Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εργαστήριο 3 – Ανταλλαγή κλειδιών κατά Diffie - Hellman

Προετοιμασία

1. Αποσυμπιέστε το zip αρχείο *diffie-hellman.zip*
2. Σε περιβάλλον cygwin ή κάποιο ισοδύναμο bash shell, τρέξτε το *bc* [και *όνομα script του bc, όπως φαίνεται παρακάτω*]

Εξερεύνηση της modular εκθετοποίησης

1. Υπολογίστε τις ακόλουθες ποσότητες:

   12^{100} mod 17=
   12^{1001} mod17=
   12^{10012} mod17=
   12^{100120} mod17=
   $12^{1001201}$ mod17=

   Σημ. Στο περιβάλλον bc η εκθετοποίηση x^a mod b γράφεται ως x^a%b

   Παρατηρείστε ότι ο χρόνος υπολογισμού στις παραπάνω πράξεις αυξάνεται εκθετικά!

2. i. Υπολογίστε τις παραπάνω ποσότητες με τη χρήση της *mpower*()

   ii. Υπολογίστε με τη χρήση της *mpower*() τις ακόλουθες ποσότητες:

   $89^{12345678987654321}$ mod 3112=
   $89^{123456789876543219999}$ mod 3112=

   Σημ.i Η *mpower*() εμπεριέχεται στο *discrete_log.bc*, η οποία φορτώνεται στο περιβάλλον της *bc* ως εξής:

   bc discrete_log.bc

   Σημ.ii Η σύνταξη της *mpower*() είναι η εξής:

   mpower (base,exponent,modulus)

Η πρόκληση του διακριτού λογάριθμου

Για μικρές τιμές, η λύση στο πρόβλημα του διακριτού λογάριθμου είναι υπολογιστικά εφικτή.

Άσκηση - πρόκληση: Βρείτε το *x,* τέτοιο ώστε 12^x=6 mod 17

Πρωτόκολλο των Diffie και Hellman

1. Με τον διπλανό σας εκτελέστε το πρωτόκολλο ανταλλαγής DH, με τα ακόλουθα στοιχεία:

   - g=3, και modulus = 2147484659
   - χρησιμοποιείστε αρχικά μόνον την *mpower*( )
   - επαληθεύστε τα αποτελέσματα με τα *alice.bc* και *bob.bc*

2. Εκτελέστε το *eve.bc* για να ανακτήσετε τα μυστικά