

הקצה עז ג' בסיון אש"ס, 16.5.2010

1. לכנס משה, יהי (n, σ) סכום החתולים של n זנזונטא, $\sigma(18) = 1+2+3+6+9+18 = 39$

$$\sigma(18) = 1+2+3+6+9+18 = 39$$

$$\sigma(28) = 1+2+4+7+14+28 = 56.$$

יהיו זיקוק מספרים באסונייב שניים, ויהי $z = pq = n$. לניח כי שלוש המספרים $(n, \sigma(n), \sigma(\sigma(n)))$ יזוים. למצא אלקזריגב "מהר" שמפרק את n .

2. למצא את המסגה הצרפתי d עבור מערכת ההצפנה RSA

$$\text{עם מסגה צ'בורי } (5352381469067, 4240501142039) = (e, n).$$

אפשר להשתמש במחשב בני כפרק את n .

3. לניח e - Alice פרסמה מעגה צ'בורי (e, n) למערכת RSA, כאשר לא ניתן לפרק את n לזק זמן מעשי. Bob רוצה

לשלוח הודעה מוצפנת ל-Alice, אך הוא שולח כס את הפרד. האם זה בטוח? תנין.

4. הפעם Alice משתמשת במערכת ההצפנה של רבין. המסגה הצ'בורי שלה היא $(4757, n)$. לניח שהיא הסכימה עם Bob שהוא שולח

רק הודעה m שהיא אינה מספר זר או שיש לה חשיבות. האחרונה שיש, כאשר m כחוב במספר ג'ינארי. Bob שולח את המספר 1935. לפרק n .

$$5. \text{ למצא } n \text{ כן } 0 \leq n < 70 \text{ - } e \equiv n \pmod{3} \text{ } e = 5770$$