AES 256 MOBILE APPLICATION

Κωστούδας Σάββας

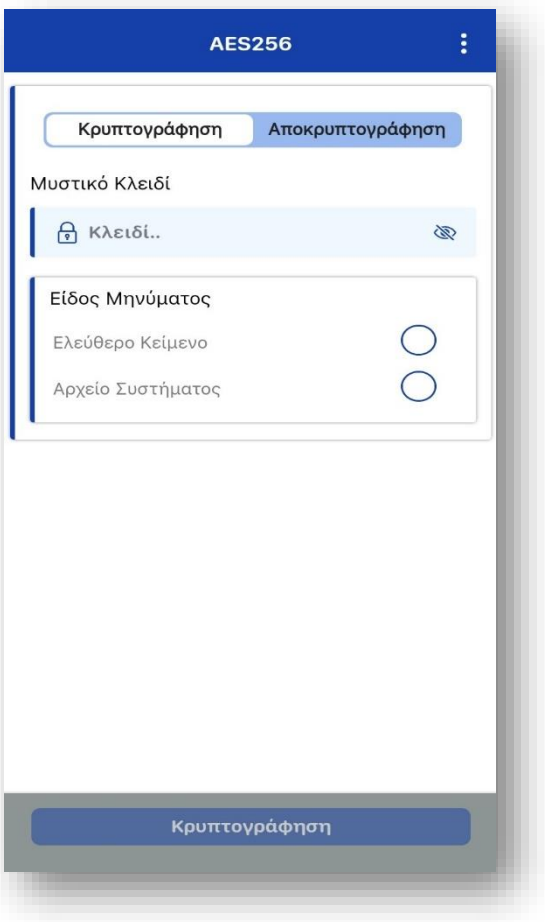
7 ΜΑΡΤΙΟΥ 2022

ΚΩΣΤΟΥΔΑΣ ΣΑΒΒΑΣ

Εισαγωγή

Το έγγραφο αυτό αποτελεί έναν σύντομο οδηγό χρήσης της εφαρμογής AES – 256. Καταρχήν, στο ακόλουθο σχήμα 1. επισυνάπτεται η βασική απεικόνιση της εφαρμογής.

Σχήμα 1. Απεικόνιση εφαρμογής



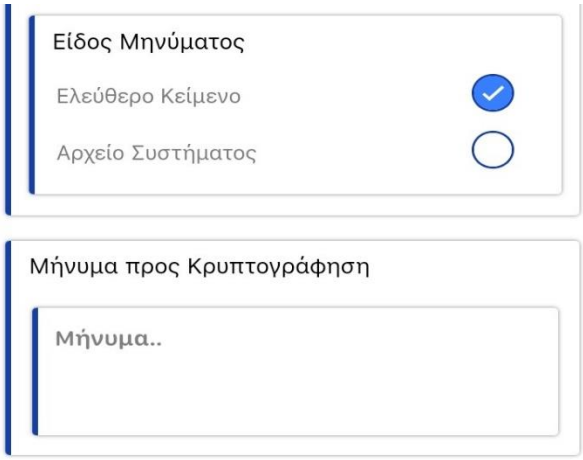
Η εφαρμογή φυσικά προσφέρει δύο βασικά modes, την Κρυπτογράφηση και την Αποκρυπτογράφηση. Για να επιλέξουμε το mode απλά κάνουμε κλικ στην κορυφή στον selector είτε το κουμπί **Κρυπτογράφηση** είτε το κουμπί **Αποκρυπτογράφηση**.

Έπειτα, το βασικό στοιχείο της εφαρμογής είναι να τεθεί το μυστικό συμμετρικό κλειδί που επιθυμεί ο χρήστης για την κρυπτογράφηση/αποκρυπτογράφηση. Το μυστικό συμμετρικό κλειδί μπορεί να είναι στα λατινικά ότι επιθυμεί ο χρήστης είτε και με αριθμούς είτε και όχι. Επομένως για να εκκινήσει την διαδικασία είναι αναγκαίο να θέσει μυστικό συμμετρικό κλειδί. Με το κλικ στο εικονίδιο ματάκι, το input αλλάζει (mode) και φανερώνει τους χαρακτήρες του μυστικού κλειδιού που έχει γράψει ο χρήστης. Για ασφάλεια εξαρχής είναι σε mode password.

Επιλογή αρχείου ή γράψιμο μηνύματος

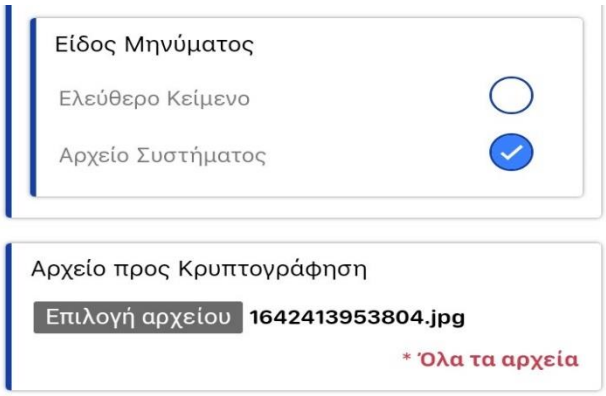
Επόμενο βήμα για την κρυπτογράφηση/αποκρυπτογράφηση είναι είτε η επιλογή αρχείου είτε να γράψει ο χρήστης ένα text μήνυμα στην αντίστοιχη περιοχή. Συγκεκριμένα:

1. **Γράψιμο text μηνύματος**: για να είναι σε θέση να γράψει το μήνυμα που επιθυμεί ο χρήστης αρκεί να κάνει κλικ στο checkbox που λαμβάνει χώρα μέσα στο **box Είδος Μηνύματος,** όπως φαίνεται και στο παρακάτω σχήμα 2:
   Σχήμα 2. Επιλογή Είδος Μηνύματος ως **Ελεύθερο Κείμενο**



   Όταν επιλέξει **Ελεύθερο Κείμενο**, τότε εμφανίζεται και η παραπάνω text area ώστε να γράψει ο χρήστης το μήνυμα που επιθυμεί να κρυπτογραφηθεί/αποκρυπτογραφηθεί.

2. **Επιλογή αρχείου προς κρυπτογράφηση**: για να είναι σε θέσει να επιλέξει αρχείο προς κρυπτογράφηση/αποκρυπτογράφηση πρέπει να κάνει κλικ στην επιλογή **Αρχείο Συστήματος**, όπως φαίνεται στο σχήμα 3:
   Σχήμα 3. Επιλογή Είδος Μηνύματος ως Αρχείο Συστήματος



   Όταν επιλέξει **Αρχείο Συστήματος**, τότε εμφανίζεται και η παραπάνω περιοχή Αρχείο προς Κρυπτογράφηση καθώς και το κουμπί **Επιλογή αρχείου** όπου όταν πατηθεί, ανοίγει την αναζήτηση αρχείων στο κινητό του χρήστη ώστε να διαλέξει ένα αρχείο προς

κρυπτογράφηση/αποκρυπτογράφηση. Όταν επιλέξει αρχείο ο χρήστης, τότε η συσκευή εμφανίζει το όνομα του επιλεγμένου αρχείου όπως φαίνεται και στο σχήμα 3.

Όπως φαίνεται και στο σχήμα 3. , η εφαρμογή υποστηρίζει όλους τους τύπους αρχείων. Αυτό σημαίνει ότι για οποιοδήποτε επιλεχθέν αρχείο θα λειτουργήσει σωστά η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης. Ωστόσο για μεγάλα αρχεία, ο συνολικός χρόνος κρυπτογράφησης αυξάνεται.

Κρυπτογράφηση και Αποκρυπτογράφηση

Για να κρυπτογραφήσουμε ή να αποκρυπτογραφήσουμε αυτά που επιθυμούμε, απαιτούνται δύο κινήσεις:

1. Γράψιμο του μυστικού συμμετρικού κλειδιού που επιθυμεί ο χρήστης.
2. Επιλογή **Ελεύθερο Κείμενο** και **γράψιμο του μηνύματος στην text area** ή επιλογή **Αρχείο Συστήματος και επιλογή του αρχείου από το σύστημα του χρήστη.**

Αν λάβουν χώρα και τα δύο παραπάνω τότε ενεργοποιείται το Κουμπί **Κρυπτογράφηση/Αποκρυπτογράφηση** και πλέον μπορούμε να εκτελέσουμε την αντίστοιχη ενέργεια. Αν δεν λάβουν χώρα και τα δύο παραπάνω τότε δεν είναι επιτρεπτή η **Κρυπτογράφηση/Αποκρυπτογράφηση καθώς ο αλγόριθμος δεν διαθέτει τις απαραίτητες πληροφορίες.**

Αποθήκευση Αρχείων Αποτελέσματος

Όταν ο αλγόριθμος τελειώσει την διαδικασία Κρυπτογράφησης/Αποκρυπτογράφησης, αποθηκεύει το αρχείο αποτελέσματος στον φάκελο **Λήψεις (Download)** του χρήστη. Η διαδικασία και η ονοματολογία των αρχείων είναι η εξής:

1. Αν ο χρήστης επέλεξε να γράψει **Ελεύθερο Κείμενο** τότε η εφαρμογή δημιουργεί το αρχείο αποτελέσματος το οποίο είναι μορφής **.txt** και το αποθηκεύει στον **φάκελο Λήψεις (Download)** με το όνομα **Aes256_Message_** + (dateNow get milliseconds) + _Encrypted.txt . Δηλαδή ένα παράδειγμα είναι το εξής: Aes256_Message_38_Encrypted.txt.

2. Αν ο χρήστης επέλεξε αρχείο για κρυπτογράφηση τότε η εφαρμογή δημιουργεί το αρχείο αποτελέσματος το οποίο είναι ότι μορφής διάλεξε εξαρχής, δηλαδή αν διάλεξε αρχείο PDF, τότε και το αποτέλεσμα θα είναι τύπου PDF, και το αποθηκεύει και αυτό στο φάκελο Λήψεις (Download) με το εξής όνομα: Όνομα Αρχείου + _Encrypted + file extension. Δηλαδή ένα

παράδειγμα είναι το εξής: 164213953804_Encrypted.jpg. Στην περίπτωση τώρα της αποκρυπτογράφησης η εφαρμογή πάλι αποθηκεύει το αποτέλεσμα στον φάκελο Λήψεις (Download) του χρήστη με το εξής όνομα όμως: Όνομα Αρχείου + _Decrypted + file extension. Δηλαδή για το παραπάνω παράδειγμα φωτογραφίας, το αποτέλεσμα αποκρυπτογράφησης είναι το εξής αρχείο με όνομα: 164213953804_Encrypted_Decrypted.jpg

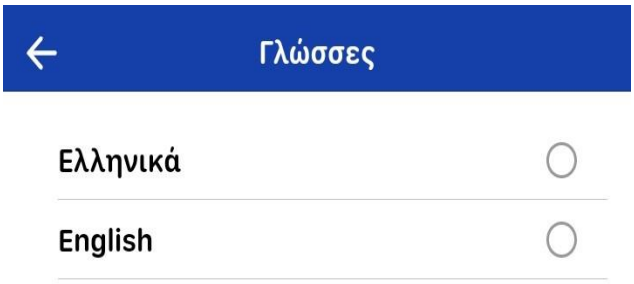
Πληροφορίες εφαρμογής, Αλλαγή Γλώσσας

Πάνω στην δεξιά γωνία της εφαρμογής εντοπίζεται το εικονίδιο τρεις τελείες. Πατώντας το εικονίδιο αυτό η εφαρμογή εμφανίζει τις επιλογές του σχήματος 4:

Σχήμα 4. Επιλογές (Η εφαρμογή), (Οδηγός Χρήσης), (Επιλογή Γλώσσας)

Η πρώτη επιλογή **Η εφαρμογή** θα περιέχει αργότερα πληροφορίες για την εφαρμογή καθώς και τον δημιουργό της αλλά και τον καθηγητή που παρείχε όλη την απαραίτητη βοήθεια. Η δεύτερη επιλογή θα αφορά έναν σύντομο οδηγό χρήσης που θα επιδεικνύεται στον χρήστη. Τέλος, η **Επιλογή Γλώσσας** όπως αναφέρει και το όνομα της, επιτρέπει στον χρήστη να αλλάξει την γλώσσα της εφαρμογής από Ελληνικά σε Αγγλικά ή και το αντίστροφο. Οι διαθέσιμες επιλογές απεικονίζονται στο σχήμα 5.

Σχήμα 5. Επιλογές Γλώσσας



Αν επιλεχθεί η Αγγλική Γλώσσα τότε η γλώσσα ολόκληρης της εφαρμογής μετατρέπεται σε Αγγλικά όπως φαίνεται και στο παρακάτω σχήμα 6.

Σχήμα 6. Εφαρμογή στην Αγγλική Γλώσσα