Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Σχολή Θετικών Επιστημών

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Κρυπτογραφία

Project I. Συμμετρική Κρυπτογραφία

Διδάσκων. Κ. Α. Δραζιώτης

Οδηγιες

1. Το project να παραδοθεί εώς **/**/**. Η εργασία αυτή αποτελεί το πρώτο μέρος της υποχρεωτικής εργασίας σας.
2. Οι ασκήσεις υπάρχουν στο textbook στο elearning.
3. Όλες οι ασκήσεις είναι ισοδύναμες (0.2 μονάδες η κάθε μία). Σύνολο 2 μονάδες.
4. Η εργασία προτείνουμε να γραφτει στο σύστημα LaTex. Μπορείτε να χρησιμοποιήσετε το template εδώ.
5. Να σταλεί το tex+pdf+κώδικας σε ένα zip file. Όλες οι ασκήσεις να βρίσκονται σε ένα tex αρχείο και όχι ξεχωριστά σε πολλά. Σε ασκήσεις που απαιτούν μόνο κώδικα, εκτός του κώδικα, να δοθεί στο τεχ και μια σύντομη ανάλυση και να σχολιαστούν τα αποτελέσματα. Σε περίπτωση που δεν τα καταφέρετε με το tex, μπορείτε να χρησιμοποιήσετε libreoffice.
7. Να μην εισάγετε τον κώδικα σας μέσα στο τεχ.
8. Η γλώσσα προγραμματισμού που θα χρησιμοποιήσετε θα είναι είτε Python 3 είτε C/C++ (με compiler gcc). Σε περίπτωση που χρησιμοποιήσετε ειδικές βιβλιοθήκες, πρέπει να αναφέρετε ποιες είναι και πως μπορούν να εγκατασταθούν.
9. Έχει σημασία και η στυλιστική παρουσίαση. Δηλαδή θα βαθμολογηθεί ο τρόπος που θα παρουσιάσετε τις λύσεις καθώς και το στιλιστικό κομμάτι (π.χ. οι μαθηματικοί τύποι πρέπει να φαίνονται σωστά κ.λπ.)
10. Απαγορεύεται αυστηρά ο πλαγιαρισμός. Εκτεταμένη και αποδεδειγμένη χρήση του, θα συνεπάγεται τον μηδενισμό όλης της εργασίας. Για παράδειγμα αν χρησιμοποιήσετε κώδικα από το stackexhange να δοθεί το link. Επίσης, μπορεί να ζητηθεί από τον διδάσκοντα κάποια προφορική συνεδρία για να εξηγήσετε το σκεπτικό κάποιας λύσης ή τον κώδικα.
11. Υπάρχουν κάποιες ασκήσεις που η θεωρία τους δεν έχει αναπτυχθεί στο μάθημα. π.χ. το θέμα 2. Είναι εύκολες ασκήσεις, απλά θα χρειαστεί ίσως να ανατρέξετε σε λίγη θεωρία που δεν έχουμε πει.

Καλή διασκέδαση!

Καλή επιτυχία

Άσκηση 1. Άσκηση 2.2 (σελ. 18)
Άσκηση 2. Άσκηση 2.3 (σελ. 18)
Άσκηση 3. Άσκηση 2.4 (σελ. 18)
Άσκηση 4. Άσκηση 2.5 (σελ. 19)
Άσκηση 5. Άσκηση 2.6 (σελ 19)
Άσκηση 6. Άσκηση 3.6 (σελ 33)
Άσκηση 7. Άσκηση 3.8 (σελ. 34)
Άσκηση 8. Άσκηση 4.3 (σελ. 43)
Άσκηση 9. Άσκηση 4.7 (σελ. 49)

Άσκηση 10. (CTF-like) Μπορείτε να ανοίξετε το secure.zip?
Hint. Ότι χρειάζεστε είναι στην διαφάνεια course-1-Introduction.pdf στο elearning.