Security Part 2 1999 (more?) (repetitive for last 4 Qs?)

Give examples of the use of a block cipher to provide assurance of confidentiality, integrity, timeliness, covertness and resistance to jamming. In each case ~~give~~ describe a possible application and indicate the mode of operation you would use. 18 pts RJA

Model answer

Confidentiality: in an email encryption system such as PGP, a block cipher is used in CBC mode to provide this.

Integrity: in bank messaging systems, a DES MAC may be used to assure message integrity.

Timeliness: in Kerberos, tickets which give access to resources contain a timestamp from the ticket granting sever, and are encrypted using DES CBC

Covertness: in steganographic systems, a stream cipher such as DES in OFB mode may be used to to select pixels in a cover image, or sound samples in an audio file, in which a message is hidden

Resistance to jamming: Fire control radars typically delay the outgoing pulse train using a lag sequence which limits opponents to follower jamming or using enough power to obscure the return signal completely. A block cipher in OFB or CFB mode may be used for this (CFB is better because of sliding window correlators