RSA

a) - cel mai cum. și util. alg. de cript. cu cheie publică

- sist. criptografic asimetric cele util. 2 chei dif pt cr. și decr: 1 pub, 1 priv

- gen. cheilor:

• se alog 2 nr. prime mari p și q util. pt a calc. un produs $n = p \cdot q$. Ac. este fol. ca modul (%) de cr / decr.

• se calc. exponentul e cale e un nr întreg $< (p-1)(q-1)$ și coprim (X)

↳ Cheia publică

• cheia privată este inversul modular al lui e mod $(p-1)(q-1)$

b) $n = 2881 = 43 \cdot 67$ $\quad e = 3/5/10$

care val este o cheie de cifrare validă

$\phi(n) = 42 \cdot 66 = 2772$

$1 < e < \phi(n)$ și $\text{cmmdc}(e, \phi(n)) = 1$

- $\text{cmmdc}(3, 2772) = 3 \neq 1$

... $\Rightarrow \underline{e = 5}$

c) $e = 13$

care este cheia de decript. d $\quad 851, 853, 856$

$de \equiv 1 \mod \phi(n)$

- $851 \cdot 2772 \equiv 1 \mod 2772$

$11063 \equiv 1 \mod 2772$

$(2772 \cdot 3) + \underline{2747} \equiv \underline{1} \mod 2772$ (A)

$\therefore$ (A) $\Rightarrow d = 853$

Sistem afin

$c \equiv a \cdot m + b \bmod 31$

a) ce valori poate lua a?

$1 \leq a < m$

$\left.\begin{array}{l} \text{cmmdc}(a,m) = 1 \\ 31 \text{ prim} \end{array}\right| \Rightarrow$

$\Rightarrow a \in \{1, 2, 3, \ldots, 30\}$

b) $(m, c) \in \{(10, 22), (12, 3)\}$

$$\begin{cases} 22 \equiv 10a + b \bmod 31 \\ 3 \equiv 12a + b \bmod 31 \end{cases} \Leftrightarrow$$

$$\begin{cases} 22 - 10a \equiv b \bmod 31 \\ 3 \equiv 12a + b \bmod 31 \end{cases}$$

$3 \equiv 12a + 22 - 10a \bmod 31$

$-19 \equiv 2a \bmod 31 \quad (+31 \ldots > 0)$

$12 \equiv 2a \Rightarrow a = 6 \ldots$