ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (Εργαστήριο)

Ενότητα 4

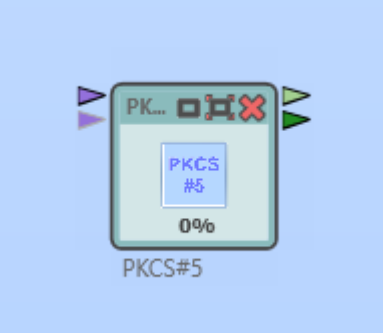
Ασφαλής Μετάδοση Κρυπτογραφημένου και Υπογεγγραμένου Μηνύματος

Εργαστηριακή Άσκηση 4: Υπογραφή, κρυπτογράφηση και αποστολή μηνύματος και ισχυρού κλειδιού κρυπτογράφησης

Στη σημερινή άσκηση θα επεκτείνουμε τις έννοιες που αναπτύξαμε στην Ενότητα 3 ώστε να διασφαλίσουμε περαιτέρω την επικοινωνία μεταξύ 2 άκρων ενισχύοντας τόσο την εμπιστευτικότητα (μέσω της χρήσης ισχυρού κλειδιού κρυπτογράφησης) όσο και την αυθεντικοποίηση και ακεραιότητα του μηνύματος (με τη χρήση ψηφιακών υπογραφών).

Δημιουργία ισχυρού κλειδιού κρυπτογράφησης με τη χρήση του προτύπου PKCS#5

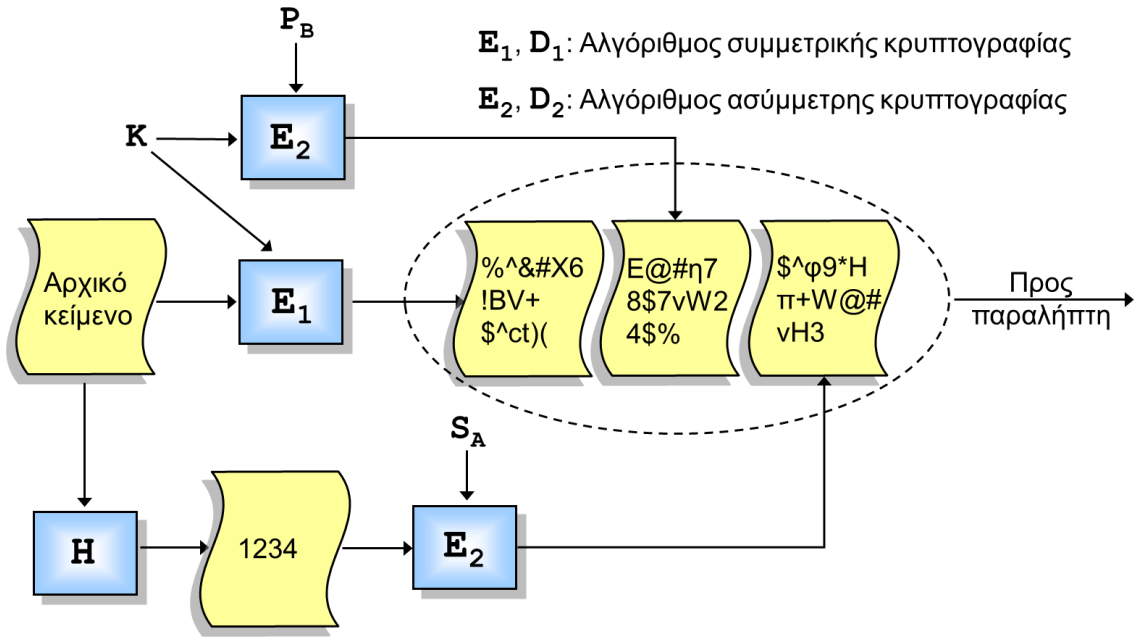
Η οικογένεια των πρότυπων **PKCS#X** αποτελεί μια σειρά από τυποποιήσεις για την χρήση «ισχυρών» κλειδιών σε αλγορίθμους κρυπτογράφησης, όπως ο **RSA** και ο **AES**. Ο σκοπός τους είναι η δημιουργία περίπλοκων κλειδιών έτσι ώστε να γίνεται ακόμα πιο δύσκολη η κρυπτανάλυση με τη μέθοδο brute-force, ενός κρυπτογραφημένου μηνύματος που έχει υποκλαπεί κατά την αποστολή του προς τον παραλήπτη. Συγκεκριμένα, στη σημερινή άσκηση θα χρησιμοποιήσετε το component PKCS#5 στην είσοδο του οποίου θα συνδέσετε το κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση του συμμετρικού κλειδιού. Για την ολοκλήρωση της άσκησης θα πρέπει να χρησιμοποιήσετε τις κατάλληλες εξόδους του component έτσι ώστε η μετάδοση του μηνύματος να ολοκληρωθεί με επιτυχία.



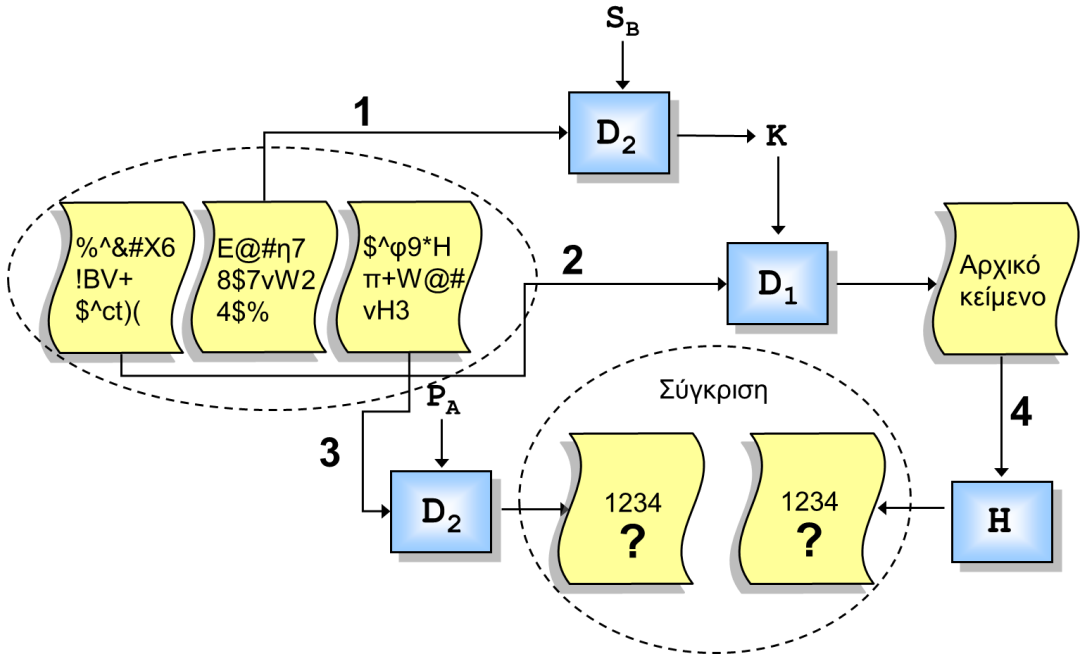
Εικόνα 1: Component PKCS#5

Επίσης, θα κληθείτε να δημιουργήσετε, με τη χρήση της συνάρτησης κατακερματισμού SHA (βλέπε σχετικό component στο Cryptool2) μια σύνοψη του αρχικού μηνύματος έτσι ώστε να μπορέσετε να δημιουργήσετε την απαραίτητη υπογραφή στο μήνυμα ώστε ο παραλήπτης να επαληθεύσει την ορθή λήψη αυτού. Η χρήση συναρτήσεων κατακερματισμού είχε πραγματοποιηθεί στην Ενότητα 1.

Υλοποιήσετε τη λειτουργικότητα που απεικονίζεται στις Εικόνες 2 και 3:



Εικόνα 2: Κρυπτογράφηση και υπογραφή κειμένου από τον αποστολέα (P_B: δημόσιο κλειδί παραλήπτη, S_A: ιδιωτικό κλειδί αποστολέα)



Εικόνα 3: Αποκρυπτογράφηση στον παραλήπτη (S_B: ιδιωτικό κλειδί παραλήπτη, P_A: δημόσιο κλειδί αποστολέα)

Συγκεκριμένα, για τις ανάγκες τις άσκησης αυτής θα πρέπει να κάνετε τα ακόλουθα βασισμένοι στο αρχείο του προηγούμενου εργαστηρίου:

1. Να κάνετε όλες τις απαραίτητες αλλαγές ώστε να κρυπτογραφείτε αρχείο αντί κειμένου.

2. Να κάνετε χρήση του PKCS#5 component για τη δημιουργία ισχυρού κλειδιού με τον τρόπο που περιγράφηκε παραπάνω. Ως είσοδο στο PKCS#5 θα δίνετε κάποιο password της επιλογής σας.

Υποσημείωση 1: Για τον AES χρησιμοποιήστε για Padding τη μέθοδο PKCS#7.

3. Να κάνετε όλες τις απαραίτητες προθήκες/αλλαγές στο project σας ώστε παράλληλα να υπογράφετε και το μη κρυπτογραφημένο αρχείο και να επαληθεύεται την υπογραφή σε αυτό. Για την επαλήθευση της υπογραφής χρησιμοποιήστε και το component "Comparators".

Υποσημείωση 2: Προφανώς για την υπογραφή θα πρέπει να χρησιμοποιήσετε ένα δεύτερο ζεύγος κλειδιών, αυτό του αποστολέα.