# ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (Εργαστήριο)

## Ενότητα 3

## Ασφαλής Μετάδοση Κρυπτογραφημένου Μηνύματος

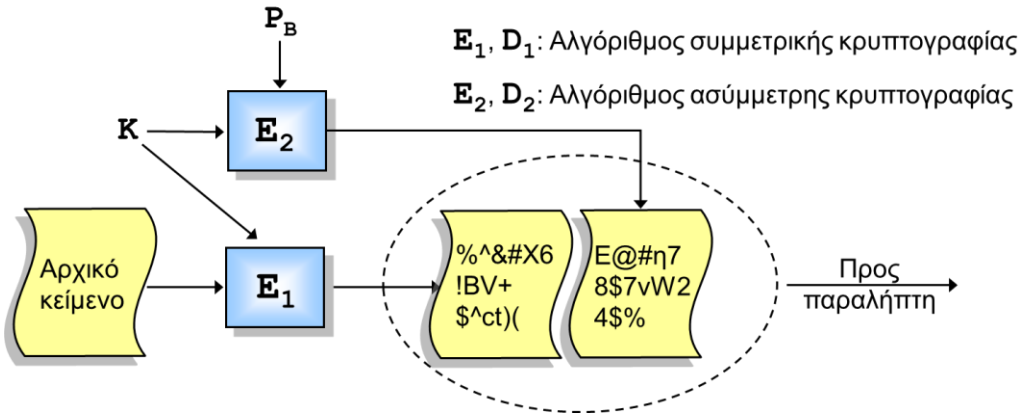
## Εργαστηριακή Άσκηση 3: Κρυπτογράφηση και αποστολή μηνύματος και κλειδιού κρυπτογράφησης

Στη σημερινή άσκηση θα εξετάσουμε την περίπτωση όπου 2 χρήστες που βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες θέλουν να επικοινωνήσουν με ασφάλεια (δηλαδή μέσα από ένα κρυπτογραφημένο κανάλι) κάνοντας χρήση κρυπτογραφίας για την εξασφάλιση της εμπιστευτικότητας στα μηνύματα τους. Όπως έχουμε αναφέρει, υπάρχουν 2 βασικές κατηγορίες αλγορίθμων κρυπτογράφησης:

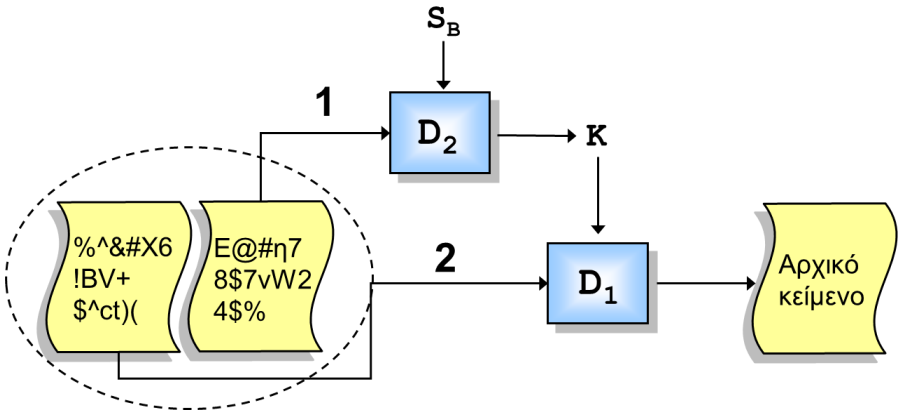
1. **Συμμετρική:** Χρησιμοποιούμε το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να διατηρείται μυστικό. Στην άσκηση θα χρησιμοποιήσουμε τον αλγόριθμο συμμετρικής κρυπτογράφησης **AES**, ο οποίος αποτελεί διεθνές πρότυπο**.**
2. **Ασύμμετρη ή Δημοσίου κλειδιού:** Χρησιμοποιούμε ζεύγη κλειδιών (δημόσιο και ιδιωτικό) για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο κάθε χρήστης έχει (τουλάχιστον) ένα δικό του ζεύγος κλειδιών. Για την κρυπτογράφηση, ο αποστολέας χρησιμοποιεί το **δημόσιο** κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα, και ο παραλήπτης το αποκρυπτογραφεί χρησιμοποιώντας το αντίστοιχο κλειδί του ζεύγους, δηλ. το **ιδιωτικό** του κλειδί. Στην άσκηση θα χρησιμοποιήσουμε τον αλγόριθμο δημοσίου κλειδιού **RSA.**

**Στη σημερινή άσκηση θα συνδυάσουμε τις παραπάνω κατηγορίες αλγορίθμων ώστε να αποστείλουμε με ασφάλεια: α) ένα μήνυμα και β) το κλειδί κρυπτογράφησης για το μήνυμα. Συγκεκριμένα, θα χρησιμοποιήσουμε συμμετρική κρυπτογράφηση για την κρυπτογράφηση του μηνύματος που θέλουμε να στείλουμε, και ασύμμετρη για την κρυπτογράφηση του κλειδιού της συμμετρικής με σκοπό την ασφαλή μετάδοση του στον παραλήπτη.** Ο παραλήπτης θα πρέπει να μπορεί να αποκρυπτογραφήσει το κλειδί της συμμετρικής κρυπτογράφησης και στη συνέχεια να το χρησιμοποιήσει για να αποκρυπτογραφήσει το μήνυμα.

Η λειτουργικότητα που καλούμαστε να υλοποιήσουμε απεικονίζεται στις Εικόνες 1 και 2.

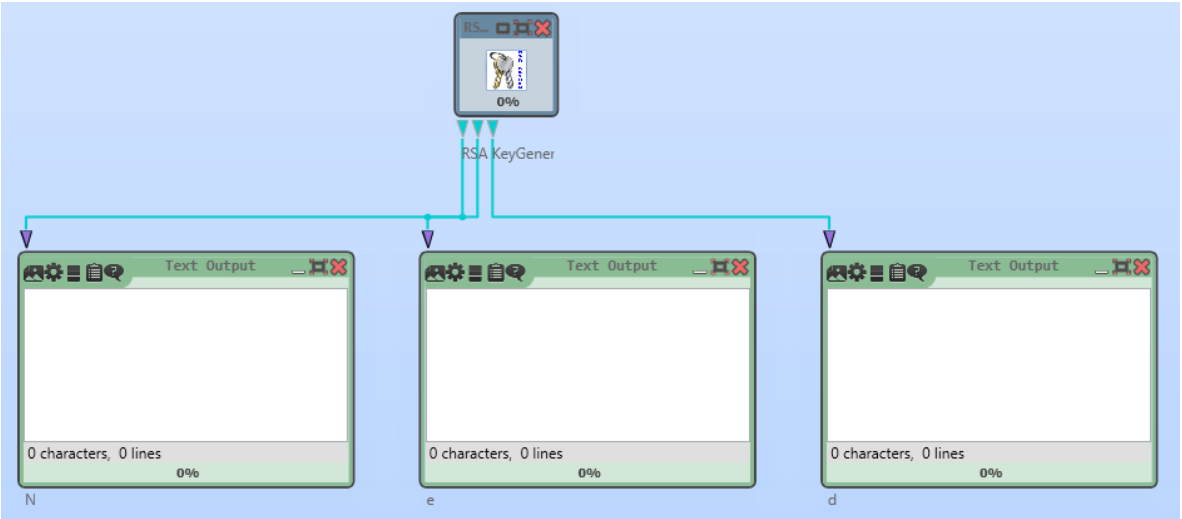



Εικόνα 1: Κρυπτογράφηση κειμένου από τον αποστολέα ($P_B$: δημόσιο κλειδί παραλήπτη)




Εικόνα 2: Αποκρυπτογράφηση στον παραλήπτη ($S_B$: ιδιωτικό κλειδί παραλήπτη)

Για τη δημιουργία των ασύμμετρων κλειδιών, θα χρησιμοποιήσετε το component του Cryptool2 με όνομα *RSA Key Generator* (Εικόνα 3).




Εικόνα 3: Γεννήτρια κλειδιών RSA

Η γεννήτρια παράγει το δημόσιο (modulus **N** + exponent **e**) και το ιδιωτικό κλειδί του ζεύγους (**d**). Για την ολοκλήρωση της άσκησης θα πρέπει να χρησιμοποιήσετε τις κατάλληλες εξόδους του RSA KeyGener τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση.

Σημείωση: για τη διευκόλυνση σας μπορείτε αρχικά να υλοποιήσετε τα δύο κρυπτοσυστήματα (της συμμετρικής και της ασύμμετρης) ξεχωριστά, ωστόσο στο ίδιο project του cryptool, και στη συνέχεια, αφού βεβαιωθείτε για την ορθή υλοποίηση τους, να προχωρήσετε στη διασύνδεση τους. Παρόμοια άσκηση για τη συμμετρική κρυπτογράφηση έχει γίνει σε προηγούμενο εργαστήριο με τον αλγόριθμο DES.