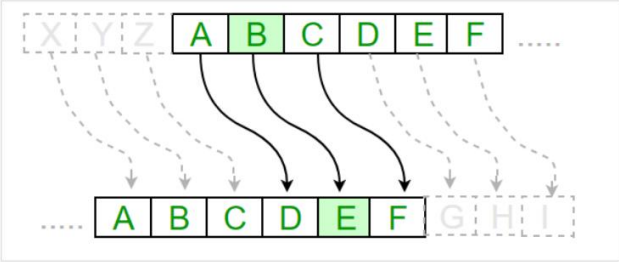
ΚΡΥΠΤΟΓΡΑΦΙΑ | ΚΛΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

ΚΛΑΣΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

Πρακτικά Ζητήματα

Εισαγωγή: Στο τελευταίο κεφάλαιο, ασχοληθήκαμε με την αντίστροφη κρυπτογράφηση. Αυτό το κεφάλαιο μιλάει για τον αλγόριθμο κρυπτογράφησης του Καίσαρα. Ο αλγόριθμος Caesar cipher έχει τα ακόλουθα χαρακτηριστικά:

- Αποτελεί μια απλή και εύκολη μέθοδος τεχνικής κρυπτογράφησης.
- Είναι απλός τύπος κρυπτογράφησης αντικατάστασης.
- Κάθε γράμμα απλού κειμένου αντικαθίσταται από ένα γράμμα με κάποιο σταθερό αριθμό θέσεων κάτω με αλφάβητο (πχ. Το κλειδί +3 μετατρέπει το γράμμα b σε e).



Κώδικας Python (Caesar Cipher):

```
# Filename: caesar.py
def encrypt(text,s):  #Ενδέχεται να πρέπει να
#διορθώσετε τον κώδικα – διαβάστε τα μηνύματα
#σφάλματος (part of the excercice)
result = ""

for i in range(len(text)):
  char = text[i]
  if (char.isupper()):
     result += chr((ord(char) + s-65) % 26 + 65)
   else:
     result += chr((ord(char) + s - 97) % 26 + 97)
return result

text = "CEASER CIPHER DEMO"
s = 4
print "Plain Text : " + text #ίσως έχει σφάλμα
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Ord(): Η συνάρτηση ord() επιστρέφει έναν ακέραιο που αντιπροσωπεύει τον χαρακτήρα Unicode. (e.g., Το P είναι 80).

Εξήγηση: Κάθε χαρακτήρας του κειμένου διασχίζεται ένας-ένας κάθε φορά.

- Με βάση το κλειδί κρυπτογράφησης κάθε χαρακτήρας μετατρέπεται σε διαφορετικό.
- Αφού ακολουθηθούν τα βήματα, δημιουργείται μια νέα συμβολοσειρά που αναφέρεται ως κρυπτογράφηση (cipher text)

Hacking Caesar Cipher: Το κρυπτογραφημένο κείμενο μπορεί να βρεθεί με διάφορες τεχνικές. Μία από είναι και το Brute Force Technique (επίθεση ωμής βίας), η οποία περιλαμβάνει τη δοκιμή κάθε πιθανού κλειδιού αποκρυπτογράφησης. Αυτή η τεχνική δεν απαιτεί μεγάλη προσπάθεια (στην συγκεκριμένη περίπτωση) και είναι σχετικά απλή.

```
# Filename: hack-caesar.py
message = 'GoodMorning' #encrypted message
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
for key in range(len(LETTERS)):
  translated = ''
  for symbol in message:
    if symbol in LETTERS:
       num = LETTERS.find(symbol)
       num = num - key
       if num < 0:
          num = num + len(LETTERS)
       translated = translated + LETTERS[num]
    else:
       translated = translated + symbol
  print('Hacking key #%s: %s' % (key, translated))
```

ΠΑΡΑΔΟΤΕΟ 05 (Caesar-cipher)

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.

Μετατρέψτε το hack-caesar σε συνάρτηση και εκτελέστε την με τον ακόλουθο τρόπο: Δημιουργήστε ένα κείμενο ή τοποθετήστε το σε μια μεταβλητή clear=”test example” εκτελέστε την κρυπτογράφηση και την αποκρυπτογράφηση με τις κατάλληλες εντολές.