

הצפנה מסוג RSA - איך זה עובד? התשובה הקצרה: מתמטיקה.

הבסיס להצפנה שאינה סימטרית (מפתח ציבורי ומפתח פרטי), היא העובדה שפירוק מספר לגורמים היא בעיה קשה (בלתי פתירה) אפילו עבור סופר-מחשבים.

למשל, נסו את הקוד הבא:

```
k1 = 1298074214633706835075030044377087
```

```
k2 = 18014398241046527
```

```
key1 = k1*k2
```

```
print (key1)
```

```
for num in range (2,int(key1**0.5)):
```

```
    if key1%num == 0:
```

```
        print ('found= ', num)
```

נתון לכם  $key1$ , והתוכנית צריכה למצוא את  $k1$ ,  $k2$

המספרים שהשתמשתי בהם כאן הם עדיין קטנים בעולם האמיתי משתמשים במספרים בעלי מאות רבות של ספרות כ"א (ראשוניים).

מדובר על מספרים בביטים של 2048 ביט או אפילו 4096 ביט, 2 בחזקת 4096 זה מספר עם למעלה מאלף ספרות.

משתמשים במתמטיקה מודולרית, כדי למצוא את המפתחות. נראה כאן את הרעיונות המרכזיים מבלי להיכנס ממש לסיבות שבגללן השיטה עובדת.

יש לבצע את הצעדים הבאים:

1. לבחור 2 מספרים ראשוניים כלשהם. בדוגמה ניקח מספרים קטנים, למשל 2 ו 7.

2. נכפיל את המספרים ונקרא לתוצאה: המודולו.  $N = 14 = 7 * 2$

3. כעת נגדיר פונקציה שנקראת פי של  $N$ . מה היא אומרת? זהו מספר המספרים שהם ראשוניים ביחס ל-  $N$  - נרשום את כל המספרים האפשריים שהם מ 1 ועד 14:

1,2,3,4,5,6,7,8,9,10,11,12,13,14 נמחוק את כל אלה שיש להם מחלק משותף

עם 14 (כלומר מתחלקים ב 2 או ב 7), לכן נוריד את 2,4,6,8,10,12,14 וגם את 7 כמובן. כמה מספרים נותרו? התשובה היא 6, ולכן פי של 14 היא 6.

המספרים שנותרו הם 1,3,5,9,11,13 והם נקראים קו-פריים עם 14. הנוסחה לחשב את פי היא:  $(p-1)*(q-1)$  כאשר  $p$  ו  $q$  הם הראשוניים.

4. כעת נבחר את המפתח הציבורי. נקרא למפתח ההצפנה  $e$  מלשון Encryption. מספר זה צריך להיות בעל התכונות: א. גדול מ 1 וקטן מפי של  $N$  (6 בדוגמה שלנו) ב. הוא צריך להיות ראשוני ביחס ל  $N$  ולפי של  $N$  (ללא מחלקים משותפים). לפי א נשארו לנו רק 2,3,4 או 5. היחיד שעונה גם על ב. הוא: 5, כלומר  $e=5$

5. כעת נמצא את מפתח הפיענוח  $d$  עבור Decryption. הנוסחה שבה נשתמש היא:  $d*e \pmod{6} = 1$  -ה- 6 זה הפי של 14. בגלל שמצאנו כבר ש  $e$  הוא 5, אפשר כעת למצוא הרבה אפשרויות עבור  $d$ . למשל: 5 או קצת יותר גדול יהיה 11. ולכן אפשר לומר שמפתח ההצפנה שלנו הוא: (5,14) ומפתח הפיענוח הוא (11,14)

כעת ננסה להצפין ולפענח. השיטה שבה RSA עובדת היא על ידי העלאה בחזקה ולקיחת המודולו.

למשל נניח שההודעה שלי מורכבת מהאות: B. נהפוך את זה למספר על פי השיטה ש A היא 1, B היא 2 וכך הלאה.

לכן B הוא 2. נעלה אותו בחזקת המפתח הציבורי וניקח מודולו של 14, כלומר 2 בחזקת 5 זה 32, מודולו 14 זה: 4

4 היא ההודעה המוצפנת.

כדי לפענח ניקח את המסר המוצפן נעלה את 4 בחזקת מפתח הפיענוח שהוא 11, ואז ניקח מודולו 14. התוצאה תהיה: 2. קיבלנו חזרה את המסר שהוצפן.

בל נשכח שבעולם האמיתי המספרים הם גדולים מאד ולכן אחת המשימות היא למצוא ראשוניים גדולים מאד (יש עבור זה אלגוריתם היוריסטי). כמו כן כדי להראות שכל מה שהזכרנו למעלה באמת עובד, צריך ללמוד קצת תכונות של מתמטיקה מודולרית.

הבסיס נמצא במשפט הקטן של פרמה: (Fermat's Little Theorem)

שאומר: אם  $p$  הוא מספר ראשוני ו  $a$  הוא מספר כלשהו ראשוני ביחס ל  $p$  אז מתקיים השוויון:

$$a^{(p-1)} \bmod p = 1$$

בין היתר כדי למצוא את המפתח הפרטי (d) השיטה שהשתמשנו בסעיף 5 אינה יעילה במספרים גדולים וצריך להפעיל את האלגוריתם המורחב של אוקלידס. גם לייצור של מספרים ראשוניים גדולים צריך אלגוריתם כמו למשל מילר-רבין. צריך לדעת מהי העלאה בחזקה מהירה ומהו הפכי מכפילי (multiplicative inverse)

אפשר להוכיח את נכונות השיטה של RSA (וכך להראות שהיא תעבוד תמיד, לא משנה איזה מספר ניבחר).

מושגים כמו חתימה דיגיטלית, פונקצית האש חד כיוונית ועוד, יעזרו בהדגמת הידע בנושא.