Simplified Standard Encryption Standard

Όνομα: Κωνσταντοπούλου Ευαγγελία
ΑΜ:1059560
Έτος: 3ο
Σχολή: Μηχανικοί Η/Υ

Ζητούμενο

Το project που ανέλαβα είναι η υλοποίηση της απλοποιημένης μορφής του συμμετρικού αλγόριθμου DES. Μιας και ο σκοπός της ύπαρξης του Simplified DES είναι εκπαιδευτικός, μου ζητήθηκε το πρόγραμμα που θα φτιάξω να απευθύνεται σε μαθητές. Έτσι επικεντρώθηκα στην αναλυτική, βήμα-προς-βήμα επεξήγηση των αναδιατάξεων, ολισθήσεων, λογικών πράξεων και συναρτήσεων που περιέχονται στον αλγόριθμο.

Γλώσσα και υλοποίηση

Ο κώδικας μου ζητήθηκε να γραφεί σε java (BlueJ). Τον κώδικα τον έγραψα σε σύστημα Linux. Για την υλοποίηση του αλγορίθμου χρειάστηκε να φτιάξω 7 κλάσεις:

Create Keys: Μέσα σε αυτή την κλάση δημιουργώ τα κλειδιά K1 και K2 , επομένως περιέχει τις αναδιατάξεις P10,P8 και τις αριστερές ολισθήσεις μίας και δύο θέσεων.

Encryption: Δέχεται το plaintext προς κωδικοποίηση. Περιέχει τις αναδιατάξεις Initial Permutation, Inversed Initial Permutation. Ύστερα περιέχει τη συνάρτηση mapping που περιλαμβάνει την Expanded Permutation,την πράξη XOR μεταξύ του αποτελέσματος αυτής και του SubKey, τα S-Boxes και την P4 αναδιάταξη. Υπάρχει η συνάρτηση FK όπου γίνεται άλλη μια πράξη XOR μεταξύ του αποτελέσματος του mapping με το αριστερό μισό της IP καθώς και η συνάρτηση SW (switch). Τέλος, έχω συμπεριλάβει μια συνάρτηση all που συνδυάζει όλες τις παραπάνω μεθόδους και τις τοποθετεί στη σωστή σειρά.

Simple DES: Η main συνάρτηση. Συνδέει τις Create Keys και Encryption και καθοδηγεί με μηνύματα τον χρήστη για τις εισόδους που πρέπει να εισάγει.

InspectInput / InspectInputExc: Exceptions που διασφαλίζουν ότι τα plaintext, Key και ciphertext που εισάγει ο χρήστης είναι δυαδικοί αριθμοί.

Practical Functions: Στην κλάση αυτή υπάρχουν οι μέθοδοι που μετατρέπουν δυαδικούς αριθμούς(δύο ξεχωριστά bit) σε δεκαδικούς αριθμούς και αντίστροφα. Χρησιμεύουν στη συνάρτηση mapping.

PrintArr: Με τη μέθοδο αυτή μπορώ και τυπώνω πίνακες ψηφίο προς ψηφίο.

Σημείωση: Λόγω της φύσης του προγράμματος εκτυπώνονται ειδικά μηνύματα σε κάθε βήμα του αλγορίθμου άρα είναι αρκετά κατανοητή η δομή του κώδικα. Επίσης υπάρχουν σχόλια για τη διευκόλυνση σας κατά τη διόρθωση.

Τεστ ορθότητας

Ένας απλός τρόπος για να ελέγξουμε την ορθότητα μιας τέτοιας υλοποόησης είναι να χρησιμοποιήσουμε τη σχέση:

X0 δυαδικός ψευδο-τυχαίος αριθμός
X(i+1) = if (i is even) then E(Xi , Xi) else D(Xi,Xi)

για τον υπολογισμό μιας ακολουθίας τιμών 8-bit: X0, X1…
Ε δηλώνει κρυπτογράφηση και D δηλώνει αποκρυπτογράφηση. Η αρχική τιμή επιλέγεται με μια σύντομη αναζήτηση προκειμένου να βρεθεί ακολουθία που δοκιμάζει αποτελεσματικά τις καταχωρήσεις του S-box. Για να δημιουργηθεί μια ψευδοτυχαία ακολουθία τιμών δοκιμής, η έξοδος ενός σταδίου χρησιμοποιείται τόσο ως κλειδί όσο και ως δεδομένα εισόδου για το επόμενο στάδιο.

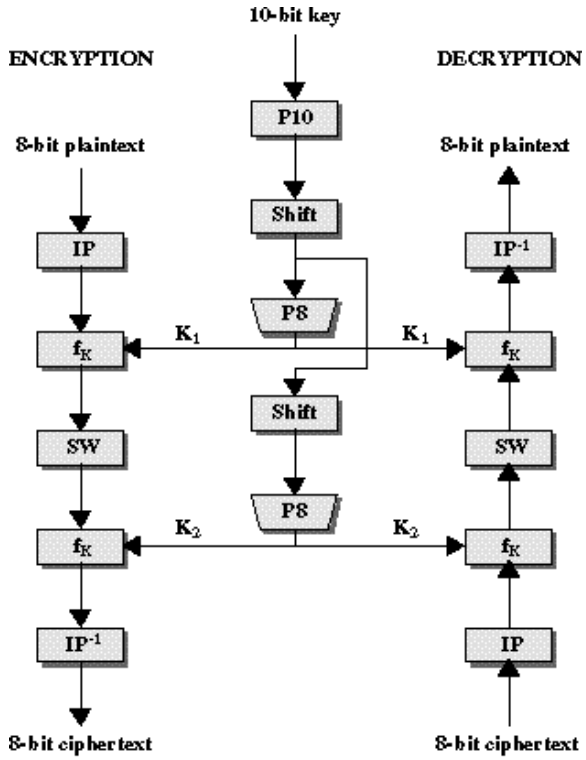

Figure 3.1 Simplified DES Scheme