performed to verify that the product is evncloning efficenty with minimum

* it fouses on the statement hares and ensure that all the statements have been exercised (testcell)

e) Implenetation* =>
maintenance : deliver fully tameting operation software the user one the software as acapectal ropted and deveoped at the statements as coeres due to ~~testing~~ change in external enimment
• the chanyes oao acares due to chaniging iequirment of the we and the change acaring in the a caring in the datal of technology
• this phases beacause of modifying accroding errors and improving the preiname of the software

2) totyping modal:
A prototging modal is appiled when the an afrent of dectail inform action of inform action regarding in input and output. requirment in the software prototyping modil is displayed on the assumption pestoping that diffrent phare by allowing to user insate be experment with working

representation of the product protyne

1] requirment gathering →
a analysis prototyping model beging with requirment analysis and requirment analysis and requirment of the syestem are defined in detail
the user is inavisered to know the requirment of the syestem

2] quick design →
* when requirment are known a primalary design or a quick delign created
• It is not a detailed design however includes the important aprators of the ecosyestem to the user
* quick design helps in developing the protyne

3] Build protyne:
• information gathred from which delign is modifi to form a prototype
• The test prototype of the requsred syestem is developed from quick design

4] Assement or weside →
evaluation * next the prospect resyerteam presented to the user gor confidration as a pasct of devolopment preocase.
* the user throughly evater the prototype and reanies its strength and ratness such as what is to be. added or removed
* comment suggections are collected from users and are provider to the devlpoan

5] prototype retement:
• once the user evolucated prototype is retoived according to the requirment
• The denpose raises the prototype to moder make it more effective and efficent accroding to the we requirment
• The new prototyped is enater in the some inamber as the previous prototype
• This prolied by the use are mect. once the were is satisfied wit the developed prototype a final esyerteam is devolpment by on the prototype

6] inner product →
one the requirment are completely known as accept the final prodotype
& A the final syerteam is throughly evaluate and test followed by

routine maintenance on continuing savi to prev large scale bulloro and to minimize downtime

3.] spiral mold

1. in 1980 Bohem introduce a proces a maled known as spiral model
2. it comprises of activities organised in a sprat which has many dilcir
3. A mold of the software dinapsed praus in which the costainct activiti tynically requirment analyse primary and detined design coding intratively until the software is complete
4. the objective of spiral moded is to emphas mangement to elocile re reschule rest an the software project
5. each cycle of the flask quansctat co-mmen with identifying the quase for that cycle in addition it determine.

The avabillity principle of security states that the resources should be available to the authorise person at all times
forces inte. be beakers of interti action on unauthorise person

said. an authorised user x may no be able to contact server y, thise leads to an instruction attack. instruction attack coulds the availibility of resources in dangeour.

① difficult and legal issues.

deffucult issuer in the security syesteam are classified into following categories

privacy it deals with individual rides to excess the personal, information

② accuracy - it deals with the responcibbility of authentification fidelity and accuracy of information.

③ properedy - it deals with the owner of information

④ excessibility - it deals with cohat information thus an organisation can collect.

* security mechanisms

on the baris of network security factor the security mechanism classified two mesure categories pervesrvaly mechanism.

pervecive security mechanism

mechanism. The may be in co-roporate into appropriate, protocal layer in-order to. provide some -of the OSI security services

denile of service attract mains and attend to prevent authorise user from excessing some services which they are eligible for

for example ⇒ an unotherised user mean send to many request to the server by using some random user id and passwords in with succesion and because of this to many request in do the the nebours, network may get slow - down or other authorise user connect excess the nebours in time. to mak a network peller these type of attacks are incore. thise is known as dinile of service.

The difference between acceve vertax and passive vertax

active vertax	passive attaver vertax
① active vertax are base on modification of origional massage	① passive attracks the attacker a serch the massage only
② The contains of origional massage are modified	② There is no modifiedion in provisional massage
③ The active attracks are easy to detect	③ are hard to detected
④ active attracks are hard to protect	④ easy to prevent

⑤ active vertax are
narpirate attracks,
modificatio attacks,
derivece service.

release to massage
The respectively easy
to trafic analisis

* Security services * (principle)
it is the important term
in network security. OSI architiecture. security
principlals are the building block to identify
the types of attack solution for attacks
there are the rect of standard that are
designed to minimize the Vulneratility
of and services to attracker to may
update on unauthorise dekses to sensitive
and important data first use a.
∴ there are diffrent security
services.

①
The confidetionality principle of
security state that only intended
sender and reciver should be able
to express masseges. if an unauthorred
person gets accest the to thise massage
the confidtionility gets comporimise.
for exsamepe=)
user A want to send a
massage to user B and A the
smart want someone else to get

excess to this message but if user some-one gets excess to these message, which is not desired then the purpose confidentiality to gets take there need to intercept that is if user c excess the message for email send by user a to user B, without permission of A and B then it is called interception and it causes lost of confidentiality

② authentication:

The authentication principle of security establish to of identify it ensure that origin of document or electronic message is correctly identified.

for example:

suppose user x send a message to user y and user said post on user x. while sending message to user y now output user y know that message from x said. and not from x. these leads to the fabricate attacks.

The attacker can act as user x. and sends front request. from x account to a bank. Now bank will transfer the fund

as requested from x account to account y, (attacker)
Now - y, may again send the fond transfer request to the bank as if he is account x. so bank may transfer the fond once agin from acount x to acound y. in absence proper authentication mechanism.

* integrating attack *
integrating principal of security states that the massage should not be altered we can say that when a contained of the massage change after sender sends it, but before it reaches to the reciver (or, Cintended reciver) if someone else make changes then integrating of massage is lost
for ex suppose user x send a massage to user y. and attacker z some how gets excess to these massage and changes the contained of massage and then sending to user y but affiqely user x and user y does not have any idea that the contained of massage has be altred these attack is known as lost of massage

integrating

* non- Repudedation:

non-Repudedation of network security does not allow the sender of the massage to repute the name of non-sending that massage.
There are some situation when user send the massg and dated refuses that H He or she and send that massage

for exp) user X. send request to bank. for fund transfer over the internate after the bank performs fund transfer load on, user X request, user X. can not plane that he had never send fund transfer request to bank.

there principle of security defids such posibbilites of denined something after having done it.

② excess control:

excess control principle of security determines we to should be able to acces thought
i.e we can specify that what user can acces which functions.

for example

we can specify that user x can view the data base records user y can view and update the database record and user z can perform all the action on database record. there principal is broadly realated two areas role manggement and rule managment

where role mbngyment concentrades on user side

which user can do thaght and rule managment concentrades on the resource side. i.e which resources is availlable

excess control list is a subset of the excess control mathrate.

Digital signature ⇒
it provides some major securi
feature like data is attach with
cryptographic transformation of a data uni
that allows the reciver of data to prov
the authenticate source and integrity
of data is also protects against some
sort of attacks.

* Excess control ⇒
it provides some excess rights to
resources.

* Data integrity ⇒
it a varity of mechanism are
to assure that the integrity of data
unit or stream of data is maintained.

* Authentification ⇒
authentification mechanism
of extend.
by means of intermission
exchange.

Traffic padding ⇒
it is a mechanism in which
the loss of data and will be restor
and then there is gap between

datastream due to loss of the data it will be overcome

* Routing control ⇒
  it enables a selection of a perticular physically secure routes for certain data it allows the some routing changes especially when the data security is suspended notarization it is the use of trusted neared party acces to esure certain properties of data exchange.

* Data in cybernet ⇒
  in these mechanism we can use certain mathematical algorithm to transfer the data into a form in which data is not easily widable. the transformation on securing of data depends on mathematical algorithm which is use for maintaining security of data.

* permehesive security mechanis ⇒
  in these mechanism. there are diffrent methods that are not specific To any (OSI) security service the mechanism are listed as below trusted functionallity in these mechanism you can establish some security policy.

for securing the data while transmitting over th networks

④ security labbed ⇒
in these mechanism the marking pound to the resources are maintained we use diffrent security atributes for that resources,

* event detection ⇒
is a mechanism that includes security realated event

* security recovery ⇒
it deals with the request from mechanism such as event handling managgement fonction e.t.c and. takes some recovery action

* symentric cycle model ⇒
The ABE, broadly contains the five important componants for encoding the plane text using a certain algorithum and a secretly to convert into cyber text these cyber text can be decoded i.e converted again into plane x using decoding algorithum the componentr are

1. plane text
2. encryption algoritham
3. secretely key
4. cypher text
5. decorption algoritham

1. plane text ⇒
   there is vorigional marrage or data which is field into the algoritham i.e. encryption algoritham is an input encryption algoritham the encryption algoritham performs various substitution and transformation on the plane text and it use the encrypted data, i.e cyber text.
   it may use one or more secrate keys

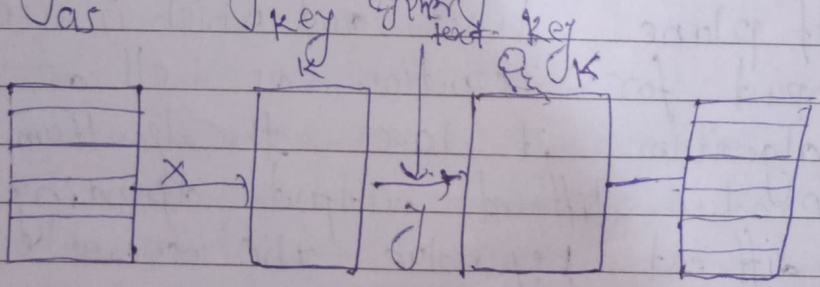
2. secrate key ⇒
   is a value which is independant of plane text and which it use as an input for incoption as well as decryption algoritam it haves the algoritham to produce diffrent output depending on diffrent key value. The secrete key is require for substitution and transformation technique to convert a plane text into cyber text.

① encryption algorithm:

this is a scrampled mess produce as produce as output as a result of encryption it depends on plane text and the secrate key for a given message two different keys will produce two diffrent cypher text the cypher text is apperently random stream of data and it is not easily understandable.

② decryption algorithm:

decryption algoritham is especially the encryption algoritham run in reverse. it take cypher text as an input as well as secrate key to produce original plane text message. a typicall symentric cycle model can be shown as



plaine text — encryption Algoritham $y = e(K, X)$ — decryption Algoritham $x = d(K, y)$ — plainted X

* ~~Crypto graphy~~ ⇒

crypto graphy is a technique for archiving the security by converting — decoding the plane text message into a non-readable format hence cryptography is responcible for archeving the security of data. in simple words we can say that crypto graphy is a scienes of secreate writing code for archieving the security of information. cryptography is a very old technique in which some secrate code writing perform for archeving the security of plane text. for any kind of attackers to make it responcible for the data violation data telecomonication system cryptography is necessary when you're comonicating over some unsecured medium like internate. there are five primary fonction of cryptography

① ~~auth~~ confidentinility or privacy ⇒
it ensure that know third party person other than the trusted one can excess(read) the data.

② authentication ⇒ it is the process of providing some security identity of to the user of length system.