

max. neighbour
likelihood decoding
is not as

(decodes tree codes)

Page No. :

Date : / /

7 or 6 marks

Sequential Decoding :- ① It is a decoding algo. for long constraint lengths conv. codes.

② This may not be accurate as Viterbi algo. but it is substantially ^{amount of comp. req.} _{m/m.}

③ It explores the code tree in such a way to try to minimize the computational cost & memory reqd. to store the tree.

④ We have two algo :- ① Stack algo

② Fano algo

③ Grepper given by Robert fano algo

STACK ALGO :- It is simplest algo. to describe a stack in which best n-paths described founded so far are stored.

FANO ALGO :- ① It has very low memory requirements.

② It donot req. stack.

③ It can only operate on code tree, \therefore it can't examine path merging (in case of trellis tree)

Fano algo repair reclaims info. repair in 3 paths :-

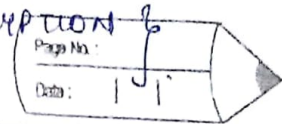
① current

② Immediate predecessor path

③ one of its successor path

Based on this info, FANO algo can move from current to either its pred. or succ. path.
 \therefore No stack reqd.

Cipher text → Unintelligible data
plain → intelligible to un-intelligible → ENCRYPTION



CRYPTOGRAPHY :-

- (A) Sym.
- (B) Asym.

Purpose :-

- ① Authentication
- ② Private
- ③ Integrity
- ④ Confidential

Accuracy

Cipher text

It is a science of converting a plain intelligible data into a un-intelligible data (garbage data) & again re-transforming message into ORIGINAL form. (so easily retrieved by Receiver)

apps :-

- ① Defence
- ② Data Security
- ③ IPS (Internet Payment System)
- ④ Business transaction
- ⑤ E-commerce (Electronic-Commerce)
- ⑥ Secure Data Comm.

① Sym. cryptography : ① It is also called "Secret key".

② Sender & Receiver uses same key and encryption or decryption algo. to encrypt or decrypt data.

② Asym. Cryptography : ① Also called "Public key cryptography"

② Sender & Receiver uses diff. keys for encryption & decryption namely PUBLIC & PRIVATE keys.

Defⁿ of Encryption } & cyphertext
 Decryption
 Cryptography } → GREEK word

Page No.:
 Date: | |

Security Threats :- ① Active attacks : dlla.

3rd p. modify data
 → read, change & send it to other

② Passive Attack :- Third person (Attacker) can only read data but can't modify it.

Passive attacks' types :- (A) RMC
 (Release of Message content) ↗ same as message reading

(B) Traffic Analysis

→ length of msg
 (कितना शब्द) who sent to
 → what OS is used?
 → comb. of above three & can try to guess msg

① Active Attacks types :- ① DOS (Deny of Service)

eg:- FB server has limit 100

hacker sends friend request many a times, so server becomes busy, so we can't be able to send requests. It is DOS.

(B) Replay

(msg. dte-dte send karati by Third person)

(C) Masquerade (On fb talking with friend as girl)

(d) Modify msg

