המשך פתרון תרגיל 11

גיבוב

4) תנו דוגמא שמראה שבגירסא של שיטת החילוק לפונקצית גיבוב בה $h(k) = k \bmod m$, כאשר $m = 2^p - 1$ ו- k היא מחרוזת תווים שמתייחסים אליה כאל מספר בבסיס 2^p (p טבעי כלשהו), אם מחרוזת x היא תמורה (=פרמוטציה, כלומר- בדיוק אותם תווים אך לא בהכרח באותו סדר) של מחרוזת y, אזי המחרוזות x ו- y מגובבות לאותו ערך. מה משמעות הדבר? (האם שיטה זו טובה או לא ומדוע?)

פתרון

ניקח לדוגמא את מחרוזות x **ו-** y:

x = “ABC”

y = “BCA”

p = 7

m = 2^7-1 = 127

נבצע גיבוב ל-x:

h(x) = “ABC” mod m = (65 + 66 + 67) mod 127 = 71

נבצע גיבוב ל-y:

h(y) = “BCA” mod m = (66 + 67 + 65) mod 127 = 71

כלומר, לקחנו מחרוזת y **שהיא תמורה של מחרוזת** x**, וקיבלנו ששתיהן מוגבבות לאותו הערך.**

שיטה זו אינה טובה **מכיוון** שפונקצית גיבוב שיוצרת התנגשות בין מפתחות באופן זה אינה מתחשבת **בסדר של התווים**, וזה **בניגוד ל"הנחת גיבוב אחיד פשוט"**. כלומר, לא בהתאם לרצוננו שפונקצית הגיבוב תפזר היטב את המפתחות בטבלה, ותהיה דומה עד כמה שניתן לפיזור אקראי. אך באופן זה הפיזור לא יהיה אקראי, שהרי לכל P שנבחר שתי המחרוזות יהיו מגובבות לאותו ערך.