RSA Cipher

תיאור מתמטי:

- נגיד שאליס בוחרת את שני מספרים ראשוניים עצומים P ו- Q .
  נגיד ש- P=17 ו- Q=11 (היא חייבת לשמור על המספרים האלו בסוד).
- היא כופלת את 2 מספרים שבחרה, ומקבלת מספר נוסף והוא N
  במצב שלנו N=187.
- מה שתעשה אליס עכשיו היא תבחר עוד מספר נוסף במקרה הוא 7 גם הוא יהיה ראשוני.
- כעת אליס תפרסם את E ואת N במסגרת רשימה הדומה לספר טלפונים. הואיל ו-2 המספרים נחוצים לצורך הצפנה, הם צריכים להיות נגישים לכל מי שעשוי לרצות להצפין הודעה עבור אליס. יחד – המספרים הללו נקראים מפתח- ציבורי .)נוסף להיותו חלק מן המפתח הציבורי של אליס ,E יכול גם להיות חלק מן המפתח-הציבורי של כל אחד, אולם לכל אחד יהיה ערך שונה של N. והערך הזה תלוי בבחירה של כל אחד בערכי ה-P ו-Q
- כדי להצפין הודעה יש להמיר תחילה את ההודעה למספר- M. לדוגמא: מילה מומרת לספרות בינאריות על פי קוד ASCII, ואפשר להתייחס לספרות הבינאריות כאל מספר עשרוני. אחר כך M מוצפן כל שהוא נותן C. על פי הנוסחה: $C = M^e \pmod N$.
- לדוגמא אם בוב רוצה לשלוח לאליס הודעה:" X". על פי קוד ASCII אות זו מיוצגת ע"י המספר 1011000, המקביל למספר 88 העשרוני. לכן – M=88.
- כדי להצפין הודעה זו, בוב מחפש תחילה את המפתח הציבורי של אליס, ומגלה ש N=187, ו- E=7. נתונים אלו מספקים לו את הנוסחה הדרושה כדי להצפין הודעות לאליס. עבור M=88 הנוסחה תהיה:

$C = 88^7 \pmod{187}$.

- ניסיון לחשב זאת במחשבון אינו עניין פשוט, כיוון שתצוגת המחשבון לא מסוגלת להציג מספרים כה גדולים. אולם קיים תכסיס יפה לחישוב של חזקות בחשבון מודולרי. אנו יודעים כי מאחר ש- 1+2+4=7 .

$88^7 \pmod{187} = [88^4 \pmod{187} * 88^2 \pmod{187} * 88^1 \pmod{187}] \pmod{187}$

$88^1 = 88 = 88 \pmod{187}$

$88^2 = 7{,}744 = 77 \pmod{187}$

$88^4 = 59{,}969{,}536 = 132 \pmod{187}$

$88^7 = 88^1 * 88^2 * 88^4 = 88*77*132 = 894{,}432 = 11 \pmod{187}$

- אנחנו יודעים כי חזקות בחשבון מודולרי הן פונקציות חד-סטריות. לכן קשה מאוד לעשות היפוך לאחור של C=11 ולגלות את ההודעה המקורית. לפיכך איב אינה יכולה לפענח את ההודעה .

- אבל אליס כן יכולה לפענח את ההודעה. כיוון שהיא מחזיקה במידע מיוחד כלשהו- היא יודעת את ערכי P ו-Q. היא מחשבת מספר מיוחד- D- מפתח הפיענוח .המכונה גם המפתח הפרטי שלה. המספר D מחושב על פי הנוסחה הבאה:

E * D = 1(mod(P-1) * (Q-)1

7*D = 1(mod 16 * 10)

7*D = 1(mod 160)

D=23

(הסקת הערך שך D אינה ענין פשוט, אבל בעזרת האלגוריתם של אוקלידס ניתן לאליס למצוא את D במהירות ובקלות) .

- כדי לפענח את ההודעה אליס פשוט משתמשת בנוסחה הבאה:

.$M = C^d$ (mod 187) :

$M = 11^{23}$ (mod 187)

$M = [11^1$ (mod 187) * 11^2 (mod 187) * 11^4 (mod 187) * 11^{16} (mod 187)] (mod

)781 M = 11 * 121 * 55 * 154 (mod 187)

M == 88 = X in ASCII

ריווסט, שמיר ואדלמן יצרו למעשה פונקציה חד-כיוונית מיוחדת. זוהי פונקציה שרק מי שיש לו גישה למידע ייחודי, כלומר ערכי P ו-Q – יכול להפוך אותה. הפונקציה נעשית אישית באמצעות בחירת ערכי P ו-Q, אשר מכפלתם נותנת את N. הפונקציה מאפשרת לכל אחד להצפין הודעות עבור אדם מסוים, ע"י הצבה של N שערכו ידוע ברבים, בנוסחה. אבל רק מי שאמר לקבל את ההודעה יכול לפענח אותה. כיוון שהוא האדם היחיד שיודע את ערכי P ו-Q, וכן הוא היחיד שידע את מפתח-הפענוח D.

מפתח-פרטי: D (מורכב מ-P ו-Q).

מפתח-ציבורי:N, E