

Άσκηση ανταλλαγής μηνυμάτων με χρήση Ψηφιακού Φακέλου (Digital Envelope)

Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί είναι ασύμμετρα κρυπτογραφημένο με κλειδί το δημόσιο κλειδί της αντίθετης πλευράς.

Η άσκηση θα πραγματοποιηθεί σε ζευγάρια φοιτητών.

Αρχικά θα πρέπει ο καθένας να γνωρίζει το email του άλλου, να υπάρχει το Cryptool στον υπολογιστή του και να έχει δημιουργήσει ζεύγος δημόσιου – ιδιωτικού κλειδιού.

Θα χρησιμοποιήσουμε σε συνδυασμό το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

Διαδικασία της άσκησης :

Ας υποθέσουμε ότι ο φοιτητής S (sender) θέλει να στείλει μήνυμα στον φοιτητή R (receiver).

Ο R στέλνει στον S με mail το δημόσιο κλειδί του.

Ο S διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το συμμετρικό κλειδί με το δημόσιο κλειδί του R.

Ο S στέλνει στον R με mail το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί.

Ο R για να διαβάσει το μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί.

Η άσκηση θα επαναληφθεί αφού τα ζευγάρια των φοιτητών αλλάξουν ρόλους. Ο αποστολέας δηλαδή θα γίνει τώρα παραλήπτης.