gamer

Ragnar Björn Ingvarsson, rbi3

23. október 2024

1

2

3

4 Endurtakið reikningana í 3a, d og e fyrir n = 77 og e = 7

a) Upplýsingar í opinberum lykli eru (n, e) en í einkalykli eru (n, d) (eða (p, q), bæði virkar)

Fáum skv. lýsingu að $n = 77$ og $e = 7$, svo við reiknum út p og q:

$$n = 77 = 7 \cdot 11$$

Svo við segjum að $p = 11$ og $q = 7$, og reiknum d:

$$d \equiv e^{-1} \bmod (p-1)(q-1) \tag{1}$$

Og við leysum þá andhverfuna:

$$de \equiv 1 \bmod 10 \cdot 6$$
$$\iff 7d \equiv 1 \bmod 60$$

Sjáum að fyrir $d = 43$ fæst $7 \cdot 43 = 301$ sem gefur 1 mátað við 60, svo við margföldum í gegn með 43 og fáum

$$43 \cdot 7 \cdot d \equiv 43 \cdot 1 \bmod 60$$
$$\iff d \equiv 43 \bmod 60$$

Svo við segjum að $d = 43$ og opinberi lykillinn er þá $(77, 7)$ og einkalykillinn er $(77, 43)$.

d) Við dulkóðum skilaboð m skv.

$$c \equiv m^e \bmod n \tag{2}$$

Svo við fáum að dulkóðuðu skilaboðin c eru

$$c \equiv 3^7 \bmod 77$$
$$\iff c \equiv 2187 \bmod 77$$
$$\iff c \equiv 31 \bmod 77$$

Svo $c = 31$.

e) Til að afkóða skilaboð þarf að nota formúluna

$$m \equiv c^d \bmod n \tag{3}$$

Svo við stingum inn gildunum og fáum

$$m \equiv 31^{43} \bmod 77$$
$$\iff m \equiv 31 \cdot (37^{21}) \bmod 77$$

Og höldum áfram svona og loks fæst

$$m \equiv 3 \bmod 77$$

Svo $m = 3$.