מודלים במסחר אלקטרוני - תרגיל בית 3

תאריך הגשה: 15/8/2007

המרצה: פרופ' משה טננהולץ. המתרגל: מר אלון אלטמן.

שאלה 1

בגלל תכיפות הבחירות בארץ הוחלט למחשב את מערכת הבחירות.

אזרחי המדינה מעוניינים לבצע הצבעה חשאית לבחירת ראש הממשלה.

לשם כך הם שולחים את ההצבעות "ש" או "פ" לשופט חשין, שכולם סומכים עליו. בהמשך נדון במספר שיטות למימוש ההצבעה ברשת מחשבים. נאמר ששיטה כלשהי עומדת בתנאי הסודיות, אם איש מלבד השופט חשין אינו מסוגל לגלות מהי הצבעתו של משתתף אחר כלשהו. לשופט חשין מותר לדעת מהן ההצבעות של המשתתפים.

א. על-מנת שהקולות לא יעברו בצורה גלויה, הוחלט להשתמש באלגוריתם RSA להצפנה. כל משתתף יצפין את ההצבעה שלו ("ש" או "פ") תחת המפתח הפומבי של חשין וישלח את התוצאה לחשין. האם שיטה זו עומדת בתנאי הסודיות? נמקו!

ב. כיצד ניתן לשפר את הפרוטוקול המוצע בא', כאשר עדיין חייבים להשתמש בה-צפנה ב-RSA, כך שההצבעה לא תיחשף?

ג. יו"ר ועדת הבחירות בחר בשיטה שעומדת בקריטריונים של סעיפים א' וב'. לאחר ההצבעה, התגלה כי אחד המשתתפים זייף הצבעות של משתתפים אחרים. הציעו שיטת הצבעה שחסינה לזיופים ועומדת בתנאי סעיפים א' וב'.