ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (Εργαστήριο)

Ενότητα 5

Ασφαλής Μετάδοση Κρυπτογραφημένου και Υπογεγγραμένου Μηνύματος

Εργαστηριακή Άσκηση 5: Βελτίωση του κρυπτοσυστήματος κρυπτογράφησης και υπογραφής μηνύματος

Στην ενότητα αυτή καλείστε να βελτιώσετε το κρυπτοσύστημα της ενότητας 4 με σκοπό

1. Να διορθώσετε το πρόβλημα ασφάλειας που έχει η υλοποίηση της ενότητας 4.
2. Να υιοθετήσετε τη χρήση των network components που προσφέρει το Cryptool ώστε η αποστολή και λήψη μηνυμάτων να γίνεται με τη χρήση δικτυακών components.

1. Βελτίωση της ασφάλειας του κρυπροσυστήματος της ενότητας 4

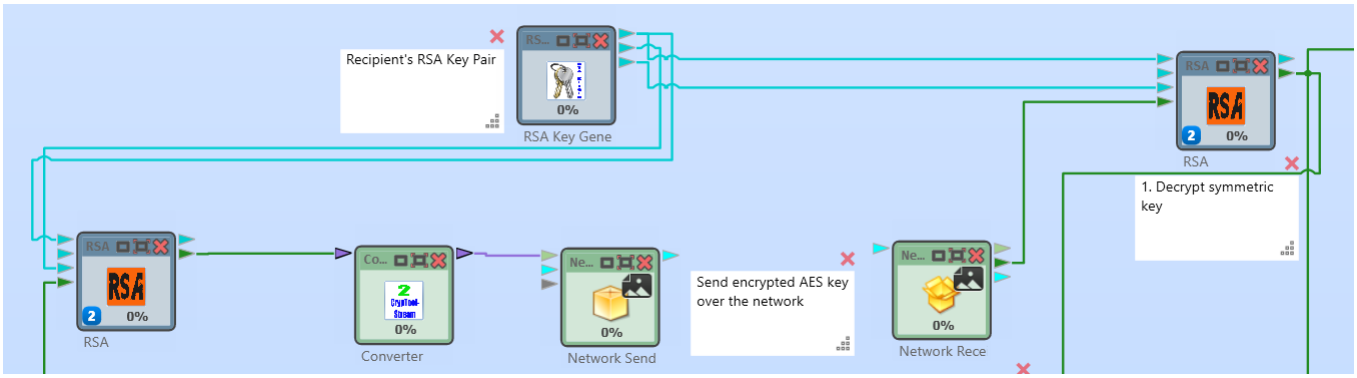
Το κρυπτοσύστημα της ενότητας 4 παρουσιάζει ένα πρόβλημα το οποίο επιτρέπει σε επιτιθέμενο να προσβάλει την αυθεντικοποίηση του μηνύματος το οποίο διακινείται. Προσπαθήστε να εντοπίσετε το πρόβλημα και προτείνετε λύση ώστε να βελτιώστε το εν λόγω κρυπτοσύστημα. Στη συνέχεια υλοποιήστε την προτεινόμενη λύση.

2. Χρήση των network components

Το Cryptool μας επιτρέπει, μεταξύ άλλων, να προσομοιώσουμε μια διαδικτυακή ανταλλαγή δεδομένων μεταξύ δύο οντοτήτων με τη χρήση των network sender και network receiver components. Έτσι θα πρέπει να διαχωρίσετε με λογικό τρόπο το κρυπτοσύστημα σας και να προσθέσετε τα απαιτούμενα network components έτσι ώστε ο αποστολέας να στέλνει στον παραλήπτη τα τρία διαφορετικά σετ δεδομένων, δηλ. το κρυπτογραφημένο κλειδί της συμμετρικής, το κρυπτογραφημένο αρχείο και την υπογραφή, δικτυακά.

Σημείωση 1: Σε ένα σωστά υλοποιημένο σύστημα τα τρία επιμέρους σετ δεδομένων θα πρέπει να συνενωθούν (με τη διαδικασία του concatenation) ώστε να αποτελέσουν ένα ενιαίο μήνυμα το οποίο φυσικά στον παραλήπτη θα πρέπει να διαχωριστεί ώστε να πάρει ο παραλήπτης τα τρία επιμέρους σετ και να τα επεξεργαστεί. Ωστόσο, επειδή αυτή η διαδικασία προσθέτει αρκετή πολυπλοκότητα, για τις ανάγκες αυτού του εργαστηρίου θα χρησιμοποιήσουμε τρία διαφορετικά σετ network components, ένα για κάθε ένα από τα προαναφερθέντα σετ δεδομένων.

Παράδειγμα: Η αποστολή του κρυπτογραφημένου κλειδιού της συμμετρικής με τη χρήση των network components μπορεί να υλοποιηθεί σύμφωνα με το σύστημα που απεικονίζεται στην Εικόνα 1.



Εικόνα 1: Χρήση network components

Στην παραπάνω υλοποίηση προσέξτε τη χρήση του converter component το οποίο χρησιμοποιείται αντί των encoders/decoders και μας βοηθά στην κωδικοποίηση των μηνυμάτων μεταξύ των components. Στην προκειμένη περίπτωση ο converter έχει χρησιμοποιηθεί για να μετατρέψει την έξοδο στου RSA σε *Cryptoolstream*, όπως απαιτεί η είσοδος του Network Sender component.

Σημείωση 2: Για την ορθή και προβλήματα χρήση των network components συνιστάται η ανταλλαγή μικρού όγκου δεδομένων, που δεν απαιτεί την επανένωση τεμαχισμένων πλαισίων στον παραλήπτη. Έτσι ως αρχείο εισόδου προς κρυπτογράφηση χρησιμοποιείστε ένα .txt αρχείο το οποίο θα περιλαμβάνει έναν πολύ περιορισμένο αριθμό λέξεων.

ΑΣΚΗΣΗ

Υλοποιήστε το παραπάνω κρυπτοσύστημα έτσι ώστε να γίνεται συνένωση των τριων επιμέρους μηνυμάτων πριν την αποστολή τους στον παραλήπτη, να στέλνονται με τη χρήση ενός και μόνο δικτυακού component, ενώ στην πλευρά του παραλήπτη τα τρία σετ δεδομένων να διαχωρίζονται με ορθό τρόπο πριν τα επεξεργαστεί ο παραλήπτης.