**AMS – דו"ח:**

מגיש: ערן נאור

ת"ז: 300511987

חילקתי את הבדיקה לשתיים. 1- בזמן התקפה. 2- בזמן רגיל.

**1 - בזמן התקפה:**

* 5000 הודעות מ IP אקראיים
* 5000 הודעות מ IP ספציפי
* N = 950023 (ראשוני)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k-wise** | **| F2- F̃2|** | **F̃2** | **F2** |  |  | **זמן\שניה** |
| 4 | 60958 | 25065982 | 25005024 | 0.5 | 1 | 1 |
| 4 | 32269 | 25037303 | 25005034 | 0.2 | 1 | 2 |
| 4 | 11993 | 25017019 | 25005026 | 0.5 | 0.5 | 3 |
| 4 | 9825 | 24995207 | 25005032 | 0.2 | 0.5 | 5 |
| 2 | 44862 | 24960172 | 25005034 | 0.5 | 1 | 1 |
| 2 | 36589 | 24968439 | 25005028 | 0.2 | 1 | 2 |
| 2 | 20457 | 25025477 | 25005020 | 0.5 | 0.5 | 2 |
| 2 | 16505 | 25021533 | 25005028 | 0.2 | 0.5 | 5 |

**2- בזמן רגיל:**

* 10000 הודעות מ IP אקראיים
* N = 950023 (ראשוני)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **k-wise** | **| F2- F̃2|** | **F̃2** | **F2** |  |  | **זמן\שניה** |
| 4 | 835 | 9273 | 10108 | 0.5 | 1 | 1 |
| 4 | 541 | 9569 | 10110 | 0.2 | 1 | 2 |
| 4 | 432 | 9676 | 10108 | 0.5 | 0.5 | 3 |
| 4 | 183 | 10309 | 10126 | 0.2 | 0.5 | 5 |
| 2 | 978 | 9114 | 10092 | 0.5 | 1 | 1 |
| 2 | 516 | 9602 | 10118 | 0.2 | 1 | 2 |
| 2 | 541 | 10627 | 10086 | 0.5 | 0.5 | 2 |
| 2 | 232 | 10306 | 10075 | 0.2 | 0.5 | 5 |

**נשים לב:**

* F2 חסום – m < F2 < m2
  + למטה למספר ההודעות, במקרה שכל הודעה הגיעה מIp שונה – התפלגות אחידה.
  + ולמעלה למספר ההודעות בשניה, במקרה שכל ההודעות הגיעו מ ip יחיד – התפלגות מרוכזת.
* ממוצע של t השערות מקטין את השונות – ע"י צ'בישב.
* חציון מקטין את ההסתברות השגיאה ל (במקום 1/8) – ע"י צ'רנוף.

**מסקנות:**

* ככל שנבחר קטן יותר כך נקבל l גדול יותר, ולכן ההסתברות לשגיאה תרד.

l = מספר הפעמים בהם נבצע את שלב הממוצע

ולבסוף ניקח את החציון מבניהם.

* ככל שנבחר קטן יותר כך נקבל t גדול יותר, ולכן הסטיה שנקבל מF2 המקורי תקטן. כלומר נקבל קירוב טוב יותר ל F2.

t = מספר פונ' h שנעשה עבור X

ולבסוף ניקח את הממוצע שלהם.

**ניתוח התוצאות:**

* ניתן להבחין בקלות בזמן התקפה ולהגדיר סף.
* 4-wise נותן לנו דיוק מעט טוב יותר.

אך אנו נשתמש גם בפי 2 יותר זיכרון כדי לחשב אותו.