ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τεύχος Εργαστηριακών Ασκήσεων

Γεώργιος Καμπουράκης
Αναπληρωτής Καθηγητής
Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Μαρία Καρύδα
Επίκουρη Καθηγήτρια
Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Αναστασία Δούμα
ΕΔΙΠ Σχολής Θετικών Επιστημών

Μάριος Αναγνωστόπουλος - Ιωάννα Τόπα
Υποψήφιοι Διδάκτορες Τμήματος Μ.Π.Ε.Σ

Απρίλιος 2016

ΑΣΚΗΣΗ 3:
ΥΛΟΠΟΙΗΣΗ ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕ ΧΡΗΣΗ ΤΟΥ JAVA API.

Περιγραφή

Σκοπός της συγκεκριμένης εργασίας είναι κυρίως η εξοικείωση με το σύνολο των κλάσεων που παρέχονται από το Java API, με σκοπό την υλοποίηση μηχανισμών αυθεντικοποίησης, κρυπτογράφησης, σύνοψης και ψηφιακής υπογραφής. Οι μηχανισμοί αυτοί μπορούν να χρησιμοποιηθούν σε διάφορες εφαρμογές με απαιτήσεις ασφαλείας.

Στα πλαίσια της εργασίας καλείστε να δημιουργήσετε μία εφαρμογή, η οποία θα αποτελεί ένα σύστημα για την ασφαλή διαχείριση εσόδων/εξόδων. Σε πρώτη φάση, η εφαρμογή θα πρέπει να παρέχει τη δυνατότητα εγγραφής ενός χρήστη μέσω μίας απλής διεπαφής χρήστη (GUI). Η εφαρμογή σας στη συνέχεια θα πρέπει να είναι σε θέση να αυθεντικοποιεί τους χρήστες με σκοπό να παρέχει μηχανισμούς διασφάλισης της εμπιστευτικότητας και της ακεραιότητας των δεδομένων της εφαρμογής.

Κατά την πρώτη εκτέλεση, η εφαρμογή θα πρέπει να παράγει ένα ζεύγος Δημόσιου και Ιδιωτικού κλειδιού, το οποίο θα πρέπει να είναι ίδιο και κατά τις επόμενες εκτελέσεις της. Το δημόσιο κλειδί θα πρέπει να το αποθηκεύει σε ένα αρχείο που θα είναι προσβάσιμο από όλους. Το ιδιωτικό κλειδί της εφαρμογής μπορεί να είναι αποθηκευμένο και αυτό σε σχετικό αρχείο (δεν είναι σωστή πρακτική να αποθηκεύεται το ιδιωτικό κλειδί χωρίς να είναι προστατευμένο, αλλά στα πλαίσια της παρούσας εργασίας είναι αποδεκτό). Εναλλακτικά, μπορείτε να το ορίσετε ως σταθερά στον κώδικα της εφαρμογής σας.

Εγγραφή Χρήστη

Ο χρήστης κατά τη διαδικασία της εγγραφής του στη εφαρμογή θα πρέπει να έχει τη δυνατότητα να εισάγει το ονοματεπώνυμο του, ένα login name και ένα συνθηματικό της επιλογής του. Η εφαρμογή θα παράγει τη σύνοψη (hash) του συνθηματικού του χρήστη. Για την παραγωγή της σύνοψης θα χρησιμοποιείται μαζί με το συνθηματικό και ένα διαφορετικό τυχαίο αλφαριθμητικό (salt) για κάθε χρήστη. Το αποτέλεσμα της σύνοψης θα κρυπτογραφείται με το δημόσιο κλειδί της εφαρμογής. Όλα αυτά τα στοιχεία (όνομα χρήστη, login name, salt, κρυπτογραφημένο συνθηματικό) θα πρέπει να αποθηκεύονται σε σχετικό αρχείο που θα περιέχει τα στοιχεία όλων των χρηστών.

Επίσης η εφαρμογή για κάθε χρήστη θα παράγει ένα συμμετρικό κλειδί, το οποίο θα το κρυπτογραφεί με το δημόσιο κλειδί της και θα το αποθηκεύει σε αντίστοιχο αρχείο.

Αυθεντικοποίηση Χρήστη

Για να έχει τη δυνατότητα ο χρήστης να εισέλθει στην εφαρμογή θα πρέπει αρχικά να αυθεντικοποιηθεί. Πιο συγκεκριμένα, ο χρήστης θα εισάγει το όνομα χρήστη (login name) και το συνθηματικό του. Αμέσως μετά, η εφαρμογή θα παράγει τη σύνοψη του συνθηματικού ακολουθώντας ακριβώς την ίδια διαδικασία που εκτέλεσε κατά τη διαδικασία της εγγραφής. Στη συνέχεια, θα αναζητά το συνθηματικό του χρήστη στο αρχείο που έχει αποθηκευμένα τα στοιχεία όλων των χρηστών. Θα το αποκρυπτογραφεί με το ιδιωτικό της κλειδί και θα συγκρίνει τις 2 συνόψεις που έχει δημιουργήσει. Αν ταιριάζουν οι συνόψεις τότε ο χρήστης θα αυθεντικοποιείται επιτυχώς στο σύστημα.

Λειτουργίες Εφαρμογής

Όσοι χρήστες έχουν ακολουθήσει την παραπάνω διαδικασία εγγραφής και αυθεντικοποίησης θα έχουν τη δυνατότητα να χρησιμοποιήσουν την εφαρμογή για τη διαχείριση των εσόδων και των εξόδων τους. Για κάθε χρήστη, η εφαρμογή θα δημιουργεί ένα κατάλογο (directory) με το username του στον οποίο θα φυλάσσονται τα απαιτούμενα αρχεία. Θα πρέπει να υλοποιήσετε κατάλληλη διεπαφή, όπου ο χρήστης θα έχει τις παρακάτω δυνατότητες:

- **Εισαγωγή εγγραφής για έσοδα ή έξοδα:** Ο χρήστης θα πρέπει να έχει τη δυνατότητα να προσθέτει μία εγγραφή κάθε φορά που θα περιέχει την ημερομηνία συναλλαγής, μία περιγραφή και το ποσό. Για κάθε χρήστη, η εφαρμογή θα παρέχει δύο αρχεία αποθήκευσης, ένα για όλες τις εγγραφές που αφορούν τα έσοδα του χρήστη και ένα για τα έξοδα.

- **Τροποποίηση στοιχείων εγγραφής εσόδων ή εξόδων:** Ο χρήστης θα καθορίζει μία συγκεκριμένη ημερομηνία και θα έχει τη δυνατότητα να επιλέξει για τροποποίηση μια από τις συναλλαγές της συγκεκριμένης ημερομηνίας.

- **Έκδοση αναφοράς για τα έσοδα και τα έξοδα ανά μήνα:** Ο χρήστης θα επιλέγει κάποιο μήνα και θα εμφανίζονται αναλυτικά τα έσοδα και τα έξοδα για τον μήνα αυτό καθώς και συνολικό άθροισμα εσόδων/εξόδων.

Με την ολοκλήρωση της κάθε συναλλαγής, η εφαρμογή θα πρέπει να κρυπτογραφεί τα δεδομένα της συναλλαγής με το συμμετρικό κλειδί του χρήστη και να τα αποθηκεύει στο σχετικό αρχείο. Αντίστοιχα για την ανάγνωση των συναλλαγών του χρήστη θα πρέπει να εκτελείται η διαδικασία της αποκρυπτογράφησης των στοιχείων.

Μηχανισμός Ακεραιότητας

Η εφαρμογή θα πρέπει να εξασφαλίζει την ακεραιότητα των αρχείων των συναλλαγών των χρηστών. Για το λόγο αυτό θα πρέπει να αναπτύξετε ένα μηχανισμό διασφάλισης των αρχείων από μη-εξουσιοδοτημένη τροποποίηση. Ο μηχανισμός αυτός ακολουθεί την παρακάτω διαδικασία:

Κατά το κλείσιμο της εφαρμογής θα πρέπει να υπολογίζονται οι συνόψεις όλων των κρυπτογραφημένων αρχείων χρησιμοποιώντας μονόδρομη συνάρτηση κατακερματισμού. Αποτέλεσμα αυτής της διαδικασίας είναι τα ζεύγη <filename, digest>. Στη συνέχεια, το σύνολο των <filename, digest> θα υπογράφονται ψηφιακά από την εφαρμογή. Τέλος, η ψηφιακή υπογραφή θα αποθηκεύεται σε κατάλληλο αρχείο.

Η αντίστροφη διαδικασία της επιβεβαίωσης θα πρέπει να εκτελείται από την εφαρμογή μετά τη διαδικασία της αυθεντικοποίησης του χρήστη. Ο χρήστης θα πρέπει να ενημερώνεται με σχετικό μήνυμα εάν έχει γίνει κάποια μη-εξουσιοδοτημένη τροποποίηση των αρχείων του.

Τροποποιείστε εσκεμμένα κάποιο αρχείο και επιβεβαιώστε ότι ο μηχανισμός ακεραιότητας που υλοποιήσατε λειτουργεί σωστά.

Ερωτήσεις

Απαντήστε σύντομα στις παρακάτω ερωτήσεις:

- Ποιος ο λόγος της χρήσης του salt για την παραγωγή της σύνοψης ενός συνθηματικού;
- Ποιες είναι κατά την γνώμη σας οι αδυναμίες του συστήματος; Περιγράψτε σύντομα τι ευπάθειες μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Προτείνετε μηχανισμούς που κατά τη γνώμη σας μπορούν να βελτιώσουν την ασφάλεια που παρέχει η εφαρμογή.

Για την υλοποίηση της εφαρμογής θα πρέπει να γίνει αποκλειστική χρήση του API της Java. Βασικές κλάσεις που θα χρησιμοποιηθούν είναι οι: **KeyGenerator**, **Cipher** και **MessageDigest**. Για την συμμετρική κρυπτογράφηση θα πρέπει να χρησιμοποιήσετε τον αλγόριθμο **AES-256**. Για την ασύμμετρη κρυπτογράφηση τον **RSA-2048** ενώ για την συνάρτηση κατακερματισμού (σύνοψη) θα πρέπει να χρησιμοποιηθεί ο αλγόριθμος **SHA-256**.

Παραδοτέα

- Πηγαίος κώδικας εφαρμογών **με τον απαραίτητο σχολιασμό.**
- Ενδεικτικές **οθόνες εκτέλεσης** (screenshots) που να φαίνεται η λειτουργικότητα της εφαρμογής σας.
- Αρχείο με δημόσιο κλειδί.
- **Το σύνολο των φακέλων** και των αρχείων που θα δημιουργήσετε. (Αρχεία που περιέχουν τα κλειδιά, directories, αρχεία χρηστών, κτλ.)
- **Αναφορά** με επεξήγηση των κλάσεων και μεθόδων Java που χρησιμοποιήσατε για την υλοποίηση της εφαρμογής. Στην αναφορά θα πρέπει να περιγράψετε το τρόπο που δουλέψατε, να τεκμηριώστε αδυναμίες, περιττά βήματα ή βελτιώσεις που προτείνετε στην εφαρμογή.

Ο πηγαίος κώδικας θα αξιολογηθεί ως προς το αν υλοποιεί τα βασικά ζητούμενα της εκφώνησης, εκτελείται χωρίς να προκύπτουν σφάλματα λογισμικού (bugs), ακολουθεί «καλές αρχές» προγραμματισμού (π.χ. σχολιασμό, στοίχιση, εύγλωττη ονοματοδοσία μεταβλητών, επαναχρησιμοποίηση κώδικα, κλπ).

Αναφορές

- Java API: http://docs.oracle.com/javase/8/docs/api/
- https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#

Οδηγίες Παράδοσης

Για την 3η εργασία θα πρέπει να παραδοθεί ένα συμπιεσμένο αρχείο που θα περιέχει ένα pdf αρχείο με όλα τα ζητούμενα της εργασίας (π.χ οθόνες εκτέλεσης, απαντήσεις στα ερωτήματα κλπ.) Δεν θα πρέπει στο zip να περιλαμβάνονται και άλλα πρόσθετα αρχεία (π.χ. jpg από οθόνες κλπ).

Το όνομα του αρχείου θα πρέπει να είναι της μορφής AM1_Lab03.zip (π.χ. icsd13001_Lab03.zip – αριθμός μητρώου του αρχηγού της ομάδας) και να μην περιέχει όλα τα μέλη της ομάδας.

Θα διορθωθούν μόνο οι ασκήσεις που πληρούν την παραπάνω περιγραφή.