|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| לקוח | טבלת מפתחות id:   |  |  | | --- | --- | | 1 | מפתח 1 | | 2 | מפתח 2 | |
| שרת 1 | טבלת מפתחות id:   |  |  | | --- | --- | | 1 | מפתח 1 | |  |  |   טבלת חיבורים:   |  |  | | --- | --- | | מקור | יעד | | לקוח | שרת 2 | |
| שרת 2 | טבלת מפתחות id:   |  |  | | --- | --- | | 2 | מפתח 2 | |  |  | |
| שרת 3 |  |
| גוגל |  |

תכנון פרויקט onion

מבנה הפקטה:

|  |
| --- |
| דגל  id  [data] |

דגל – 1 – key  
 2- data

לקוח מגריל שרת ופונה אליו עם הצעה ל id. אם הid תפוס אצל השרת השרת סוגר את החיבור. יוצרים מפתח משותף. אם החלפת המפתחות מצליחה השרת מחזיר OK

1

Abc

1234

\_\_\_\_\_\_\_\_\_\_

2

Abc

Incripted data

הלקוח פונה אל השרת הבא בפרוקסי דרך השרת הראשון ועושה את אותה פעולה.

שוב פעם דרך שרת שלישי.

כל שרת מאזין לכל החיבורים. כאשר מגיעה הודעה, אם היא מגיעה מכיון הלקוח הוא מוריד שכבת הצפנה ומעביר אותה הלאה. לכיוון ההפוך הפוך

1. לקוח פונה לשרת 1 ויוצר מפתח. מקבל id
2. לקוח שולח הודעה מוצפנת במפתח 1 לשרת 1 שמקף את ההצפנה ושולח לשרת 2 זאת הודעת יצירת מפתח.

* אם סוקט מכיוון כלשהו נסגר לסגור גם את השני