

**Α 44 – ΚΡΥΠΤΟΓΡΑΦΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #1**

ΘΕΟΔΩΤΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

(1) Σχεδιάστε και υλοποιήστε ένα τμηματικό κώδικα (block cipher) με τις παρακάτω παραμέτρους:

- μέγεθος τμήματος: 8 χαρακτήρες,
- μέγεθος κειδιού: 6 χαρακτήρες,
- αριθμός γύρων: 4.

Χρησιμοποιήστε τον κώδικα που σχεδιάσατε σε ECB mode και CBC mode για να κρυπτογραφήσετε τα μηνύματα

- **ΠΟΥΛΗΣΕ ΔΕΚΑ ΜΕΤΟΧΕΣ**
- **ΑΓΟΡΑΣΕ ΔΕΚΑ ΜΕΤΟΧΕΣ**

Παρατηρήστε τη βασική αδυναμία του ECB mode.