Department of Computer Science - Τμήμα Πληροφορικής
University of Cyprus - Πανεπιστήμιο Κύπρου

Εργαστήρια ΕΠΛ 221
Χειμερινό 2017

Κατοίκων Εργασία 1
Ημερομηνία: 18/09/2017
Παράδοση: 02/10/2017

Υπεύθυνος Εργαστηρίου
Πέτρος Παναγή
(B118/petrosp@cs.ucy.ac.cy)

ΣΚΟΠΟΣ:

Σκοπός της άσκησης αυτής είναι:

- να εξοικειωθείτε με τα εργαλεία gcc, gdb, objdump και hexdump.
- να μάθετε τη χρήση των καταχωρητών.
- να μάθετε τις βασικές εντολές για λήψη αποφάσεων.
- να δουλέψετε με βρόχους (Loops).

ΑΣΚΗΣΗ:

Να γράψετε ένα πρόγραμμα σε ARMv8-A το οποίο θα κρυπτογραφεί ένα κείμενο που βρίσκεται αποθηκευμένο στην μνήμη ενός υπολογιστή με την συμμετρική μέθοδο του XOR.

C = (XOR(XOR C, KEY),KEY)

όπου **C** είναι ένας χαρακτήρας της συμβολοσειράς και **KEY** είναι το κλειδί κρυπτογράφησης και αποκρυπτογράφησης που παίρνει τις τιμές από 0 μέχρι 255.

Κατά την διαδικασία κρυπτογράφησης το αρχικό κείμενο στην μνήμη του υπολογιστή αντικαθίστατε από το κρυπτογραφημένο. Το αντίστροφο γίνεται κατά την αποκρυπτογράφηση.

Παραδείγματα εκτέλεσης:

1)

```
./a.out
Please Enter the Encryption Key (0-255):-30
Please Enter the Encryption Key (0-255):300
Please Enter the Encryption Key (0-255):123
[[[?[ZZZq[[3
Please Enter the Decryption Key (0-255):33
?6957?z.5z
hhkz;4>z;,?z;z439?z;#z{{{P
```

2)

```
./a.out
Please Enter the Encryption Key (0-255):123
[[[?[ZZZq[[3
Please Enter the Decryption Key (0-255):123
Welcome to EPL221 and Have a nice Day !!!
```

Η παράδοση της εργασίας να γίνει σύμφωνα με τις οδηγίες που σας έχουν δοθεί στα εργαστήρια.

1. Ο ARMv8-A κώδικας σας πρέπει να έχει σχόλια για κάθε γραμμή.
2. Να συμπεριλάβετε το σχεδιάγραμμα ροής (**flowchart**) για το πρόγραμμα σας.
3. Στο τέλος της έκθεσης να δημιουργήσετε ένα πίνακα που να περιέχει όλες τις εντολές που χρησιμοποιήσατε με την περιγραφή τους (δες παραδείγματα).

- **Περιορισμοί**

Δεν επιτρέπετε να ορίσετε συναρτήσεις.

Χρησιμοποιήστε καταχωρητές σύμφωνα με την τυποποίηση (Name Convention).

Η έκθεση να παραδοθεί στις 02/10/2017 την ώρα του εργαστηρίου.