אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

קריפטוגרפיה מועד א'- פתרון שאלה 3
שאלה 3 [20 נקודות]

בין אליס לבוב ישנם שני ערוצי שידור. איב יכולה להאזין לערוץ אחד בלבד. יהי q מספר ראשוני. אליס רוצה לשלוח הודעה $m \in \mathbb{Z}_q$, כאשר כל הודעה $m \in \mathbb{Z}_q$ אפשרית.

סעיף א [4 נקודות]
כדי לשלוח הודעה $m \in \mathbb{Z}_q$, אליס מגרילה באקראי בהתפלגות אחידה $r_1 \in \mathbb{Z}_q$, מחשבת $r_2 \leftarrow (m + r_1) \bmod q$, שולחת r_1 בערוץ אחד ושולחת r_2 בערוץ השני.
הסבירו בקצרה מדוע איב היכולה להאזין רק לאחד מהערוצים אינה לומדת מידע על ההודעה שאליס שלחה.

תשובה: איב אינה לומדת דבר אם היא מאזינה לערוץ הראשון כי r_1 נבחר באופן בלתי תלוי ב- m.
איב אינה לומדת דבר אם היא מאזינה לערוץ השני כי r_2 הוא הצפנה של m בעזרת מערכת הצפנה מושלמת (הוכחתם זאת בתרגיל בית 1 שאלה 2).

סעיף ב [5 נקודות]
הסבירו מדוע בוב לא יכול לדעת אם איב שינתה את המידע שנשלח על אחד הערוצים.

תשובה: ללא הגבלת הכלליות, נניח כי איב שינתה את תוכן ערוץ אחד מ- r_1 ל- $r_1' \in \mathbb{Z}_q$. במקרה זה $r_1' - r_2 \triangleq m'$ היא הודעה חוקית ב- $\mathbb{Z}_q$, ולכן בוב לא יוכל לזהות זאת.

סעיף ג [11 נקודות]
כדי להתגבר על הבעיה מסעיף ב, אליס מגרילה באקראי בהתפלגות אחידה חמש מחרוזות $r_1, a_1, b_1, a_2, b_2 \in \mathbb{Z}_q$, מחשבת $r_2 \leftarrow (m + r_1) \bmod q$, $c_1 \leftarrow (a_1 r_1 + b_1) \bmod q$ ו- $c_2 \leftarrow (a_2 r_2 + b_2) \bmod q$, שולחת r_1, c_1, a_2, b_2 בערוץ אחד ושולחת r_2, c_2, a_1, b_1 בערוץ השני. נתון כי איב יכולה להאזין לאחד מהערוצים ולשנות את המידע שנשלח בו.
הוכיחו כי לא משנה איך איב תשנה את תוכן השידור, ההסתברות שבוב לא יוכל לזהות שינוי היא לכל היותר $1/q$.

תשובה: מטעמי סימטריה, נוכל להניח לה"כ, כי איב שינתה את תוכן ערוץ אחד. אם איב שינתה את c_1, r_1 ל- c_1', r_1', אז בוב לא יגלה זאת רק אם c_1', r_1' היא נקודה על הישר $y \equiv a_1 x + b_1 \pmod q$ (כלומר, $c_1' \equiv a_1 r_1' + b_1 \pmod q$). נשים לב כי איב יודעת כי הנקודה c_1, r_1 היא על הישר, ולכן יודעת שישנם q ישרים אפשריים $y \equiv ax + c_1 - a r_1 \pmod q$ עבור $a \in \mathbb{Z}_q$. איב מצליחה לנחש נקודה על הישר $y \equiv a_1 x + c_1 - a_1 r_1 \pmod q$ אם ורק אם היא מצליחה לנחש את a_1, וזה קורה לכל היותר בהסתברות $1/q$.

אם איב שינתה את c_2, b_2 ל- a_2', b_2', אז בוב לא יגלה זאת רק אם c_2, r_2 היא נקודה על הישר $y \equiv a_2' x + b_2' \pmod q$, ושוב ההסתברות לכך היא לכל היותר $1/q$.