Cursuri 7 + 8

Conceptul de criptografie cu cheie publică:

K J

$Dec_{priv}(m)$

$Enc(m)_{K_{pub}}$

22.000.000

în loc de 22.000.000 chei secrete, doar o cheie publică și o cheie privată.

One way function

Factoring $(p, q) \xrightarrow{prod} pq^{N}$ easy

$N = pq \xrightarrow{factoring} (p, q)$ diffi

Probleme matematice

FACTORING
Given $N = pq$, find p and q.

RSA
Given e such that $\gcd(e, (p-1)(q-1)) = 1$
Given c
Find m such that $m^e = c \bmod N$.

QUADRES
Given a, determine if a is a square mod N.

SQR ROOT
Given a such that $a = x^2 \bmod N$, find x.

DLP (discrete logarithm)
Given $(G, \cdot)$ finite abelian group; $g, h \in G$ such that $h = g^x$
Find x

DHP (Diffie - Hellman) Given $(G, \cdot)$ finite abelian group
Given $g \in G$, $a = g^x$, $b = g^y$
Find c such that $c = g^{xy}$.

DDH Decision Diffie-Hellman problem

Given $g \in G$, $a = g^x$, $b = g^y$ and $c = g^z$, determine if $z = xy$

(x, y, z unknown!)

<u>Lemma</u> $(G, \cdot, 1)$ grup abelian finit

$\Rightarrow$ DHP nu este mai grea decât DLP

(Dem) Oracol $\mathcal{O}_{DLP}$, $\mathcal{O}_{DLP}(g^x, g) = x$. în timp polinomial.

Fie $a = g^x$, $b = g^y$

$\alpha = \mathcal{O}_{DLP}(a, g)$

$c = b^{\alpha}$ $\Rightarrow$ DHP rezolvată în timp polinomial.

Output c.

<u>Lema</u> DDH nu e mai grea decât DHP

$\mathcal{O}_{DDH}(g^x, g^y, g) = g^{xy}$

$d = \mathcal{O}_{DDH}(a, b, g)$

<u>if</u> $(d = c)$ <u>output</u> "da" <u>else</u> <u>output</u> "nu".

<u>Despre pătrate în corpuri prime</u>

$$sq : \mathbb{F}_p \longrightarrow \mathbb{F}_p$$

$$sq(\alpha) = \alpha^2$$

$sq(\mathbb{F}_p^{\times}) \leq \mathbb{F}_p^{\times}$ cu $[\mathbb{F}_p^{\times} : sq(\mathbb{F}_p^{\times})] = 2$

$\# sq(\mathbb{F}_p^{\times}) = \frac{p-1}{2}$

Legendre Symbol $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{dacă } p \mid a \\ +1 & \text{dacă } a \bmod p \in sq(\mathbb{F}_p^{\times}) \text{ (rest pătratic)} \\ -1 & \text{altfel.} \end{cases}$

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$, cam ineficient.

Mai bine folosim următoarele reguli de calcul

p, q prime

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

Legea de reciprocitate pătratică a lui Gauss

$$\Leftrightarrow \quad \left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{dacă } p, q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{altfel.} \end{cases}$$

Reguli adiționale :

$$\left(\frac{q}{p}\right) = \left(\frac{q \bmod p}{p}\right)$$

$$\left(\frac{qr}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{r}{p}\right)$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Atenție, p^2-1 întotdeauna div. cu 8 !

Dacă putem factoriza eficient, putem calcula simbolul Legendre

$$\left(\frac{15}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{5}{17}\right) = \left(\frac{17}{3}\right)\left(\frac{17}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1)^3 = 1$$

Următorul algoritm extrage rădăcina pătrată fără a factoriza:

Algoritmul lui Shanks de extragere a rădăcinii pătrate modulo p.

Inputs: p prim, $n \in \mathbb{Z}_p^\times$ a.î. $\exists\, r$, $n = r^2 \bmod p$.

Output r

- Find Q, S: $p-1 = 2^S Q$, Q odd
- Search for $z \in \{1, \dots p-1\}$ with $\left(\frac{z}{p}\right) = -1$.
- $M \leftarrow S$

  $c \leftarrow z^Q$

  $t \leftarrow n^Q$

  $R \leftarrow n^{\frac{Q+1}{2}}$

- Loop if $t = 1$ return R

  Otherwise use repeated squaring to find least i, $0 < i < M$, $t^{2^i} = 1$

  $b := c^{2^{M-i-1}}$

  $M \leftarrow i$

  $c \leftarrow b^2$

  $t \leftarrow t b^2$

  $R \leftarrow R b$

Dacă cel mai mic i cu $t^{2^i} = 1$ este $i = M$, nu există soluție.

Demonstrație: Observăm că în cursul algoritmului următoarele rămân constante:

$$c^{2^{M-1}} = -1$$

$$t^{2^{M-1}} = 1$$

$$R^2 = tn$$

La început

$$c^{2^{M-1}} = 2^{Q\cdot 2^{S-1}} = 2^{\frac{p-1}{2}} = -1$$ deoarece 2 nu e rest pătratic.

$$t^{2^{M-1}} = n^{Q\cdot 2^{S-1}} = n^{\frac{p-1}{2}} = 1$$ deoarece n rest pătratic

$$R^2 = n^{Q+1} = n t$$

La fiecare nouă iterație, cu M', c', t', R' noi valori care înlocuiesc M, c, t, R

$$c'^{2^{M'-1}} = \left(b^2\right)^{2^{i-1}} = c^{2^{M-i}\cdot 2^{i-1}} = c^{2^{M-1}} = -1$$

$$t'^{2^{M'-1}} = \left(t b^2\right)^{2^{i-1}} = t^{2^{i-1}} b^{2^i} = (-1)(-1) = 1$$

unde $t^{2^{i-1}} = -1$ deoarece $t^{2^i} = 1$ și $t^{2^{i-1}} \neq 1$ (i = cea mai mică val. a.î. $t^{2^i} = 1$)

$$b^{2^i} = c^{2^{M-i-1}\cdot 2^i} = c^{2^{M-1}} = -1$$

$$R'^2 = R^2 b^2 = t n b^2 = t' n$$

M is strictly smaller at each iteration!
so the algorithm halts!

$p = 17$, $n = 15$

$p - 1 = 16 = 2^4 \cdot 1$, $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{9-1}{8}} = -1$, $z = 3$,

$S = 4$, $Q = 1$

$M = 4$
$c = 2^Q = 3$
$t = n^Q = 15$
$R = \cancel{}\, 15^1$

Repeat squaring

$15^2 = (-2)^2 = 4$

~~$15^2 = 3^2 \cdot 5^2 = 9 \cdot 8 = 72 = 68 = 4$~~

$4^2 = 16 = -1$
$(-1)^2 = 1 = (-1)^2 = 4^4 = 15^8 = 15^{2^3}$, $i = 3$

$b = c^{2^{M-i-1}} = 3^{2^{4-3-1}} = 3^1 = 3$

$M = 3$

$c = 9$

$t = 15 \cdot 3^2 = \cancel{45 = 45 - 34} \; 5 \cdot 27 = 5 \cdot 10 = 16$

$R = 15 \cdot 3 = 11$

Repeat squaring $\cancel{11^2 = (-6)^2 = 36 - 34 = 2}$

$\cancel{2^2 = 4}$

$\cancel{4^2 = -1}$

$\cancel{(-1)^2 = 1 = (-1)^2 = 4^4 = 2^8 = 11^{16} = 11^2} \; 4$, $\cancel{\boxed{i=4}}$

$\cancel{f = c^{2^{4-4-1}}}$ ~~nu e soluție ?~~

$16 = -1$, $\boxed{i = 1}$

$b = c^{2^{M-i-1}} = 9^{2^{3-1-1}} = 81 - 68 = 13 = (-4)$

$M = 1$

$C = 16$

$t = 1$

$R = 11 \cdot 4 = (-1) = 10(-1) = 7$

Acum $t = 1 \Rightarrow$ return 7. Da $7^2 = 49 - 34 = 15$!

Teoremă FACTORING și SQRROOT sunt polinomial-time echivalente

SQRROOT $\hookrightarrow$ FACTORING

O_F = factoring oracol

Dat $z = x^2 \bmod N$, cum calculăm x ?

$O_F(N) = \text{"}\prod p_i^{\alpha_i}\text{"}$

$s_i = \sqrt{z} \bmod p_i$ folosind Shanks

mai greu, dar în cazul $N = pq$

$s_1 = \sqrt{z} \bmod p$ găsim X : $\begin{cases} x \bmod p = s_1 \\ x \bmod q = s_2 \end{cases}$

$s_2 = \sqrt{z} \bmod q$

$\Rightarrow X^2 \bmod pq = z.$

FACTORING $\hookrightarrow$ SQRROOT

Again $N = pq$. Assume O_S face $\sqrt{z} \bmod N$.

Pick random $x \in \mathbb{Z}_N^\times$

$$z = x^2 \bmod N$$

$$y = \sqrt{z} \bmod N \quad \text{cu } O_S$$

Există 4 asemenea rădăcini deoarece $N = pq$.

Cu prob. de 50% obținem $y \neq \pm x \bmod N$ (altfel repetăm)

$x^2 = y^2 \bmod N \Rightarrow N \mid (x-y)(x+y)$

dar $N \nmid (x-y)$, $N \nmid (x+y)$, deci factorii lui N

sunt distribuiți aici. Deci $\gcd(x-y, N) = p$ sau q.

Lemă RSA nu este mai grea decât FACTORING.

O_F oracol $\Rightarrow$ găsim p și q, calculăm $\phi = \varphi(N)$, calculăm

$$d = \frac{1}{e} \bmod \phi \Rightarrow c^d = m^{ed} = m^{1 \bmod \phi} = m \pmod N$$

O.K.

Cifrări asimetrice

1. RSA : istoric, primul algoritm cu cheie publică.

Alice alege nr. prime mari p, q:

Calculează $N = pq$. $\varphi(N) = pq(1-\frac{1}{p})(1-\frac{1}{q}) = (p-1)(q-1) = \# \mathbb{Z}_N^\times$

Alege e : $\gcd(e, (p-1)(q-1)) = 1$.

Cheia publică (N, e). $= K_p$

Găsește d : $ed \equiv 1 \mod (p-1)(q-1)$

Cheia privată (d, p, q). (secretă) : K_s

Bob calculează și trimite $c = m^e \mod N$.

Alice calculează $c^d \mod N$

Teoremă : $m = c^d \mod N$

Dem $\# \mathbb{Z}_N^\times = (p-1)(q-1)$, deci $\forall x \in \mathbb{Z}_N^\times$
$x^{(p-1)(q-1)} = 1 \mod N$

~~Pentru un $s \in \mathbb{Z}$~~

$$\cancel{ed - s(p-1)(q-1) = 1}$$

$$c^d = (m^e)^d = m^{ed} = m^{1+s(p-1)(q-1)} = m \cdot m^{s(p-1)(q-1)}$$

~~Dacă $m \in \mathbb{Z}_N^\times \Rightarrow m^{(p-1)(q-1)} = 1 \mod N \Rightarrow m$~~

~~Dacă $p \mid m$~~

$ed \equiv 1 \mod (p-1)(q-1)$

$$\Rightarrow \begin{cases} ed \equiv 1 \mod (p-1) \\ ed \equiv 1 \mod (q-1) \end{cases} \Rightarrow \begin{cases} ed = K(p-1)+1 \\ ed = h(q-1)+1 \end{cases}$$

Dacă $\gcd(m, p) = 1$

$m^{p-1} = 1 \mod p$

$m^{ed} = m^{K(p-1)+1} = (m^{p-1})^K m \equiv 1^K m = m \mod p$

Dacă $p \mid m$

$m^{ed} \equiv 0 \equiv m \mod p$

La fel $m^{ed} \equiv m \mod q$

Deoarece $\gcd(p, q) = 1 \Rightarrow \boxed{m^{ed} = m \mod N}$

<u>Obs</u> ~~Dacă problema RSA dificilă $\Rightarrow$ RSA OPA - sigură~~ nici acum.

<u>Obs</u> Dacă cunoaștem N, e, d, putem factoriza N.

Dem $ed - 1 = s(p-1)(q-1)$

Alegem un $x \in \mathbb{Z}_N^{\times}$, $x^{ed-1} \equiv 1 \mod N$

Dar $ed-1$ par, fie $y_1 = \sqrt{x^{ed-1}} = x^{\frac{ed-1}{2}}$

$y_1^2 - 1 = 0 \mod N$

deci $(y_1-1)(y_1+1) = 0 \mod N$

Dacă ~~ori~~ $y_1 \neq \pm 1 \mod N$, factorii lui N se distribuie între $y-1$ și $y+1$ deci $\gcd(y_1-1, N) = p$ sau q.

Dacă $y_1 = \pm 1 \mod N$

- $y_1 \equiv -1 \mod N$ return and pick another x
- $y_1 = 1 \mod N$

  $y_2 = \sqrt{y_1} = x^{\frac{ed-1}{4}}$

din nou $y_2^2 - 1 = y_1 - 1 = 0 \mod N$

$\gcd(y_2-1, N)$ poate fi un factor al lui N

Asta se repetă până când $\frac{ed-1}{2^t}$ devine impar.

În cazul acesta se alege altă valoare x

Exemplu $N = 1441499$, $e = 17$, $d = 507905$, $x = 2$

$\Rightarrow y_1 = 1$, $y_2 = 1$, $y_3 = 119533$, $\gcd(y_3-1, N) = 1423$

Obs Dacă știm N și $\varphi(N)$, putem factoriza N.

$$\varphi(N) = (p-1)(q-1) = pq - p - q + 1$$

$$S = N + 1 - \varphi(N) = p + q$$

$$X^2 - SX + P = 0$$

are soluții p, și q.

$N = 18923$

$\phi = 18648$

$$S = N + 1 - \phi = 18924 - 18648 = 2\cancel{7}6$$

$$X^2 - 276X + 18293 = 0$$

$$\Delta = 276^2 - 4 \cdot 18\cancel{9}23 = \cancel{2\,1\,0\,2\,4\,5\,7\,6}-$$

$$= 76176 - \underset{75692}{\cancel{73172\ 3004}} = 484 = 4 \cdot 121$$

$$\sqrt{\Delta} = 22$$

$$p, q = \frac{276 \pm 22}{2} = 138 \pm \cancel{11} \begin{cases} 149 \\ 127 \end{cases}$$

Shared modulus Presupunem că mai mulți useri folosesc

același N și au doar (e_i, d_i) diferite.

> atac prin insider

Știe $e_1, d_1 \Rightarrow$ factorizează $N \Rightarrow$ află $\varphi(N) = (p-1)(q-1)$

$\Rightarrow$ află $d_2 = e_2^{-1} \bmod (\varphi(N))$!

> atac din exterior

Alice trimite același mesaj m folosind cheile publice

(N, e_1) și (N, e_2) ale unor useri.

$$c_1 = m^{e_1} \bmod N$$
$$c_2 = m^{e_2} \bmod N$$

Eve

Calculează $t_1 = e_1^{-1} \bmod e_2$

$$t_2 = \frac{e_1 t_1 - 1}{e_2} \qquad \frac{e_1 t_1 - 1}{e_2}$$

deci $e_2 t_2 = e_1 t_1 - 1$

$$C_1^{t_1} C_2^{-t_2} = m^{e_1 t_1} m^{-e_2 t_2} = m^{1 + e_2 t_2 - e_2 t_2} = m \mod N$$

<u>Exemplu</u> $N = 18923$, $e_1 = 11$, $e_2 = 5$

$c_1 = 1514$, $c_2 = 8189$

$t_1 = 11^{-1} \mod 5 = 1^{-1} \mod 5 = 1$

$t_1 e_1 = 11$

$t_2 = \frac{11-1}{5} = 2$

$m = c_1^{t_1} c_2^{-t_2} = 100 \mod N$

în cazul în care c_2 inversabil

<u>Morala</u> - mesajul să fie randomly padded before transmission
- use biger encoding exponents like $e = 65537$.

Elgamal

Altfel decât la RSA, parametrii publici pot fi folosiți de mai mulți useri în același timp.

<u>Public</u> p - prim mare, ≈ 1024 bits

$p-1$ divizibil printr-un prim mediu $q \approx 160$ bits

$g \in \mathbb{F}_p^\times$ such that $q \mid \mathrm{ord}(g)$

$g = r^{\frac{p-1}{q}} \mod p \neq 1$ pt un $r \in \mathbb{F}_p^\times$

$G = \langle g \rangle$, $|G| = q$ domain parameter.

Cazul făcut curent g generator... pt $\mathbb{Z}_p^\times$

Private key $K_s = x$

Public key $h = g^x \bmod p$.

(e mai ieftin de ales decât la RSA)

Criptare $m \in \mathbb{F}_p^\times$.

- Aleg cheie efemeră K
- $c_1 = g^K \bmod p$
- $c_2 = m \cdot h^K \bmod p$
- trimit (c_1, c_2)

Decriptare $\dfrac{c_2}{c_1^x} = \dfrac{m\, h^K}{g^{xK}} = \dfrac{m\, g^{xK}}{g^{xK}} = m$.

~~Obs DHP grea $\Rightarrow$ Elgamal CPA sigur.~~ nu acum

Lem Fie $\mathcal{O}$ un oracol de descifrat Elgamal.

$\mathcal{O}(h, (c_1, c_2)) = m$

Se dau g^x și g^y. Se cere g^{xy}.

Fie $c = (c_1, c_2) = (g^y, u)$ unde $u \in \mathbb{F}_p^\times$ random.

Calculăm $m = \mathcal{O}(h, (c_1, \underset{u}{c_2}))$

Atunci $\dfrac{u}{m} = \dfrac{m\, h^y}{m}$ (fiindcă $c_1 = g^y$) $= h^y = g^{xy}$!

Codificarea Rabin

- se bazează tot pe dificultatea factorizării.
- mai exact se bazează pe dificultatea extragerii de rădă cini pătrate mod (pq). [cele două probleme sunt echivalente]
- este mult mai rapid ca alte sisteme.

Fie numere prime ~~p,q~~ $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ fiindcă în cazul lor "square root" e foarte rapidă.

$K_s = (p, q)$. cheia secretă

$N = pq$, $B \in \{0, 1, \dots N-1\}$ ales random.

$K_p = (N, B)$ cheia publică

Criptare $\quad c = m(m+B) \bmod N$

Decriptare $\quad m^2 + mB - c = 0 \bmod N$

$\Delta = B^2 + 4c$

$m_{1,2} = (\sqrt{\Delta} \pm B)\frac{1}{2} \bmod N$

Sunt 2 răd mod p, deci 4 răd mod pq ...

~~Mai~~ Exemplu $\quad p = 127$, $q = 131$

$N = 16637$, $B = 12345$

$m = 4410 \hookrightarrow c = m(m+B) \bmod N = 4633$

Decryption $\quad \Delta = \left(\frac{B^2}{4} + c\right) \bmod N = 1500$

$\sqrt{\Delta'} \bmod p = \pm 22$, $p = 127$

$\sqrt{\Delta'} \bmod q = \pm 37$, $q = 131$

Lema Chineză : $\sqrt{\Delta'} = \pm 3705$ sau ± 14373

Scădem $\frac{B}{2}$: $\boxed{4410}$, 5851, 15078, 16519

Este necesară desambiguation. Din această cauză nu s-a folosit sistemul, deși e mai sigur și mai rapid ca RSA.

Criptarea Paillier

- p, q prime de aceeași lungime $\Rightarrow \gcd(pq, (p-1)(q-1)) = 1$
- $N = pq$
- K_s : d a.î. $\begin{cases} d \equiv 1 \bmod N \\ d \equiv 0 \bmod (p-1)(q-1) \end{cases}$ cu lema chineză
- K_p : N
- Mesajele m : $0 \leq m < N$

Criptarea Alegem r la întâmplare în $(\mathbb{Z}/N^2\mathbb{Z})^*$!

$$c = (1+N)^m \cdot r^N \bmod N^2$$

Decriptarea

Calculăm $t = c^d \bmod N^2$

$$= (1+N)^{md} \cdot r^{dN} \bmod N^2$$

$$= (1+N)^{md} \bmod N^2 \quad \text{fiindcă } (p-1)(q-1) \mid d$$

$$= 1 + mdN \bmod N^2$$

$$= 1 + mN \bmod N^2 \quad \text{fiindcă } d \equiv 1 \bmod N$$

<u>Atunci</u> $m = \dfrac{t-1}{N}$ împărțire cu rest.

$p = 5,\ q = 7,\ N = 35$

$5 \nmid 6$

$7 \nmid 4$

$$\begin{cases} d \equiv 1 \bmod 35 \\ d \equiv 0 \bmod 24 \end{cases}$$

$$\begin{array}{r} 35\,\cdot \\ 24 \\ \hline 140 \\ 70 \\ \hline 840 \end{array}$$

$M_1 = 24,\ y_1 = 24^{-1} \bmod 35,\ \boxed{y_1 = 31}$

$$0 = 35 = 1 \cdot 24 + 11$$
$$24 = 2 \cdot 11 + 2$$
$$11 = 2 \cdot 5 + 1$$

$$1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) = \cancel{3 \cdot 11 - 24} =$$

$$\cancel{= 3(-24) - 24 = (-4) \cdot 24 = 31 \cdot 24}$$

$M_2 = 35,\ y_2 = 35^{-1} \bmod 24 = 11^{-1} \bmod 24 = 11$

$\cancel{24 = 2 \cdot 11 + 2} \qquad \cancel{1 = 11 - 5 \cdot 2 = 11 - 5(-2 \cdot 11) =}$

$\cancel{11 = 5 \cdot 2 + 1} \qquad \cancel{= 11 \cdot 11}$

$$1 = \underbrace{11} - 5 \cdot \underbrace{2} = \underbrace{11} - 5\left(\underbrace{24} - 2 \cdot \underbrace{11}\right) =$$

$$= 11 \cdot \underbrace{11} - 5 \cdot \underbrace{24} = 11\left(-\underbrace{24}\right) - 5 \cdot \underbrace{24} = -16 \cdot \underbrace{24}$$

$$= 19 \cdot \underbrace{24}$$

$$\begin{array}{r} 24 \cdot \\ 19 \\ \hline 216 \\ 24 \\ \hline 456 \end{array} \qquad \begin{array}{l} 456 : 35 = 13 \\ 35 \\ \hline 106 \\ 105 \\ \hline =1 \end{array} \qquad \boxed{d = 456}$$

Criptarea lui 11 : $\quad r = 2$

$$c = 36^{11} \cdot 2^{35} \bmod 35^2$$

<u>Criptarea Goldwasser – Micali</u>

Se bazează pe dificultatea lui <u>QUADRES</u> resp. a factorizării

$N = pq$

<u>Cheia publică</u> Găsim K_p:

Fie y_p, y_q $\quad \left(\frac{y_p}{p}\right) = \left(\frac{y_q}{q}\right) = -1$

Lema Chineză $\quad \begin{cases} K \equiv y_p \bmod p \\ K \equiv y_q \bmod q \end{cases}$

K așezi "pseudopătrat"!

<u>Criptare</u> Dat bit $b \in \{0,1\}$, alege $x \in \mathbb{Z}_N^*$ la întâmplare

$$c = y^b x^2 \bmod N$$

(18)

<u>Decriptare</u> Dacă $\left(\frac{c}{p}\right) = 1 \Rightarrow b = 0$

Dacă $\left(\frac{c}{p}\right) = -1 \Rightarrow b = 1$

(cheia secretă este unul dintre p și q!)

$d = \sum a_i M_i y_i \bmod M$

$= 1 \cdot 24 \cdot 31 \bmod 840 = 744$

$744 : 35 = 21$
70
$=44$
35
11

$24, 48, 72, 96, 120, 144, 168, 192$

$36, 71, 106, 141, 176, 211, \cancel{246}$

$35k+1$ care nu se divide cu 24

31
24
124
62
744