**מבוא להצפנה – תרגיל 5**

~~נסביר איך בעזרת הרעיון של חתימה עיוורת ניתן לקבל זיוף סלקטיבי של חתימה RSA עם התקפת הודעה נבחרת.~~

**~~הסבר:~~**

~~כאשר היא ההודעה המקורית ו- הוא המפתח הציבורי ו- היא ההודעה המוצפנת.~~

~~את החתימה בוב מבצע על ידי:~~

*~~ולאחר מכן אליס מחשבת את החתימה על ידי:~~*

*~~כאשר .~~*

*~~כאשר משתמשים פעמיים באותו מפתח RSA להצפנה ולחתימה, אנו מקבלים:~~*

*~~לאחר מכן, אליס מחשבת את:~~*

*~~כאשר .~~*

*~~כאשר בוב מבצע את החתימות הוא מחשב:~~*

תיאור הבדיקה של בוב את החתימה בעזרת המפתח הציבורי של אליס:

*החתימה תקינה אם: .*

ניתן לראות ש- זהה בשתי החתימות, והערך של הוא – .

זה אומר שאליס השתמשה באותו לחתימת שתי ההודעות.

*נראה מה קורה כאשר אליס משתמש באותו :*

*קיבלנו משוואה עם נעלם אחד . יש לה פתרונות.*

*נציב בשביל למצוא את הפתרונות:*

*נציב כעת ב- ונבדוק אם שווה ל- .*

*ולכן, המפתח הסודי של אליס הוא – .*