Οι εργασίες είναι ο μοναδικός τρόπος εξέτασης του μαθήματος και γίνονται από ομάδες μέχρι 3 άτομα. Η κάθε ομάδα δηλώνει την πρόθεση εξέτασής της με email στο kpatsak@unipi.gr με θέμα "**ΘΠΚ2021 Δήλωση ομάδας**" και στο σώμα τα στοιχεία των μελών της ομάδας. Ο διδάσκοντας θα σας απαντήσει ποια από τις 4 εργασίες θα σας ανατεθεί. Η εργασία πρέπει να κατατεθεί μέχρι τις **23/7** και η κάθε ομάδα θα παρουσιάσει **26/7**.

Εργασία 1 Ο χρήστης περνάει σαν παραμέτρους τις διαστάσεις των κωδίκων που θα δημιουργηθούν και όποιες άλλες απαραίτητες παράμετροι κρίνετε ότι χρειάζονται. Το πρόγραμμά σας δημιουργεί κάθε φορά τυχαίους γραμμικούς κώδικες C_1, C_2 με γεννήτορες πίνακες G_1, G_2. Επιπλέον, ο χρήστης δηλώνει το κείμενο msg προς κωδικοποίηση. Έστω πίνακες S, P, υπολόγίστε τον πίνακα $G' = S \times G_1 \times P$ και κωδικοποιήστε το μήνυμα msg ως $c = msg \times G'$.

Στείλτε για κωδικοποίηση το μήνυμα c με τον κώδικα C_2 και προσθέστε τυχαίο θόρυβο (μικρότερο της ελάχιστης απόστασης του κώδικα C_2) για να πάρετε το μήνυμα c'. Εμφανίζετε στον χρήστη την αποκωδικοποίηση του c'.

Εργασία 2 Ο χρήστης περνάει σαν παραμέτρους τις διαστάσεις των κωδίκων που θα δημιουργηθούν και όποιες άλλες απαραίτητες παράμετροι κρίνετε ότι χρειάζονται. Το πρόγραμμά σας δημιουργεί κάθε φορά τυχαίους κυκλικούς κώδικες C_1, C_2 με γεννήτορες πίνακες G_1, G_2. Επιπλέον, ο χρήστης δηλώνει το κείμενο msg προς κωδικοποίηση. Έστω πίνακες S, P, υπολόγίστε τον πίνακα $G' = S \times G_1 \times P$ και κωδικοποιήστε το μήνυμα msg ως $c = msg \times G'$.

Στείλτε για κωδικοποίηση το μήνυμα c με τον κώδικα C_2 και προσθέστε τυχαίο θόρυβο (μικρότερο της ελάχιστης απόστασης του κώδικα C_2) για να πάρετε το μήνυμα c'. Εμφανίζετε στον χρήστη την αποκωδικοποίηση του c'.

Εργασία 3 Ο χρήστης περνάει σαν παραμέτρους τις διαστάσεις των κωδίκων που θα δημιουργηθούν και όποιες άλλες απαραίτητες παράμετροι κρίνετε ότι χρειάζονται. Το πρόγραμμά σας δημιουργεί κάθε φορά τυχαίους κώδικες C_1, C_2 με γεννήτορες πίνακες G_1, G_2, όπου C_1 γραμμικός και C_2 κυκλικός. Επιπλέον, ο χρήστης δηλώνει το κείμενο msg προς κωδικοποίηση. Έστω πίνακες S, P, υπολόγίστε τον πίνακα $G' = S \times G_1 \times P$ και κωδικοποιήστε το μήνυμα msg ως $c = msg \times G'$.

Στείλτε για κωδικοποίηση το μήνυμα c με τον κώδικα C_2 και προσθέστε τυχαίο θόρυβο (μικρότερο της ελάχιστης απόστασης του κώδικα C_2) για να πάρετε το μήνυμα c'. Εμφανίζετε στον χρήστη την αποκωδικοποίηση του c'.

Εργασία 4 Ο χρήστης περνάει σαν παραμέτρους τις διαστάσεις των κωδίκων που θα δημιουργηθούν και όποιες άλλες απαραίτητες παράμετροι κρίνετε ότι χρειάζονται. Το πρόγραμμά σας δημιουργεί κάθε φορά τυχαίους κώδικες C_1, C_2 με γεννήτορες πίνακες G_1, G_2, όπου C_1 κυκλικός και C_2 γραμμικός. Επιπλέον, ο χρήστης δηλώνει το κείμενο msg προς κωδικοποίηση. Έστω πίνακες S, P, υπολόγίστε τον πίνακα $G' = S \times G_1 \times P$ και κωδικοποιήστε το μήνυμα msg ως $c = msg \times G'$.

Στείλτε για κωδικοποίηση το μήνυμα c με τον κώδικα C_2 και προσθέστε τυχαίο θόρυβο (μικρότερο της ελάχιστης απόστασης του κώδικα C_2) για να πάρετε το μήνυμα c'. Εμφανίζετε στον χρήστη την αποκωδικοποίηση του c'.

Σημείωσεις για όλες τις εργασίες Όπου αναφέρεται τυχαίος πίνακας, κώδικας κτλ. σημαίνει ότι κάθε φορά το δημιουργείτε από την αρχή με τυχαίο τρόπο.

Το κείμενο πρέπει να χωρίζεται σε τμήματα του κατάλληλου μήκους! Αν το μήκος του κειμένου msg ή c δεν είναι όσο χρειάζεται ο κώδικάς σας, προσθέστε στο τέλος του μηνύματος το μήκος του κειμένου ως ένα string 4 χαρακτήρων, και όσα τυχαία bits χρειάζονται πριν από αυτό για να έχει το απαιτούμενο μήκος.

Πίνακας P: Τυχαία μετάθεση του μοναδιαίου πίνακα. Παράδειγμα: $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Πίνακας S: Τυχαίος αντιστρέψιμος πίνακας

Προσοχή: Το κείμενο πρέπει να χωρίζεται σε τμήματα του κατάλληλου μήκους! Αν το μήκος του κειμένου msg ή c δεν είναι όσο χρειάζεται ο κώδικάς σας, προσθέστε στο τέλος του μηνύματος το μήκος του κειμένου ως ένα string 4 χαρακτήρων, και όσα τυχαία bits χρειάζονται πριν από αυτό για να έχει το απαιτούμενο μήκος.