

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 , υπολογίστε 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' .

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.

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 , υπολογίστε 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' .

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.

Σημειώσεις για όλες τις εργασίες

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