Κρυπτογραφία 2015-2016



ΗΜΕΡΟΜΗΝΙΑ:22/2/2016

ΚΑΘΗΓΗΤΗΣ : Κωνσταντίνος Πατσάκης

ΜΕΛΗ ΟΜΑΔΑΣ :

Π10027 Ζαφειράκης Χριστόφορος

Π10143 Χαραλάμπους Τριαντάφυλλος

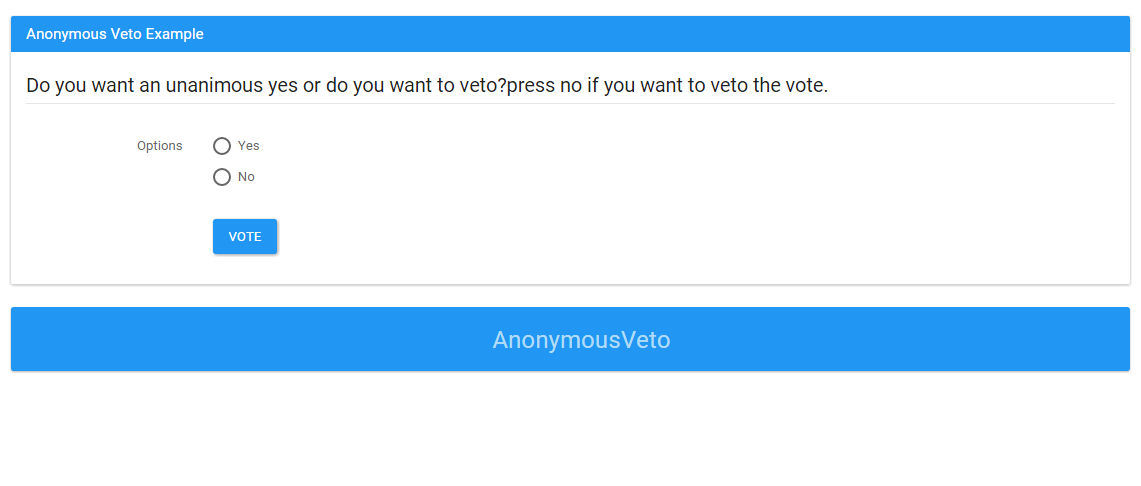
Χρησιμοποιήθηκε το Anonymous Veto Network protocol για να βγει το αποτέλεσμα της ψηφοφορίας.

Οι αριθμοί xi που παράγουμε μπορούν να γραφούν ως δύναμη του 2.Και ως knowledge proof για το xi χρησιμοποιούμαι το schnorr protocol με g = 2.

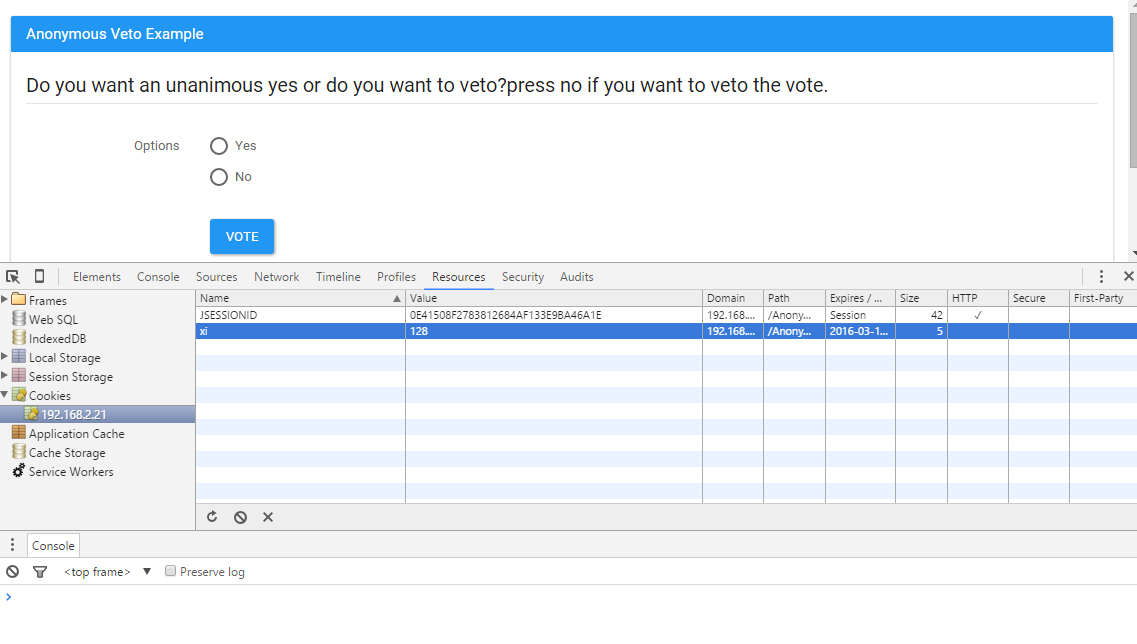
Ο κώδικας είναι σε java και για το xi χρησιμοποιούμε την class Random τις java και υψώνουμε το 2 στον αριθμό που μας βγάζει 2.

Αποφύγαμε να κάνουμε πράξεις όσο γινότανε λόγο του μεγέθους των αριθμών που προκύπταν οπότε η υλοποίηση των υπολογισμών έγινε ως μεταβλητές του τύπου x1,x2…. y1,y2…… etc και με απλοποιήσεις βάσει της λογικής του Anonymous Veto Network protocol.

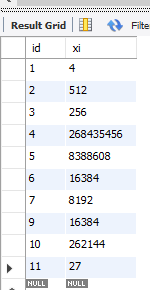
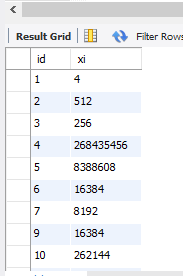
Ο χρήστης έχει 2 επιλογές για το ερώτημα πχ ναι η όχι.



Όταν ο χρήστης μπαίνει στην σελίδα της εφαρμογής του βάζουμε ένα cookie με το xi που θα έχει. Είναι πιθανό 2 χρήστες να τύχουν το ίδιο xi αλλά δεν μας επηρεάζει αφού χρησιμοποιείτε μόνο για επαλήθευση της επιλογής και όχι για ταυτοποίηση του χρήστη.

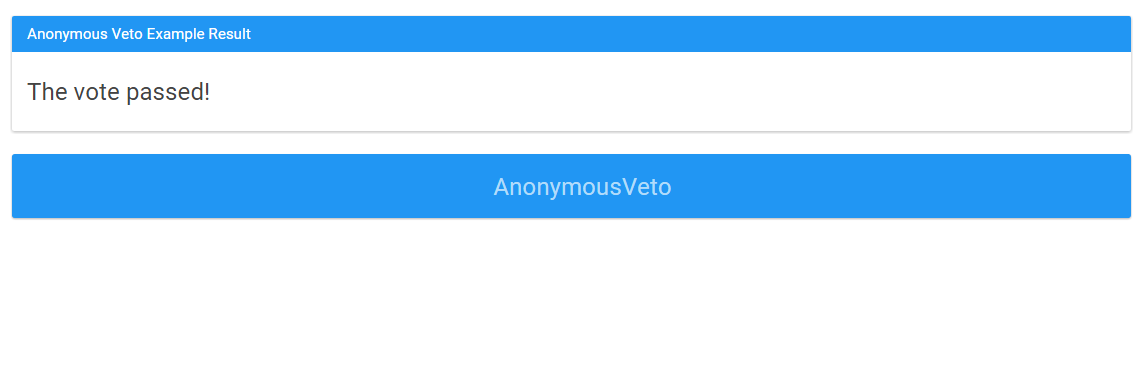


Αφού επιλεχθεί μια από της επιλογές και πατηθεί το vote εμείς κρατάμε στη βάση το xi αν ήταν yes και αν ήταν no τότε στη βάση βάζουμε ένα ri το οποίο είναι ένας τυχαίος αριθμός πολλαπλασιασμένος με το 3 για να μην γράφεται ως κάποια δύναμη με βάση το 2.

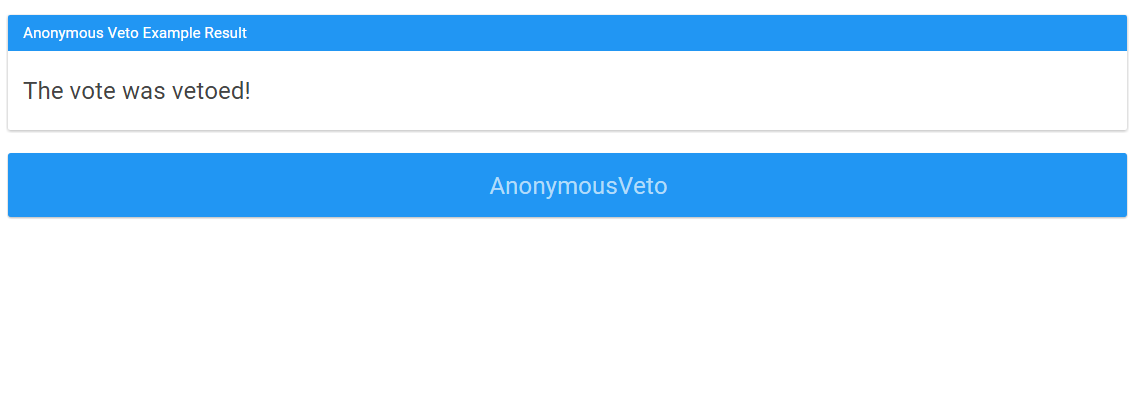


Από το 1-10 είναι xi το 11 είναι ένα ri όταν ζητηθεί το result γίνεται ο έλεγχος των xi βάση των τύπων του Anonymous Veto Network protocol πχ

Όταν η βάση είναι όπως στην πρώτη φωτογραφία:



Ενώ όταν η βάση είναι όπως στην δεύτερη φωτογραφία:



Η οθόνη για την εμφάνιση των αποτελεσμάτων.

