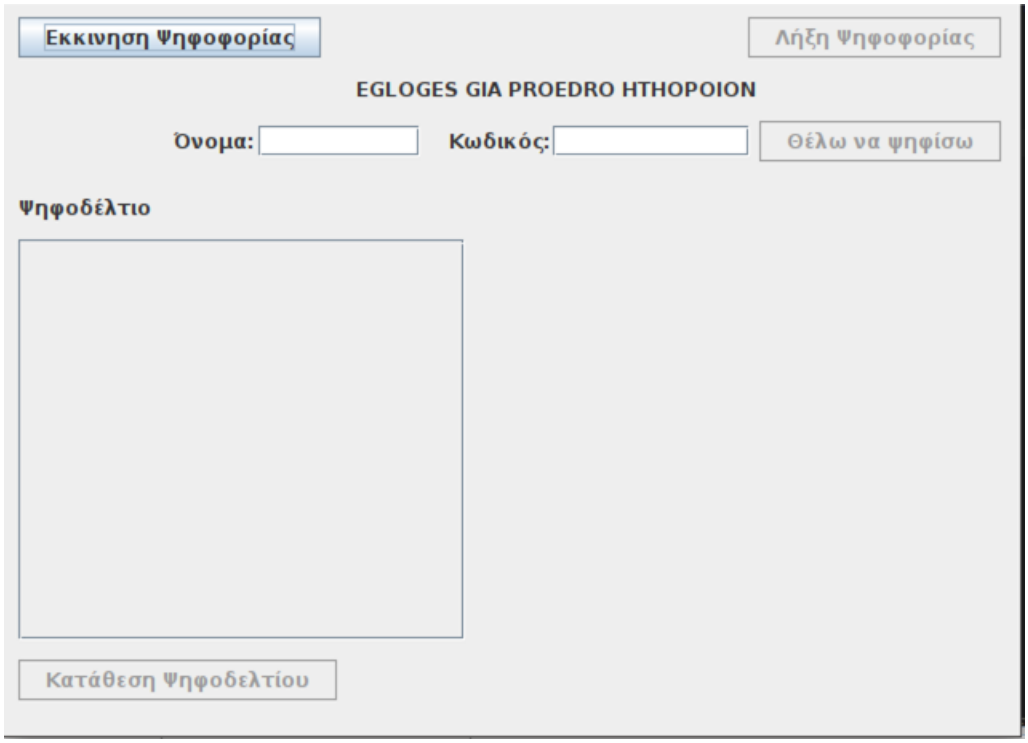
Ονοματεπώνυμο: Τριανταφύλλου Χρήστος
Αρ. Μητρώου: 3212017194

ΕΦΑΡΜΟΓΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

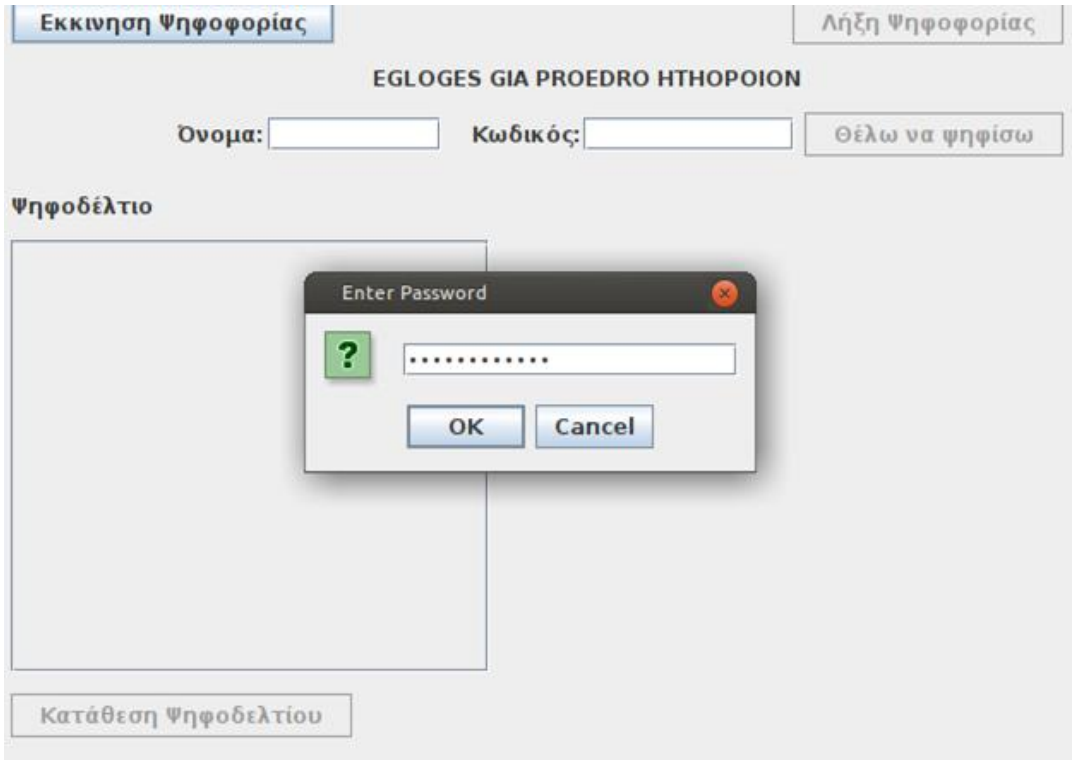
Η εφαρμογή κατά την εκκίνηση της δημιουργεί παράγει ένα ζεύγος κλειδιών RSA τα οποία αποθηκεύει σε αρχεία. Κάθε εκτέλεση της εφαρμογής σηματοδοτεί την έναρξη διαδικασιών για μία νέα ψηφοφορία οπότε χάνονται στοιχεία από τυχόν προηγούμενη. Εάν επιθυμούμε να κρατήσουμε τα στοιχεία κάποιας ψηφοφορίας πρέπει να αντιγράψουμε το φάκελο election σε άλλη τοποθεσία.
Η εκτέλεση της εφαρμογής προϋποθέτει την ύπαρξη του φάκελου election στη διαδρομή εκτέλεσης της εφαρμογής ο οποίος περιέχει αρχικά 2 άρχεία. Το αρχείο voters και το αρχείο ballot.
Το αρχείο voters περιλαμβάνει τα στοιχεία των ψηφοφόρων δηλαδή όνομα και email. Τα στοιχεία είναι χωρισμένα με “;” και κάθε γραμμή του αρχείου περιέχει τα στοιχεία ενός ψηφοφόρου.
Το αρχείο ballot περιέχει τα στοιχεία του ψηφοδελτίου. Η πρώτη γραμμή περιέχει την ονομασία της εκλογικής αναμέτρησης, η τελευταία το μέγιστο πλήθος σταυρών και όλες οι ενδιάμεσες γραμμές τα στοιχεία των υποψηφίων με 1 υποψήφιο ανά γραμμή.

Με την έναρξη της εφαρμογής δημιουργούνται και αποθυκεύονται τα αρχεία passwords, key.private, key.public, hashfile και key.AES.
Το αρχείο *passwords* περιέχει τα ονόματα χρήστη και τους κωδικούς των ψηφοφόρων καθώς και του μέλους της εφορευτικής επιτροπής σε απλό κείμενο. Στην πράξη αυτό το αρχείο δεν θα έπρεπε να υπάρχει, αποτελεί όμως το τρόπο να μάθουμε τους κωδικούς πρόσβασης για να χρησιμοποιήσουμε δοκιμαστικά την εφαρμογή.
Τα αρχεία *key.private* και *key.public* περιέχουν το ιδιωτικό και το δημόσιο κλειδί RSA-2048 που δημιουργεί η εφαρμογής.
Το *hashfile* έχει αποθυκευμένα τα στοιχεία των ψηφοφόρων και το κρυπτογραφημένο κωδικό τους.
Τέλος το αρχείο *key.AES* περιέχει το συμμετρικό κλειδί
Όλα τα αρχεία αποθηκεύονται στο φάκελο election.
Με τη λήξη της ψηφοφορίας δημιουργείται το αρχεία results.txt το οποίο περιέχει τα αποτελέσματα της ψηφοφορίας

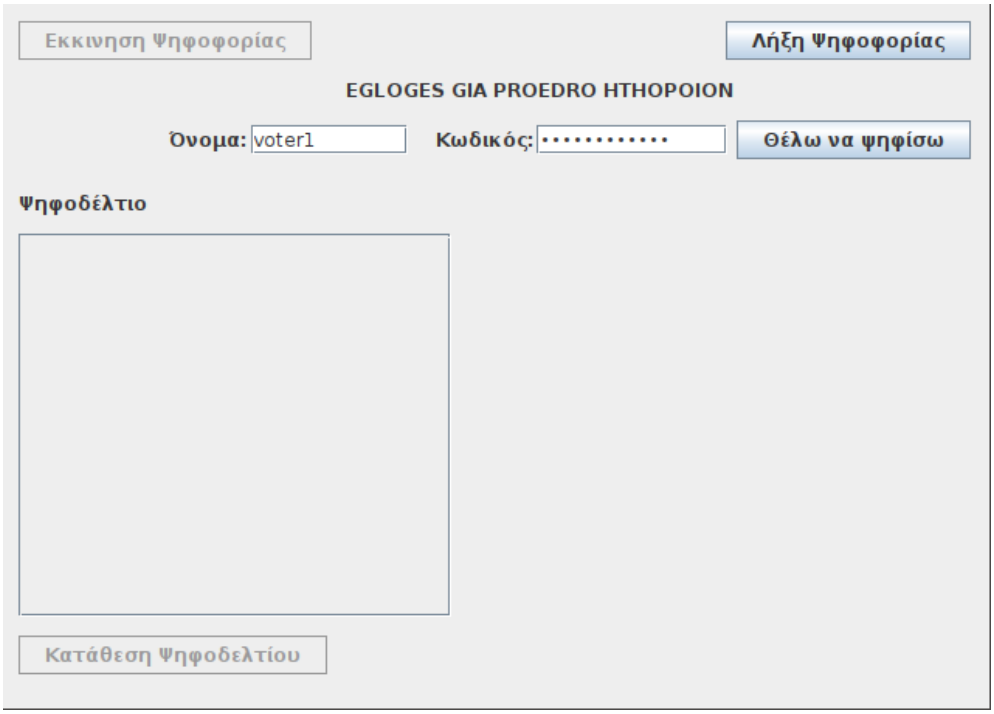
Οθόνες εκτέλεσης της εφαρμογής



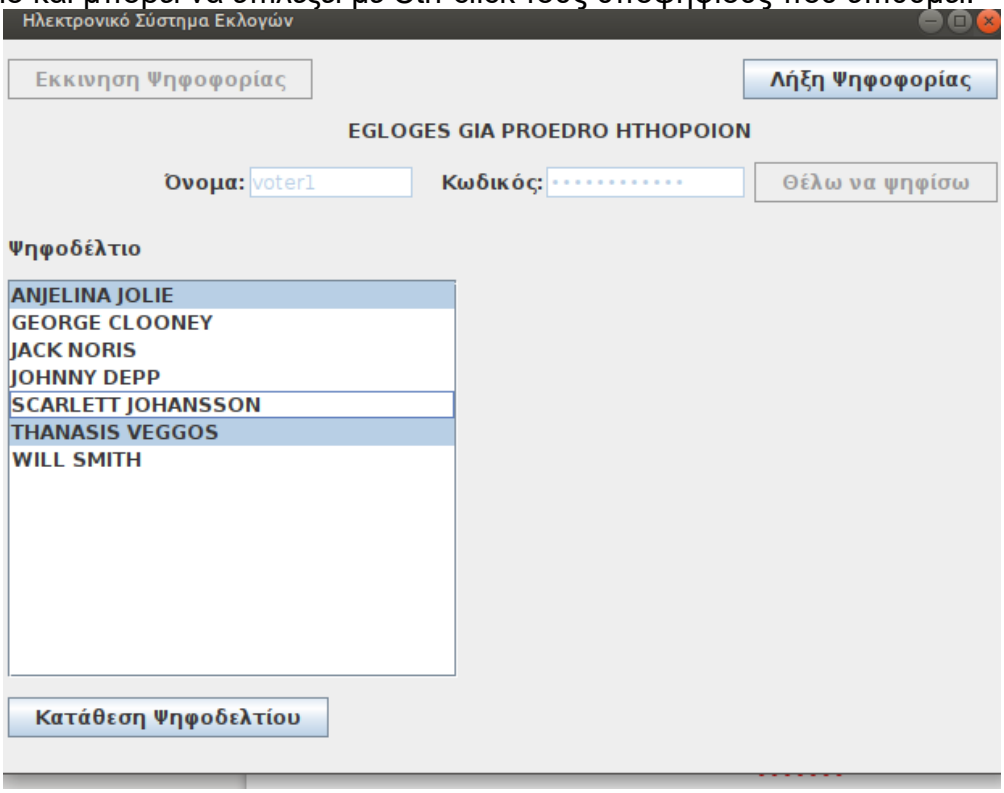
Η αρχική οθόνη έχει ενεργοποιημένο μόνο το πλήκτρο για εκκίνηση της ψηφοφορίας όταν το πατήσουμε μας ζητάει τον κωδικού του μέλους εφορευτικής τον οποίο μπορούμε να βρούμε στο αρχείο passwords που μόλις δημιουργήθηκε.



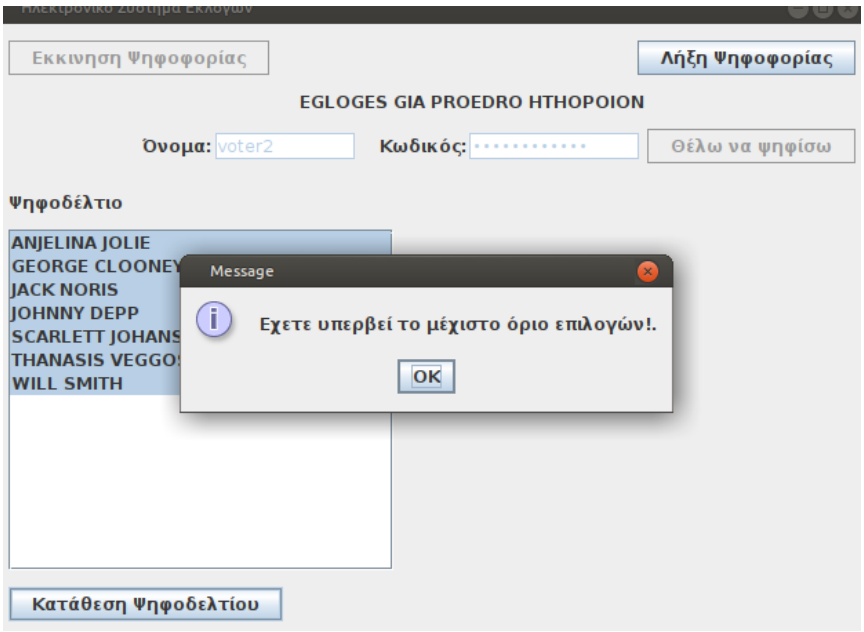
Δίνοντας τον κωδικό και πατώντας OK ξεκινάειη εκλογική διαδικασία.
Κατα την εκλογική διαδικασία οι ψηφοφόροι μπορούν να δώσουν τα στοιχεία τους στα πεδία Όνομα και Κωδικός και στη συνέχεια να πατήσουν το πλήκτρο “Θέλω να ψηφίσω” για να συμμετέχουν στην εκλογική διαδικασία.



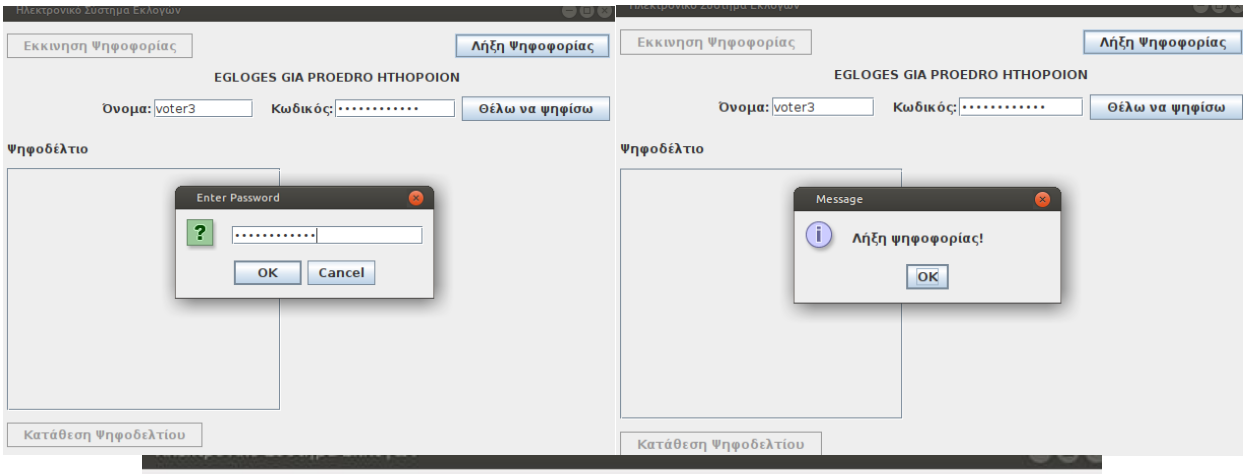
Όπως φαίνεται έχουν ενεργοποιηθεί τα πλήκτρα “Λήξη Ψηφοφορίας” και “Θέλω να ψηφίσω”. Ο Ψηφοφόρος δίνοντας τα στοιχεία και πατώντας το Θέλω να ψηφίσω βλέπει το ψηφοδέλτιο και μπορεί να επιλέξει με Ctrl-click τους υποψηφίους που επιθυμεί.

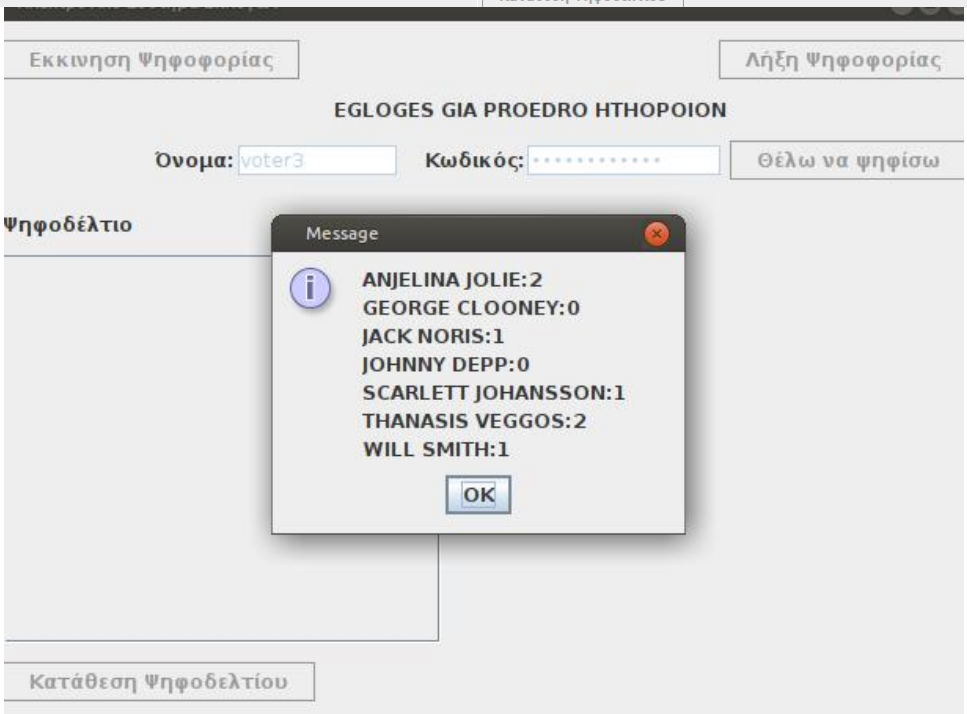


Μετά την επιλογή των υποψηφίων και πατώντας το πλήκτρο “Κατάθεση ψηφοδελτίου” γίνεται έλεγχος για το πλήθος των σταυρών και ο ψηφοφόρος ενημερώνεται για την επιτυχή ή όχι υποβολή του ψηφοδελτίου.



Εάν το μέλος της εφορευτικής επιτροπή επιλέξει τη λήξη ψηφοφορίας η εφαρμογή ζητάει ξανά τον κωδικό του και εάν είναι σωστός ολοκληρώνεται η εκλογική διαδικασία και γίνεται η καταμέτρηση των ψήφων.





Τα αποτελέσματα των εκλογών αποθηκεύονται και στο αρχείο results.txt ώστε να μπορεί κάποιος να τα δεί και μετά τον τερματισμό της εφαρμογής.

Ερωτήματα

1. Η χρήση του salt δημιουργεί διαφορετικά hash για τον ίδιο κωδικό πρόσβασης. Έτσι εαν 2 ψηφοφόροι έχουν ίδιο κωδικό δεν θα μπορεί κάποιος που γνωρίζει τον κωδικό του ενός και έχει πρόσβαση στο αρχείο με τα hash να γνωρίζει ότι οι 2 κωδικοί είναι ίδιοι μεταξύ τους.

2. Σύμφωνα με την περιγραφή οι κωδικοί αποστέλλονται στους χρήστες με απλό e-mail. Η επικοινωνία με e-mail ενέχει γενικά τον κίνδυνο κάποιος 3ος να υποκλέψει το μήνυμα και συνεπώς τους κωδικούς του ψηφοφόρου. Για να μην είναι εφικτό κάτι τέτοιο θα έπρεπε και η αποστολή των e-mail να γίνεται κρυπτογραφημένα.

Η εφαρμογή των εκλογών όταν ξεκινάει αρχίζει την εκλογική διαδικασία από την αρχή. Κάποιος κακόβουλος θα μπορούσε να διακόψει την διαδικασία διακόπτοντας π.χ. το ρεύμα στον υπολογιστή που εκτελείτε η εφαρμογή. Καλό θα ήταν η εφαρμογή να κρατάει ιστορικό της διαδικασίας ώστε να γνωρίζει εάν η διαδικασία διακόπηκε βίαια και σε επανεκκίνηση της εφαρμογής να μπορεί το μέλος της εφορευτικής να επιλέξει συνέχιση της εκλογικής διαδικασίας.

Τεκμηρίωση Κλάσεων - Μεθόδων

Τεκμηρίωση Κλάσης securevote.KeyHandler

Συναρτήσεις Πακέτου

KeyHandler () throws NoSuchAlgorithmException
void **savePublicKey** (String publickey)
void **savePrivateKey** (String privatekey)
String **readPublicKey** ()
String **readPrivateKey** ()
void **generateAndStoreAESKey** ()
SecretKey **readAESKey** ()
String **encode** (String text)
String **decode** (String text)
String **AESencode** (String text)
String **AESdecode** (String text)

Λεπτομερής Περιγραφή

Δημιουργεί το δημόσιο, ιδιοτικό RSA και το συμμετρικό AES κλειδια και και τα αποθυκεύει σε αρχεία. Υλοποιεί συναρτήσεις για κωδικοποίηση ή αποκωδικοποίηση με τη χρήση των κλειδιών.

Τεκμηρίωση Constructor & Destructor

securevote.KeyHandler.KeyHandler () throws NoSuchAlgorithmException `[package]`

Κατασκευαστής της κλάσης Η κλάση δεν διατηρεί στη μνήμη τα κλειδιά που δημιουργεί οπότε δεν έχει αντίστοιχα ιδιωτικά στοιχεία. Η δημιουργία του ζεύγους κλειδιών RSA και

αποθήκευση τους σε αρχείο γίνεται με την δημιουργία ενός τέτοιου αντικειμένου Όχι όμως και η δημιουργία και αποθήκευση του συμμετρικού κλειδιού

Τεκμηρίωση Συναρτήσεων Μελών

String securevote.KeyHandler.AESdecode (String *text*) [package]

Αποκρυπτογραφεί ένα αλφαριθμητικό χρησιμοποιώντας συμμετρικό κλειδί AES

Παράμετροι

text	Κρυπτογραφημένο κείμενο

Επιστρέφει

το αποκρυπτογραφημένο κείμενο

String securevote.KeyHandler.AESencode (String *text*) [package]

Κρυπτογραφεί ένα αλφαριθμητικό χρησιμοποιόντας το συμμετρικό κλειδί AES

Παράμετροι

text	Το αλφαριθμητικό που θέλουμε να κρυπτογρφίσουμε

Επιστρέφει

Το κρυπτογραφημένο αλφαριθμηυικό

String securevote.KeyHandler.decode (String *text*) [package]

Αποκρυπτογραφεί ένα αλφαριθμητικό χρησιμοποιώντας το ιδιοτικό κλειδί RSA

Παράμετροι

text	Κρυπτογραφημένο κείμενο

Επιστρέφει

το αποκρυπτογραφημένο κείμενο

String securevote.KeyHandler.encode (String *text*) [package]

Κρυπτογραφεί ένα αλφαριθμητικό χρησιμοποιόντας το δημόσιο κλειδί RSA

Παράμετροι

text	Το αλφαριθμητικό που θέλουμε να κρυπτογρφίσουμε

Επιστρέφει

Το κρυπτογραφημένο αλφαριθμηυικό

void securevote.KeyHandler.generateAndStoreAESKey () [package]

Δημιουργεί και αποθυκεύει συμμετρικό κλειδί για το μέλος της εφορευτικής

SecretKey securevote.KeyHandler.readAESKey () [package]

Διαβάζει και ξαναδημιουργεί το συμμετρικό κλειδί του μέλους από το αρχείο

Επιστρέφει

το συμμετρικό κλειδί

String securevote.KeyHandler.readPrivateKey () [package]

Διαβάζει και επιστρέφει συμβολοσειρά του ιδιωτικού κλειδιού από αρχείο

Επιστρέφει

τη συμβολοσειρά ιδιωτικού κλειδιού που αποθηκεύτηκε

String securevote.KeyHandler.readPublicKey () [package]

Διαβάζει και επιστρέφει συμβολοσειρά του δημόσιου κλειδιού από αρχείο

Επιστρέφει

τη συμβολοσειρά δημόσιου κλειδιού που αποθηκεύτηκε

void securevote.KeyHandler.savePrivateKey (String *privatekey*) [package]

Αποθηκεύει το αλφαριθμητικό που θα λάβει στο αρχείου του ιδιωτικου κλειδιού Το αλφαριθμητικό πρέπει να έχει λάβει μορφή ώστε να μην περιέχει χαρακτήρες οι οποίοι δεν μπορούν να αποθηκευτούν.

Παράμετροι

publickey	Συμβολοσειρά που δημιουργείται από το ιδιωτικό κλειδί. Πρέπει να είναι κωδικοποιημένη χρησιμοποιόντας το Base64.

void securevote.KeyHandler.savePublicKey (String *publickey*) [package]

Αποθηκεύει το αλφαριθμητικό που θα λάβει στο αρχείου του σημόσιου κλειδιου Το αλφαριθμητικό πρέπει να έχει λάβει μορφή ώστε να μην περιέχει χαρακτήρες οι οποίοι δεν μπορούν να αποθηκευτούν.

Παράμετροι

publickey	Συμβολοσειρά που δημιουργείται από το δημόσιο κλειδί. Πρέπει να είναι κωδικοποιημένη χρησιμοποιόντας το Base64.

Τεκμηρίωση Κλάσης securevote.PasswordHandler

Συναρτήσεις Πακέτου

PasswordHandler ()
String **generatePassword** ()
String **generateSalt** ()

Μεταβλητές Πακέτου

ArrayList< String > **pwds** = new ArrayList()

Λεπτομερής Περιγραφή

Βοηθητική κλάση για τη δημιουργία των κωδικών πρόσβασης

Τεκμηρίωση Constructor & Destructor

securevote.PasswordHandler.PasswordHandler () [package]

Τεκμηρίωση Συναρτήσεων Μελών

String securevote.PasswordHandler.generatePassword () [package]

Δημιουργεί password με 12 στοιχεία. Τα στοιχεία μπορεί να είναι κεφαλαία λατινικά γράμματα και αριθμοί

Επιστρέφει

τον κωδικό πρόσβασης

String securevote.PasswordHandler.generateSalt () [package]

Δημιουργεί τυχαίο salt.

Επιστρέφει

τον salt που δημιούργησε

Τεκμηρίωση Κλάσης securevote.SecureVote

Στατικές Δημόσιες Μέθοδοι

static void **main** (String[] args) throws NoSuchAlgorithmException

Συναρτήσεις Πακέτου

String **getElectionTitle** ()

Στατικές Συναρτήσεις Πακέτου

static void **readVoterFile** ()
static void **readBallotFile** ()
static void **savePasses** ()
static void **saveHashes** ()
static boolean **authenticate** (String username, String password)
static boolean **canVote** (String **voter**)
static void **recieveVote** (String votername, int[]**votes**)
static void **endElections** ()
static void **results** ()
static void **addAVoteTo** (String name)

Στατικές Μεταβλητές Πακέτου

static ArrayList< String > **voter** = new ArrayList()
static ArrayList< String > **email** = new ArrayList()
static ArrayList< String > **pass** = new ArrayList()
static ArrayList< String > **salt** = new ArrayList()
static String **adminPass**
static String **adminSalt**
static ArrayList< String > **candidate** = new ArrayList()
static ArrayList< Integer > **votes** = new ArrayList()
static ArrayList< String > **hasVoted** = new ArrayList()
static ArrayList< String > **ballotbox** = new ArrayList()
static String **electionTitle**
static int **maxVotes** = 0
static **PasswordHandler p** = new **PasswordHandler**()
static **KeyHandler k**
static JFrame **frame** = new JFrame("Ηλεκτρονικό Σύστημα Εκλογών")
static JPanel **activePanel** = new **Vote**()

Λεπτομερής Περιγραφή

Κύριο κομμάτι της εφαρμογής προσομοίωσης ασφαλούς ηλεκτρονικής ψηφορφορίας.

Τεκμηρίωση Συναρτήσεων Μελών

static void securevote.SecureVote.addAVoteTo (String *name*) `[static], [package]`

προθέτει ψήφο σε κάποιο υποψήφιο

Παράμετροι

name	

static boolean securevote.SecureVote.authenticate (String *username*, String *password*) `[static], [package]`

Ελέγχει αν είναι σωστός συνδυασμός χρήστη και κωδικού

Παράμετροι

username	όνομα χρήστη
password	κωδικός

Επιστρέφει

True εάν είνα σωστό, False διαφορετικά.

static boolean securevote.SecureVote.canVote (String *voter*) `[static], [package]`

Επιτρέφει εάν κάποιος ψηφοφόρος έχει δικαίωμα να ψηφίσει.

Παράμετροι

voter	όνομα ψηφοφόρου

Επιστρέφει

True έχει δικαίωμα, False έχει ήδη ψηφήσει

static void securevote.SecureVote.endElections () `[static], [package]`

Τερματίζει την εκλογική διαδικασία και ξεκινάει την καταμέτρηση

static void securevote.SecureVote.main (String[] *args*) throws NoSuchAlgorithmException `[static]`

Παράμετροι

args	the command line arguments

static void securevote.SecureVote.readBallotFile () `[static], [package]`

Διαβάζει τα στοιχεία από το αρχείο ψηφοδελτίου. Το αρχείο έχει στην 1η γραμμή τον τίτλο των εκλογώ Στην τελευταία γραμμή το μέγιστο πλήθος σταυρών και στις ενδιάμεσες τα ονόματα των υποψηφίων ένα ανά γραμμή

static void securevote.SecureVote.readVoterFile () `[static], [package]`

Διαβάζει τα στοιχεία από το αρχείο ψηφοφόρων. Το αρχείο έχει γραμμές της μορφής "ονομαψηφοφόρου;e-mail"

static void securevote.SecureVote.recieveVote (String *votername*, int[] *votes*) `[static], [package]`

Παραλαμβάνει μία νέα ψήφο την καταχωρεί και ανακατεύει τα ψηφοδέλτια.

Παράμετροι

votername	όνομα ψηφοφόρου
votes	λίστα ακεαίων με τις θέσεις των σταυρών στο ψηφοδέλτιο

static void securevote.SecureVote.results () `[static], [package]`

Κάνει την καταμέτρηση των ψήφων και ελέγχει ότι τα ψηφοδέλτια είναι ίδια σε πλήθος με τους ψηφίσαντες. Δείχνει τα αποτελέσματα και τα αποθηκεύει σε αρχείο

static void securevote.SecureVote.saveHashes () `[static], [package]`

Αποθηκεύει τα στοιχεία των ψηφοφόρων καθώς και το κρυπτογραφημένο κωδικό

static void securevote.SecureVote.savePasses () `[static], [package]`

Αποθηκεύει ονοματα και κωδικούς στο αρχείο passwords ώστε να μπορούμε να διαβάσουμε και να χρησιμοποιήσουμε τους κωδικούς για δοκιμή της εφαρμογής

Τεκμηρίωση Κλάσης securevote.Vote

Κληρονομεί την JPanel.

Δημόσιες Μέθοδοι

Vote ()
void **endElections** ()

Ιδιωτικές Μέθοδοι

void **initComponents** ()
void **formAncestorAdded** (javax.swing.event.AncestorEvent evt)
void **StartVotingActionPerformed** (java.awt.event.ActionEvent evt)
void **EndVotingActionPerformed** (java.awt.event.ActionEvent evt)
void **VoteNowActionPerformed** (java.awt.event.ActionEvent evt)
void **PostVoteActionPerformed** (java.awt.event.ActionEvent evt)

Ιδιωτικα Χαρακτηριστικά

javax.swing.JList< String > **CanditateList**
javax.swing.JButton **EndVoting**
javax.swing.JPasswordField **Password**
javax.swing.JButton **PostVote**
javax.swing.JButton **StartVoting**
javax.swing.JLabel **Title**
javax.swing.JButton **VoteNow**
javax.swing.JLabel **jLabel1**
javax.swing.JLabel **jLabel3**
javax.swing.JLabel **jLabel4**
javax.swing.JScrollPane **jScrollPane1**
javax.swing.JTextField **username**

Λεπτομερής Περιγραφή

Γραφικό περιβάλλον της εφαρμογής. Δημιουργήθηκε με τη βοήθεια του netbeans

Πηγές

https://www.devglan.com/java8/rsa-encryption-decryption-java

https://stackoverflow.com/questions/18228579/how-to-create-a-secure-random-aes-key-in-java

https://stackoverflow.com/questions/18142745/how-do-i-generate-a-salt-in-java-for-salted-hash

https://www.baeldung.com/java-shuffle-collection

https://stackoverflow.com/questions/1925104/easy-way-to-store-restore-encryption-key-for-decrypting-string-in-java

Η τεκμηρίωση των κλάσεων και των μεθόδων έγινε από τα σχόλια της εφαρμογής με τη βοήθεια του εργαλείου doxygen.