Introduction to Security (1B) 2001

p 3 q 4
p 10 q 5
RJA

Which mode (or modes) of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect the following:

(1) interbank funds transfers

(2) email messages

(3) a high-frequency radio modem link

(4) passwords stored on a local disk

(5) the pulse train from a gearbox sensor to the tachograph in a truck

Model answer

(1) MAC for authenticity, plus maybe OFB or CBC for confidentiality

(2) CBC for confidentiality

(3) CFB to recover from bit slip / synch errors / burst errors; perhaps OFB + synch protocol instead

(4) ECB, maybe multiple times

(5) Goal is to prevent substitution, delay or repetition. Various ways to do this, e.g. CBC with maybe a synch protocol. ECB, CFB are bad.