Ατομική Εργασία

Ασκήσεις Κρυπτογραφίας

Στην εργασία αυτή καλείστε να υλοποιήσετε ένα πρωτόκολλο KEM/DEM. Δηλαδή, ο αποστολέας (Alice) θα στείλει ένα μήνυμα (ή αρχείο) στον αποδέκτη (Bob) γνωρίζοντας μόνο το δημόσιο κλειδί του και χωρίς να έχουν επικοινωνήσει ποτέ και χωρίς να έχουν συμφωνήσει σε κάποιο κοινό μυστικό.

Στάδιο προετοιμασίας

Ο Bob δημιουργεί ένα ζευγάρι κλειδιών (prB, puB) και ο Ο Bob αποθηκεύει το ιδιωτικό του κλειδί prB. Οι πληροφορίες του στατικού δημόσιου κλειδιού puB του Bob προσδιορίζονται ανακτώνται από το τοπικό κατάστημα αξιοπιστίας (η Alice εχει αποκτήσει το puB, π.χ με τη βοήθεια υποδομής PKI).

Στάδιο κανονικής λειτουργίας

Η Alice θέλει να στείλει ένα plaintext M στον Bob, π.χ ένα συνημμένο το οποίο στέλνεται με ένα μήνυμα. Το επίπεδο της ασφάλειας θα είναι λ=128 bits. Το πρωτόκολλο λειτουργεί ως ακολούθως.

Alice:

1. Ένα εφήμερο ζευγάρι κλειδιών (prA,puA) συμφωνίας αρχικού κλειδιού ανά μήνυμα για την Alice κατασκευάζεται για τον απαιτούμενου τύπο καμπύλης.
2. Ένα κοινό μυστικό K δημιουργείται από τα κλειδιά (που αναφέρονται στο σημείο 1 και στο στάδιο προετοιμασίας) χρησιμοποιώντας το ECDH.
3. Το κοινό μυστικό K χρησιμοποιείται ως είσοδος στη μέθοδο παραγωγής κλειδιού (KDF) για την παραγωγή ενός κλειδιού K'.
4. Το κλειδί K' χρησιμοποιείται για την κρυπτογράφηση των συνημμένο M. Το παραγόμενο κρυπτογράφημα είναι το C και η ετικέτα tag.
5. Το κρυπτογράφημα C και η ετικέτα tag αποστέλλονται μαζί με το δημόσιο τμήμα puA του ζεύγους κλειδιών που κατασκευάστηκε στο βήμα 1.

Bob

1. Ο Bob λαμβάνει τα (C,tag, puA)
2. Το κοινό μυστικό K δημιουργείται από τα κλειδιά prB και puA χρησιμοποιώντας το ECDH.
3. Το κοινό μυστικό K χρησιμοποιείται ως είσοδος στη μέθοδο παραγωγής κλειδιού (KDF) για την παραγωγή ενός κλειδιού K'.
4. Το κλειδί K' χρησιμοποιείται για τον έλεγχο ακεραιότητας και την αποκρυπτογράφηση του C. Παράγεται το μήνυμα M ή το μήνυμα λάθους.

Καλείστε να υλοποιήσετε το πιο πάνω πρωτόκολλο χρησιμοποιώντας τους κατάλληλους κρυπτογραφικούς αλγορίθμους της επιλογής σας. Μπορεί να υλοποιηθεί σε οποιαδήποτε γλώσσα,

αλλά συστήνεται η Python για απλότητα. Μπορείτε να χρησιμοποιήσετε οποιαδήποτε από τις βιβλιοθήκες: PyNaCl, Cryptography, PyCryptodome.

Θα πρέπει να παραδώσετε:

- τον κώδικα με σχόλια και ένα παράδειγμα που λειτουργεί
- το κείμενο τεκμηρίωσης των επιλογών σας.