**הצעת הגשה לממ"ן תכנותי בנושא צופן RSA**

**נושא הפיתוח** – הנושא שבו ארצה לעסוק במטלה התכנותית הוא קריפטוגרפיה, ובפרט מערכת ההצפנה RSA. ההצעה מבוססת על התרגיל התכנותי מספר 2 בפרק 3 במדריך הלמידה.

במסגרת המטלה, ארצה לבנות תכנה המהווה את סט-הכלים הדרוש להצפנת RSA – התכנה תאפשר למשתמש להצפין, לפענח ולחולל פרמטרים מתאימים להצפנה. כמו כן, התכנה תאפשר למשתמש להפעיל שתי התקפות ידועות על RSA המאפשרות להשיג את המפתח הפרטי של ההצפנה בהינתן המודולוס והמפתח הפומבי (חזקת ההצפנה).

**אפיון האלגוריתמים וצורת מימוש** – התכנה תכתב בשפת Java ותכיל מימוש של מספר אלגוריתמים מרכזיים הנוגעים להצפנת RSA:

1. אלגוריתם מילר רבין לבדיקת ראשוניות – אלגוריתם זה הוא אלגוריתם הסתברותי המאפשר לבדוק האם מספר הוא ראשוני.
2. אלגוריתם לפירוק לגורמים של המודולוס בהינתן חזקת הפענוח – אלגוריתם זה הוא אלגוריתם הסתברותי המאפשר לפרק לגורמים בהינתן חזקת ההצפנה והפענוח (החשיבות של אלגוריתם זה היא בכך שקיומו מראה שלא מספיק להחליף את חזקת ההצפנה במקרה שהתגלתה חזקת הפענוח, אלא שיש להחליף גם את המודולוס).
3. אלגוריתם פולרד לפירוק לגורמים – האלגוריתם מחשב את אחד הגורמים הראשוניים של המודולוס (ניתן להגיע בקלות לגורם השני על ידי של המודולוס ב-) כאשר הגורמים הראשוניים של הם קטנים.
4. אלגוריתם וינר לגילוי חזקת הפענוח עבור חזקות קטנות – אלגוריתם וינר מבוסס על אלגוריתם אוקלידס ומאפשר לגלות את חזקת הפענוח בהינתן המודולוס כאשר מתקיים: .

**אפיון ממשקי משתמש** – התכנה תכלול ממשק גרפי המאפשר למשתמש לבחור את הפונקציונאליות הרצויה:

1. המשתמש יוכל להשתמש במחולל פרמטרים להצפנת RSA.
2. המשתמש יוכל להצפין הודעות וקבצים ולפענח אותם, באמצעות אלגוריתם RSA תוך שימוש בפרמטרים שיזין (תוך חלוקה של התוכן שמיועד להצפנה לבלוקים בגודל מתאים).
3. המשתמש יוכל לבצע בדיקות ראשוניות על מספרים שיבחר.
4. המשתמש יוכל לפרק לגורמים את המודולוס בהינתן חזקת הפענוח.
5. המשתמש יוכל להפעיל אלגוריתמים לתקיפה על RSA – בהינתן המודולוס והמפתח הפומבי (חזקת ההצפנה), המשתמש יוכל להפעיל, אם ניתן, את אלגוריתם פולרד או אלגוריתם וינר כדי לגלות את המפתח הפרטי (חזקת הפענוח).

התכנה תאפשר למשתמש להתאים את הליך ההצפנה ויצור הפרמטרים על ידי כך שתאפשר לקבוע seed למספרים הרנדומלים ולקבוע את גודל הבלוקים בהצפנה ואת גודל הפרמטרים להצפנה (בביטים). התכנה תתמוך גם בעבודה עם מספרים גדולים (למשל, 128 ביטים).

**מקור**:

D.R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. (‏﻿Chapman & Hall/CRC, 2006‎)‏