Προγραμματιστική Ασκηση 4

PCY

Compile: g++ -std=c++11 -O2 -flto PCY.cpp -o PCY
Run:

- **Windows:** .\PCY.exe 6800
- **Linux:** ./PCY 6800

Το K (ελάχιστη στήριξη π.χ. 6800) χρησιμοποιείται στην πρώτη και στην δεύτερη φάση του αλγόριθμου. Το πλήθος των ζευγαριών κυμαίνεται στα 6500-7000 και των τριπλών στα 140-200. Προφανώς αν το K εφαρμοστεί και στις τριπλέτες, τότε δεν θα εμφανιστεί καμία ως συχνή.

Για τον αλγόριθμο PCY χρησιμοποιήθηκε η μη κρυπτογραφική συνάρτηση κατακερματισμού Fowler-Noll-Vo (FNV-1a 32-bit). Η επιλογή της συνάρτησης αυτής έγινε με βάση την ταχύτητα κατακερματισμού και το ποσοστό των συγκρούσεων για ακέραιους. Προφανώς για λόγους ταχύτητας αποφεύχθηκαν κρυπτογραφικές συναρτήσεις, εφόσον έχουν ως στόχο την ασφάλεια και όχι την ταχύτητα. Όπως αναφέρεται στα σχόλια του κώδικα ο κατακερματισμός 2M διαφορετικών κλειδιών σε 4M (2^22) κάδους είχε 2% ποσοστό συγκρούσεων. Η κατανομή των κλειδιών και η ταχύτητα σε σχέση με άλλες μη κρυπτογραφικές συναρτήσεις (Murmur2, DJB2a, SDBM, CRC32) ήταν καλύτερη. Για την δημιουργία λιγότερων από 2^32 κάδων (λόγω περιορισμών μνήμης), χρησιμοποιήθηκε μια τεχνική xor-fold για 22 bits από την 32bit έξοδο του FNV-1a, η οποία είναι πιο αποδοτική από την επιλογή απλά των πρώτων 22 bits σύμφωνα με τους δημιουργούς.

Αλγόριθμος FNV-1a:

```
hash = FNV_offset_basis

for each byte_of_data to be hashed
    hash = hash xor byte_of_data
    hash = hash × FNV_prime
endfor

return hash
```

Τα FNV_offset_basis και FNV_prime δίνονται από τους δημιουργούς για τις εκδόσεις διαφόρων εξόδων (32, 64, 128 bits).