4η Εργαστηριακή Άσκηση του Μαθήματος "Θεωρία Γραφημάτων"

Τμήμα: Μηχανικών Η/Υ & Πληροφορικής
Διδάσκων: Ιωσήφ Πολενάκης
Ημερομηνία: 15/3/2023

1. Το G είναι ένα μη-κατευθυνόμενο άκυκλο γράφημα. Αποδείξτε ότι κάθε συνεκτικό υπο-γράφημα του G θα είναι και επαγόμενο υπο-γράφημα του G. [2 Μονάδες]

2. Το G είναι ένα μη-κατευθυνόμενο άκυκλο γράφημα, και τα γραφήματα $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ είναι συνεκτικά υπο-γραφήματα του G. Αποδείξτε ότι, αν τα G_1, G_2 έχουν κοινές κορυφές, το γράφημα $(V_1 \cap V_2, E_1 \cap E_2)$ θα είναι συνεκτικό. [2 Μονάδες]

CONFIDENTIAL

3. Κατά τη παρακολούθηση για την εξάρθρωση μιας σπείρας κακοποιών, αναλαμβάνετε το ρόλο ενός αναλυτή πληροφοριών στο πλευρό των μυστικών υπηρεσιών. Για την συγκεκριμένη σπείρα υπάρχουν αδιάσειστα στοιχεία ότι [redacted] και [redacted] ενώ μάλιστα αποδείχθηκε ότι [redacted]. Όπως αναφέρεται σε απόρρητο έγγραφο της υπηρεσίας με Αρ. Πρωτ. [redacted] ο φερόμενος ως αρχηγός της σπείρας [redacted] εμπλέκεται σε [redacted], [redacted] και [redacted]. Για τη συγκεκριμένη αποστολή, καλείστε να υλοποιήσετε ένα σύστημα το οποίο να ορίζει ένα δίκτυο διοχέτευσης πληροφοριών μεταξύ "πρακτόρων". Το δίκτυο θα πρέπει να αναπαρίσταται με τρόπο ώστε να μην είναι εμφανής η δομή του και να μπορεί να το μεταφέρει ο εκάστοτε πληροφοριοδότης (για τη συγκεκριμένη αποστολή ο κύριος [redacted] στα κεντρικά της υπηρεσίας (στον αρχηγό της μυστικής υπηρεσίας, κύριο [redacted] ώστε ο ίδιος στη συνέχεια να μπορεί μέσω της αναπαράστασης να κατασκευάζει το αντίστοιχο δίκτυο διοχέτευσης πληροφοριών και να το χρησιμοποιεί για να ενημερώνει τους "πράκτορες". Για λόγους ασφαλείας, καλείστε επιπρόσθετα να υλοποιήσετε κατάλληλη ρουτίνα κρυπτογράφησης τύπου:

a) είτε «ολίσθησης», όπου δεδομένου ενός ακεραίου *K* ως μυστικό κλειδί, θα προσαυξάνονται οι τιμές της αναπαράστασης κατά (*K*) προκειμένου να δημιουργηθεί το κρυπτοκείμενο (μετατοπισμένη αναπαράσταση) ενώ αντίστροφα θα μειώνονται κατά (*K*) προκειμένου να δημιουργηθεί το αποκρυπτογραφημένο μήνυμα (αρχική αναπαράσταση),

b) είτε «μετάθεσης», όπου η μετάθεση S (ίση με το μήκος της αναπαράστασης) θα αποτελεί μυστικό κλειδί, με τα στοιχεία της αναπαράστασης των πρακτόρων να αναδιατάσσονται σύμφωνα με την θέση τους στη μετάθεση S.

Επιλέγοντας προς υλοποίηση έναν από τους δύο προτεινόμενους τύπους (όποιον επιθυμείτε εσείς), θα πρέπει να ακολουθήσετε την εξής ροή εκτέλεσης:

Encoding >> *Encryption* >> *Decryption* >> Decoding

Το δίκτυο των "πρακτόρων" με κωδικό όνομα [redacted] παρατίθεται στη συνέχεια μέσω των αναγνωριστικών ονομασιών των πρακτόρων με αμφίδρομη σχέση {αποστολέα-παραλήπτη} ως εξής:

[Alpha-Charlie]; [Alpha-Golf]; [Bravo-Delta]; [Delta-Alpha];
[Delta-Echo]; [Echo-Fox]; [Echo-Hotel];

- *Η παράδοση του σχετικού λογισμικού θα γίνει την Τετάρτη 22/3 στις 23:55 στο σημείο* [redacted] *υπόψιν του κυρίου* [redacted].
- *Οι κωδικοί συνθήματος και παρασυνθήματος είναι* [redacted] *και* [redacted].

[6 Μονάδες]