Affiliation: Ionian University Course: Cryptography Issue #001

ΚΡΥΠΤΟΓΡΑΦΙΑ | PYTHON

ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ PYTHON

Πρακτικά Ζητήματα

Εισαγωγή: Η κρυπτογραφία είναι η τέχνη της επικοινωνίας μεταξύ δύο χρηστών μέσω κωδικοποιημένων μηνυμάτων. Η επιστήμη της κρυπτογραφίας αναδύθηκε με βασικό κίνητρο την παροχή ασφάλειας στα εμπιστευτικά μηνύματα που μεταφέρονται από το ένα μέρος στο άλλο. Η κρυπτογραφία ορίζεται ως η τέχνη και η επιστήμη της απόκρυψης του μηνύματος.

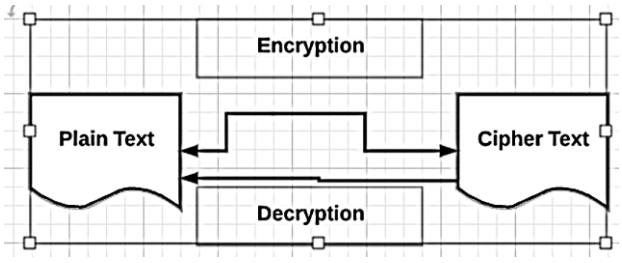
Ορολογία: Οι όροι που χρησιμοποιούνται συχνά στην κρυπτογραφία εξηγούνται στη συνέχεια.

Απλό κείμενο: Το απλό μήνυμα κειμένου είναι το κείμενο που είναι αναγνώσιμο και κατανοητό από όλους τους χρήστες. Το απλό κείμενο είναι το μήνυμα που υφίσταται κρυπτογράφηση.

Κείμενο κρυπτογράφησης: Το κρυπτογραφημένο κείμενο είναι το μήνυμα που λαμβάνεται μετά την εφαρμογή κρυπτογραφίας σε απλό κείμενο.

Κρυπτογράφηση: Η διαδικασία μετατροπής απλού κειμένου σε κρυπτογραφημένο κείμενο ονομάζεται κρυπτογράφηση. Ονομάζεται επίσης ως κωδικοποίηση.

Αποκρυπτογράφηση: Η διαδικασία μετατροπής κρυπτογραφημένου κειμένου σε απλό κείμενο ονομάζεται αποκρυπτογράφηση. Ονομάζεται επίσης ως αποκωδικοποίηση. Το διάγραμμα που δίνεται παρακάτω δείχνει μια απεικόνιση της πλήρους διαδικασίας κρυπτογραφίας:



Σχήμα 1. Η διαδικασία της κρυπτογράφησης

Χαρακτηριστικά της Σύγχρονης Κρυπτογραφίας. Τα βασικά χαρακτηριστικά της σύγχρονης κρυπτογραφίας είναι τα εξής:

- Λειτουργεί σε ακολουθίες bit.
- Χρησιμοποιεί μαθηματικούς αλγόριθμους για την ασφάλεια των πληροφοριών.
- Απαιτεί από τα μέρη που ενδιαφέρονται για ασφαλές κανάλι επικοινωνίας για να επιτύχουν το απόρρητο

Python: Η Python είναι μια ανοιχτού κώδικα γλώσσα υψηλού επιπέδου με εύκολη ερμηνεία καθώς και είναι διαδραστική και αντικειμενοστραφής. Έχει σχεδιαστεί για να είναι ευανάγνωστη. Η σύνταξη της γλώσσας Python είναι εύκολο να κατανοηθεί και χρησιμοποιεί συχνά αγγλικές λέξεις-κλειδιά.

Τα βασικά σημεία της γλώσσας προγραμματισμού Python είναι τα εξής:

- Περιλαμβάνει λειτουργικό και δομημένο προγραμματισμό και μεθόδους για αντικειμενοστραφή προγραμματισμό.
- Μπορεί να χρησιμοποιηθεί ως γλώσσα scripting ή ως ολοκληρωμένη γλώσσα προγραμματισμού.
- Περιλαμβάνει αυτόματη αποκομιδή σκουπιδιών (garbage collection).
- Περιλαμβάνει υψηλού επιπέδου δυναμικούς τύπους δεδομένων.
- Η Python περιλαμβάνει την δυνατότητα ενοποίησης με C, C++ και γλώσσες όπως η Java.

Ο σύνδεσμος λήψης για τη γλώσσα Python είναι ο ακόλουθος: https://www.python.org/downloads/.

Το link/URL περιλαμβάνει τα πακέτα για διάφορα λειτουργικά συστήματα όπως Windows, MacOS και Linux διανομές.

ΒΗΜΑ 01

Εγκαταστήστε την Python v. 3+ στον υπολογιστή σας ανάλογα με το λειτουργικό σύστημα. Ανοίξτε το IDLE ή το περιβάλλον. Εγκαταστήστε το VScode ή Notepad++ για καλύτερη επεξεργασία του κώδικα.

ΚΡΥΠΤΟΓΡΑΦΙΑ | PYTHON (2)

Python Strings: Η βασική δήλωση συμβολοσειρών φαίνεται παρακάτω.

```
str = 'Hello World!' #Αυτό είναι ένα σχόλιο. Αποθηκεύουμε στη μεταβλητή με όνομα str την τιμή Hello World. Η τιμή στην συγκεκριμένη περίπτωση είναι αλφαριθμητικό. Δώστε αντίστοιχα και τρέξτε την εντολή με δικές σας τιμές.
```

Python Lists: Οι λίστες των Python μπορούν να δηλωθούν ως σύνθετοι τύποι δεδομένων, διαχωρισμένοι με κόμματα και περικλείεται μέσα σε αγκύλες (πχ. [ ]).

```
list = [ 'abcd', 786 , 2.23, 'john', 70.2 ]
tinylist = [123, 'john']
```

Python Tuples: Μια πλειάδα είναι ένας δυναμικός τύπος δεδομένων της Python που αποτελείται από ένα σύνολο από αριθμούς και τιμές που χωρίζονται με κόμμα. Οι πλειάδες περικλείονται με παρενθέσεις.

```
tinytuple = (123, 'john')
```

Python Dictionary: Το λεξικό είναι ένα τύπος δεδομένων στην Python που λειτουργεί ως ευρετήριο. Ένα κλειδί λεξικού (key) μπορεί να είναι σχεδόν οποιοσδήποτε τύπος δεδομένων Python, και είναι συνήθως αριθμοί ή συμβολοσειρές.

```
tinydict = {'name': 'omkar','code':6734, 'dept': 'sales'}
```

Μπορούμε να φανταστούμε τη γλώσσα ως μια αριθμομηχανή όπου οι τέσσερεις βασικές πράξεις λειτουργούν με τα σύμβολα +, -, *, /. Κάθε φορά που θέλουμε να τυπώσουμε το αποτέλεσμα μιας πράξης γράφουμε την εντολή print.

```
print (5+3)
print ((7-2)*4)
```

Η γλώσσα επιτρέπει τη χρήση παρενθέσεων. Επίσης μπορούμε να τυπώνουμε πολλά αποτελέσματα με την ίδια εντολή, αρκεί να χωρίζουμε με κόμματα:

Μια μικρή προσοχή χρειάζεται στην πράξη της διαίρεσης. Η Python εκτελεί ακέραια διαίρεση, εκτός αν δηλώσουμε ότι θέλουμε να κάνει διαίρεση πραγματικών αριθμών. Ο πιο απλός τρόπος να το δηλώσουμε αυτό είναι να γράψουμε τον διαιρετέο ή τον διαιρέτη (ή και τους δυο) ως πραγματικούς.

```
print (7/2, 7/2.0, 7.0/2, 7.0/2.0, 7./2, 7/2., 7./2.)
```

Η ύψωση σε δύναμη δηλώνεται ως εξής.

```
print (9**2, 9**0.5)
```

Έστω ότι θέλουμε να φτιάξουμε ένα πρόγραμμα που θα υπολογίζει τις λύσεις της δευτεροβάθμιας εξίσωσης 2x2 - 5x+2=0.

```
a=2
b=-5
c=2
diak=(b*b-4*a*c)
print (diak)
```

Cryptography Packages: Η Python περιλαμβάνει ένα πακέτο που ονομάζεται κρυπτογραφία που παρέχει κρυπτογραφικές συναρτήσεις. Υποστηρίζεται από την Python 2.7, Python 3.4+ και PyPy 5.3+. Η βασική εγκατάσταση του πακέτου κρυπτογραφίας επιτυγχάνεται με την παρακάτω εντολή.

```
pip install cryptography
```

ΠΑΡΑΔΟΤΕΟ 01

Εκτελέστε τις εντολές δημιουργώντας ένα αρχείο .py και **σχολιάστε σε κάθε γραμμή τι συντελείται**.

Υποχρεωτικά! Προσθέστε **δικές σας τιμές** σε κάθε περίπτωση. Ανεβάστε το αρχείο py.