

Systémy s verejným kľúčom

Využitie tzv. ťažkých problémov v kryptológii predpovedal už Shannon (1949).

- ▶ R.M. Needham one-way cipher (1968)
- ▶ Clifford Cocks z britskej Communications - Electronics Security Group (CESG 1973)
- ▶ zverejnený prvý kandidát, G. Purdy (1974)

$$f(x) = x^{2^{24}+17} + a_1 x^{2^{24}+3} + a_2 x^3 + a_3 x^2 + a_4 x + a_5 \bmod 2^{64} - 59$$

kde a_i sú 19 miestne ľubovoľné čísla.

- ▶ W. Diffie a M. Hellman: New Directions in Cryptography, IEEE (1976)

Najpopulárnejšie sú tieto problémy:

1. faktorizácia čísel: RSA, Rabin, Goldwasser - Micali
2. diskretný logaritmus v konečných poliach: ElGamal
3. diskretný logaritmus v konečných grupách: Menezes - Vanstone
4. problém naplnenia ruksaku (nákladový problém, subset sum problem): Merkle - Hellman, Chor - Rivest
5. dekódovanie lineárneho kódu: McEliece

RSA algoritmus

Ron Rivest, Adi Shamir, Len Adleman z MIT RSA (1977).

- Každý účastník siete zverejní tzv. verejný (šifrovací) kľúč (n, e) , kde $n = pq$ a $\gcd(e, \varphi(n)) = 1$.

RSA algoritmus

Ron Rivest, Adi Shamir, Len Adleman z MIT RSA (1977).

- ▶ Každý účastník siete zverejní tzv. verejný (šifrovací) kľúč (n, e) , kde $n = pq$ a $\gcd(e, \varphi(n)) = 1$.
- ▶ Zároveň si vypočíta tajný dešifrovací kľúč (n, d) , splňujúci rovnosť $ed = 1 \bmod \varphi(n)$.

RSA algoritmus

Ron Rivest, Adi Shamir, Len Adleman z MIT RSA (1977).

- ▶ Každý účastník siete zverejní tzv. verejný (šifrovací) kľúč (n, e) , kde $n = pq$ a $\gcd(e, \varphi(n)) = 1$.
- ▶ Zároveň si vypočíta tajný dešifrovací kľúč (n, d) , splňujúci rovnosť $ed = 1 \bmod \varphi(n)$.
- ▶ Otvorený text (správa) je $x \in Z_n$. Šifrovanie a dešifrovanie je dané vzťahmi $E(x) = x^e \bmod n$ a $D(y) = y^d \bmod n$.
- ▶ V norme sa používa $\lambda(n)$ namiesto $\varphi(n)$.

Možné použitie:

1. elektronický podpis

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)
3. identifikácia, kedy používateľ dokazuje, že je oprávnená osoba...

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)
3. identifikácia, kedy používateľ dokazuje, že je oprávnená osoba...
4. nepopretie obsahu (nonrepudiation) spochybnenie, že som niečo podpísal... (napr. cez postranný kanál vytvorí rovnaký platný podpis s inými parametrami)

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)
3. identifikácia, kedy používateľ dokazuje, že je oprávnená osoba...
4. nepopretie obsahu (nonrepudiation) spochybnenie, že som niečo podpísal... (napr. cez postranný kanál vytvorí rovnaký platný podpis s inými parametrami)
5. prenos kľúčov pre symetrickú kryptografiu

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)
3. identifikácia, kedy používateľ dokazuje, že je oprávnená osoba...
4. nepopretie obsahu (nonrepudiation) spochybnenie, že som niečo podpísal... (napr. cez postranný kanál vytvorí rovnaký platný podpis s inými parametrami)
5. prenos kľúčov pre symetrickú kryptografiu
6. elektronické bankovníctvo

Možné použitie:

1. elektronický podpis
2. utajenie správy (pomalé...)
3. identifikácia, kedy používateľ dokazuje, že je oprávnená osoba...
4. nepopretie obsahu (nonrepudiation) spochybnenie, že som niečo podpísal... (napr. cez postranný kanál vytvorí rovnaký platný podpis s inými parametrami)
5. prenos kľúčov pre symetrickú kryptografiu
6. elektronické bankovníctvo
7. elektronické hlasovanie

Výpočtové problémy

Squaring method a Timing attack (1996) Výpočet hodnoty

$R = y^d \bmod n$ kde d je w -bitové číslo

Let $s_0 = 1$.

For $k = 0$ upto $w - 1$:

 If (bit k of d) is 1 then

 Let $R_k = (s_k \cdot y) \bmod n$ •

 Else

 Let $R_k = s_k$ •

 Let $s_{k+1} = R_k^2 \bmod n$.

EndFor.

Return (R_{w-1}).

Ak máme možnosť merať spotrebu pre rôzne y , potom s pravdepodobnosťou ≥ 0.84 vieme odlíšiť situácie •

Ochrana: blinding - clonenie

1. Zvoľ náhodne $r \in Z_n, \gcd(r, n) = 1$.
2. Vypočítaj $y' = y \cdot r^e \bmod n$.
3. Vypočítaj $x' = (y')^d = x \cdot r^{ed} = x \cdot r \bmod n$.
4. Vypočítaj $x = (x') \cdot r^{-1} \bmod n$.

Systémy s verejným kľúčom

RSA algoritmus

Výpočtové problémy pri použití RSA-algoritmu

Faktorizácia modulu

Rabinov algoritmus

Goldwasser-Micaliho algoritmus

Paillierov algoritmus

Hľadanie vhodných prvočísel

Je dosť veľa prvočísel?

Hľadanie náhodného prvočísla

Rýchle dešifrovanie

Voľba šifrovacieho exponentu

Hľadanie vhodných prvočísel

Dokazovanie prvočíselnosti má dlhú históriu.

1. *Eratosthenovo sito* - prakticky použiteľné len pre malé P .

Hľadanie vhodných prvočísel

Dokazovanie prvočíselnosti má dlhú históriu.

1. *Eratosthenovo sito* - prakticky použiteľné len pre malé P .
2. *Wilsonova veta* - prakticky použiteľné len pre malé P .

Hľadanie vhodných prvočísel

Dokazovanie prvočíselnosti má dlhú históriu.

1. *Eratosthenovo sito* - prakticky použiteľné len pre malé P .

2. *Wilsonova veta* - prakticky použiteľné len pre malé P .

P je prvočíslo vtedy a len vtedy ak

$$(P - 1)! = -1 \bmod P$$

3. *Fermatova veta* - chyba $\text{Prob} < \frac{1}{2} P^{-\frac{\ln \ln \ln P}{2 \ln \ln P}}$.

$$2^{340} = 1 \bmod 341, \text{ ale } 341 = 11 * 31$$

$$3^{90} = 1 \bmod 91, \text{ ale } 91 = 7 * 13$$

$$a^{560} = 1 \bmod 561, \text{ gcd}(a, 561) = 1, \text{ ale } 561 = 3 * 11 * 17$$

Hľadanie vhodných prvočísel

Dokazovanie prvočíselnosti má dlhú históriu.

1. *Eratostenovo sito* - prakticky použiteľné len pre malé P .

2. *Wilsonova veta* - prakticky použiteľné len pre malé P .

P je prvočíslo vtedy a len vtedy ak

$$(P - 1)! = -1 \bmod P$$

3. *Fermatova veta* - chyba $Prob < \frac{1}{2} P^{\frac{-\ln \ln \ln P}{2 \ln \ln P}}$.

$$2^{340} = 1 \bmod 341, \text{ ale } 341 = 11 * 31$$

$$3^{90} = 1 \bmod 91, \text{ ale } 91 = 7 * 13$$

$$a^{560} = 1 \bmod 561, \gcd(a, 561) = 1, \text{ ale } 561 = 3 * 11 * 17$$

4. *Solovayov test* - pre ľubovoľné prvočíslo $P > 2$ platí

$$J\left(\frac{a}{P}\right) = a^{\frac{1}{2}(P-1)} \bmod P.$$

Ak rovnosť neplatí, potom je P číslo zložené. Ak platí, tak máme aspoň 50% šancu, že je to prvočíslo.

Pravdepodobnosť chyby

- ▶ A: udalosť, že číslo danej veľkosti je zložené

Pravdepodobnosť chyby

- ▶ A : udalosť, že číslo danej veľkosti je zložené
- ▶ B : S-S odpovie $P = p \cdot m \times$ za sebou, $P(B/\bar{A}) = 1$

Pravdepodobnosť chyby

- ▶ A : udalosť, že číslo danej veľkosti je zložené
- ▶ B : S-S odpovie $P = p \cdot m \times$ za sebou, $P(B/\bar{A}) = 1$
- ▶ $P(B/A) \leq 2^{-m}$, $P(A/B) = ?$

Pravdepodobnosť chyby

- ▶ A : udalosť, že číslo danej veľkosti je zložené
- ▶ B : S-S odpovie $P = p \times m$ za sebou, $P(B/\bar{A}) = 1$
- ▶ $P(B/A) \leq 2^{-m}$, $P(A/B) = ?$
- ▶ $1 - P(A) =$
- ▶ (počet p) / (počet nepárnych čísel $n \leq P \leq 2n$) $= 2 / \ln n$

Pravdepodobnosť chyby

- ▶ A : udalosť, že číslo danej veľkosti je zložené
- ▶ B : S-S odpovie $P = p \cdot m \times$ za sebou, $P(B/\bar{A}) = 1$
- ▶ $P(B/A) \leq 2^{-m}$, $P(A/B) = ?$
- ▶ $1 - P(A) =$
- ▶ (počet p) / (počet nepárnych čísel $n \leq P \leq 2n$) $= 2 / \ln n$
- ▶ $P(A/B) = \dots (\ln n - 2) / (\ln n - 2 + 2^{m+1})$,
 $n = 2^{512}$, $m = 100$, $P(A/B) = 0.139 \times 10^{-27}$

4. *Rabin - Mullerov test* (MV Fermatova)

Let $P - 1 = 2^k m$, m -nepárne, $a \in Z_P^*$, $b = a^m \pmod{P}$.

If $b = 1 \pmod{P}$ then P je prvočíslo.

Else

For $i = 0$ upto $k - 1$:

 If $b = -1 \pmod{P}$ then P je prvočíslo.

Else

$b = b^2 \pmod{P}$.

EndFor.

Return P je zložené.

Odpoveď P je prvočíslo je správna aspoň v 75%.

5. *Prvočíselný problém* má polynomickú zložitosť.

Je p prvočíslo? patrí do triedy **P** a má zložitosť $\mathcal{O}(\log^6 p)$; (R-M test: $\mathcal{O}(\log^4 p)$ ak platí Riemanova hypotéza)...

Autori dôkazu sú Manindra Agrawal, Neeraj Kayal, Nitin Saxena, Indian Institute of Technology, Kanpur, august 2005. Ich pôvodná verzia mala zložitosť $\mathcal{O}(\log^{11} p)$.

Je dosť veľa prvočísel?

Carl Friedrich Gauss (1777-1855) ako 15-ročný: Pre počet prvočísel menších ako m , $\pi(m)$ platí

$$\pi(m) = \frac{m}{\ln m}.$$

Pre $m = 10^6$ je $\pi(m) = 78498$ a Gaussov odhad je 72382. Počet w -bitových prvočísel $\delta = \delta(2^w) - \delta(2^{w-1})$ a ich hustota medzi nepárnyimi číslami daného rozsahu $\varrho = \frac{\delta}{2^{w-2}}$.

w	δ	ϱ	ϱ^{-1}	$Prob$
64	$2 * 10^{17}$	0,045	22,18	$2 * 10^{-4}$
128	$2 * 10^{36}$	0,023	44,36	$2 * 10^{-7}$
256	$3 * 10^{74}$	0,011	88,72	$3 * 10^{-13}$
512	$2 * 10^{151}$	0,006	177,44	$3 * 10^{-23}$

Hľadanie náhodného prvočísla

Úloha: Generuj náhodné dvojmiestne prvočíslo.

1. Riešenie: Do urny dáme všetkých 21 prvočísel 11, 13, . . . , 89,

97. Pomocou GNZ generujeme jedno z čísel 1, 2, . . . , 21, atď'.

Toto sa nedá prakticky realizovať pre veľké P .

Hľadanie náhodného prvočísla

Úloha: Generuj náhodné dvojmiestne prvočíslo.

1. Riešenie: Do urny dáme všetkých 21 prvočísel 11, 13, . . . , 89, 97. Pomocou GNZ generujeme jedno z čísel 1, 2, . . . , 21, atď.

Toto sa nedá prakticky realizovať pre veľké P .

2. Riešenie: Pomocou GNZ generujeme jedno z 45 dvojmiestnych nepárnych čísel $P = 11, 13, 15, . . . , 99$ a testujeme ho na prvočíselnosť. Ak test nevyjde, vezmeme najbližšie ďalšie v poradí. Toto opakujeme, pokiaľ takto zvolené číslo prejde testom.

Hľadanie náhodného prvočísla

Úloha: Generuj náhodné dvojmiestne prvočíslo.

1. Riešenie: Do urny dáme všetkých 21 prvočísel 11, 13, . . . , 89, 97. Pomocou GNZ generujeme jedno z čísel 1, 2, . . . , 21, atď'. Toto sa nedá prakticky realizovať pre veľké P .
2. Riešenie: Pomocou GNZ generujeme jedno z 45 dvojmiestnych nepárnych čísel $P = 11, 13, 15, . . . , 99$ a testujeme ho na prvočíselnosť. Ak test nevyjde, vezmeme najbližšie ďalšie v poradí. Toto opakujeme, pokiaľ takto zvolené číslo prejde testom. Aká je pravdepodobnosť, že tým náhodne zvoleným prvočíslom bude 17? To dostanem, len pri voľbe 15 resp. 17, tj. $2/45 = 1/21$. Celkove existuje 7 prvočísel, ktoré zvolíme s pravdepodobnosťou $1/45$, 6 s pravdepodobnosťou $2/45$, 7 s $3/45$ a jedno (97) - s pravdepodobnosťou $4/45$.

3. Norma: Hellman-Bach patent, 31.5.1984 - tzv. silné $2b$ -bitové prvočíslo

1. generuj prvočíslo s , t , $|s| \approx |t| = b - 1$, napr. R-M testom
2. zvol' i_0 a nájdi prvočíslo $r = 2it + 1$, $i_0, i_0 + 1, \dots, i$, $|r| = b$
3. $p_0 = 2(s^{r-2} \bmod r)s - 1$, $|p_0| = b$
4. zvol' j_0 a nájdi prvočíslo $p = p_0 + 2jrs$, $j_0, j_0 + 1, \dots, j$, $|p| = 2b$
5. Return(p).

Vlastnosti: $r|p - 1$, $s|p + 1$, $t|r - 1$.

4. Riešenie v PGP(1994)

Najprv sa zvolí náhodné w -bitové nepárne číslo P . Zistí sa súdeliteľnosť so všetkými 16-bitovými prvočíslami. Potom sa vykoná maximálne 6 testov na základe Fermatovej vety pre $a = 2, 3, 5, 7, 11, 13$. Ak zvolené číslo prejde týmito testami, považuje sa za náhodne zvolené w -bitové prvočíslo. Doteraz nie je známe žiadne 512 bitové zložené číslo, ktoré by prešlo týmito testami. Jedno prvočíslo sa nájde na 200MHz PC asi za 2sec.

5. Riešenie LSI IBM-Tokyo (1997)

V prvej fáze sa zisťuje súdeliteľnosť P s 256 nepárnyimi prvočíslami $p = 3, 5, 7, \dots, 1633$. Výsledky sa ukladajú do tabuľky hodnôt $P \bmod p$. Týmto testom prejde v priemere jedno z 6,6 čísel. Ak P nevyhovuje, celá tabuľka sa jednoducho prepíše hodnotami $P + 2 \bmod p$, tj. pripočítaním 2 a prípadným odčítaním p . Z tabuľky 2.2 vidno, že napr. jedno z 178 nepárnych 512-bitových čísel je prvočíslo. Vzhľadom na prvú fázu je preto nutné vykonať v druhej fáze len $178 : 6,6 = 27$ testov Fermatovou vetou pre $a = 2$. Jedno modulárne umocňovanie trvá 5,9msec, tj. jeden pár prvočísel čip nájde za $5,9 \times 27 \times 2 = 0,32\text{sec}$. Pravdepodobnosť, že takto nájdené číslo $P \approx 2^{512}$ nie je prvočíslo je menšia, ako (Pozri Tab. 2.2) $\text{Prob} < 3 \times 10^{-23}$.

Rozmery čipu sú $5,31 \times 5,31\text{mm}^2$.

Rýchle dešifrovanie

Oprávnený adresát pozná faktorizáciu $n = pq$, môže pri dešifrovaní využiť CRT:

$$d_1 = d \pmod{p-1} \quad d_2 = d \pmod{q-1}$$

$$1 = uq \pmod{p} \quad 1 = vp \pmod{q}$$

$$y_1 = y \pmod{p} \quad y_2 = y \pmod{q}$$

$$x_1 = y_1^{d_1} \pmod{p} \quad x_2 = y_2^{d_2} \pmod{q}$$

$$x = x_1 \pmod{p} \quad x = x_2 \pmod{q}$$

$$x = x_1 uq + x_2 vp \pmod{n}$$

Rýchle dešifrovanie

Oprávnený adresát pozná faktorizáciu $n = pq$, môže pri dešifrovaní využiť CRT:

$$d_1 = d \pmod{p-1} \quad d_2 = d \pmod{q-1}$$

$$1 = uq \pmod{p} \quad 1 = vp \pmod{q}$$

$$y_1 = y \pmod{p} \quad y_2 = y \pmod{q}$$

$$x_1 = y_1^{d_1} \pmod{p} \quad x_2 = y_2^{d_2} \pmod{q}$$

$$x = x_1 \pmod{p} \quad x = x_2 \pmod{q}$$

$$x = x_1 uq + x_2 vp \pmod{n}$$

Príklad. Parametre A sú $p = 7, q = 11, n = 77, e = 7, d = 43$.

Vypočíta $u = 2, v = 8, d_1 = 1, d_2 = 3$. Ak $y = 58$, tak ...

Voľba šifrovacieho exponentu

1. Zlá je voľba $e = d$, $e^2 = 1 \pmod{\varphi(pq)}$, tj. napr.
 $e = 1$, $e = \varphi(pq) - 1$.

Voľba šifrovacieho exponentu

1. Zlá je voľba $e = d$, $e^2 = 1 \pmod{\varphi(pq)}$, tj. napr.
 $e = 1$, $e = \varphi(pq) - 1$.
2. Aby E bola permutácia na Z_n musí byť $\gcd(e, \varphi(pq)) = 1$, tj.
 $\gcd(e, p - 1) = \gcd(e, q - 1) = 1$.

Voľba šifrovacieho exponentu

1. Zlá je voľba $e = d$, $e^2 = 1 \pmod{\varphi(pq)}$, tj. napr.
 $e = 1$, $e = \varphi(pq) - 1$.
2. Aby E bola permutácia na Z_n musí byť $\gcd(e, \varphi(pq)) = 1$, tj.
 $\gcd(e, p - 1) = \gcd(e, q - 1) = 1$.
3. Počet správ, ktoré sa nezašifrujú, tj. $E(x) = x$ je daný
vzorcom $[1 + \gcd(e - 1, p - 1)][1 + \gcd(e - 1, q - 1)] \geq 9$.
Preto $\gcd(e - 1, p - 1)$, resp. $\gcd(e - 1, q - 1)$ musí byť malé.

Voľba šifrovacieho exponentu

1. Zlá je voľba $e = d$, $e^2 = 1 \pmod{\varphi(pq)}$, tj. napr.
 $e = 1$, $e = \varphi(pq) - 1$.
2. Aby E bola permutácia na Z_n musí byť $\gcd(e, \varphi(pq)) = 1$, tj.
 $\gcd(e, p - 1) = \gcd(e, q - 1) = 1$.
3. Počet správ, ktoré sa nezašifrujú, tj. $E(x) = x$ je daný
vzorcom $[1 + \gcd(e - 1, p - 1)][1 + \gcd(e - 1, q - 1)] \geq 9$.
Preto $\gcd(e - 1, p - 1)$, resp. $\gcd(e - 1, q - 1)$ musí byť malé.

Dôkaz:

- Rovnosť $x^e = x \bmod (pq)$ je podľa CRT ekvivalentná s sústavou $x^e = x \bmod p$ a $x^e = x \bmod q$.

Dôkaz:

- ▶ Rovnosť $x^e = x \bmod (pq)$ je podľa CRT ekvivalentná s sústavou $x^e = x \bmod p$ a $x^e = x \bmod q$.
- ▶ Rovnica $x^e = x \bmod p$ má jedno triviálne riešenie $x = 0$, a potom riešenia $x^{e-1} = 1 \bmod p$.

Dôkaz:

- ▶ Rovnosť $x^e = x \bmod (pq)$ je podľa CRT ekvivalentná s sústavou $x^e = x \bmod p$ a $x^e = x \bmod q$.
- ▶ Rovnica $x^e = x \bmod p$ má jedno triviálne riešenie $x = 0$, a potom riešenia $x^{e-1} = 1 \bmod p$.
- ▶ V grupe Z_p^* je $x = g^t$, kde g je generátor, preto riešime $g^{t(e-1)} = 1 \bmod p$.

Dôkaz:

- ▶ Rovnosť $x^e = x \bmod (pq)$ je podľa CRT ekvivalentná s sústavou $x^e = x \bmod p$ a $x^e = x \bmod q$.
- ▶ Rovnica $x^e = x \bmod p$ má jedno triviálne riešenie $x = 0$, a potom riešenia $x^{e-1} = 1 \bmod p$.
- ▶ V grupe Z_p^* je $x = g^t$, kde g je generátor, preto riešime $g^{t(e-1)} = 1 \bmod p$.
- ▶ Jedno riešenie je $t_0 = \frac{p-1}{\gcd(e-1, p-1)}$ a ďalšie sú $\ell t_0, \ell = 1, 2, \dots, \gcd(e-1, p-1)$ a s pomocou CRT

Dôkaz:

- ▶ Rovnosť $x^e = x \bmod (pq)$ je podľa CRT ekvivalentná s sústavou $x^e = x \bmod p$ a $x^e = x \bmod q$.
- ▶ Rovnica $x^e = x \bmod p$ má jedno triviálne riešenie $x = 0$, a potom riešenia $x^{e-1} = 1 \bmod p$.
- ▶ V grupe Z_p^* je $x = g^t$, kde g je generátor, preto riešime $g^{t(e-1)} = 1 \bmod p$.
- ▶ Jedno riešenie je $t_0 = \frac{p-1}{\gcd(e-1, p-1)}$ a ďalšie sú $\ell t_0, \ell = 1, 2, \dots, \gcd(e-1, p-1)$ a s pomocou CRT
- ▶ $[1 + \gcd(e-1, p-1)][1 + \gcd(e-1, q-1)]$.

4. *Iterované šifrovanie* $E(E \dots E(x) \dots) = E^h(x)$ a z rovnosti $E^{h+1}(x) = E(x) \bmod n$ určíme pôvodnú správu x , $E^h(x) = x \bmod n$ bez faktorizácie modulu. Navyše, z poslednej rovnosti môžeme aj faktorizovať modul.

4. *Iterované šifrovanie* $E(E \dots E(x)) \dots) = E^h(x)$ a z rovnosti $E^{h+1}(x) = E(x) \bmod n$ určíme pôvodnú správu x , $E^h(x) = x \bmod n$ bez faktorizácie modulu. Navyše, z poslednej rovnosti môžeme aj faktorizovať modul.

Ide o riešenie rovnice $x^{e^{h+1}} = x^e \bmod (pq)$. Preto počet správ, ktoré môžeme dešifrovať s cyklom h je

$$[1 + \gcd(e^h - 1, p - 1)][1 + \gcd(e^h - 1, q - 1)].$$

5. Častá je voľba $e = 3$ resp. $e = 2^{16} + 1$. Vo všeobecnosti ide o tzv. *krátke exponenty* $e = 2^k + 1$. Ak volíme náhodne prvočísla, potom asi 3% z nich sú také, že vyhovujú pre ľubovoľný krátky exponent $1 \leq k \leq 1023$.

5. Častá je voľba $e = 3$ resp. $e = 2^{16} + 1$. Vo všeobecnosti ide o tzv. *krátke exponenty* $e = 2^k + 1$. Ak volíme náhodne prvočísla, potom asi 3% z nich sú také, že vyhovujú pre ľubovoľný krátky exponent $1 \leq k \leq 1023$.
6. Pri malom e je možný útok *príbuznými správami*. (1996)

VSTUP: $e = 3, n = pq, (x_1, x_2 \equiv \alpha x_1 + \beta \pmod{n}),$

$$\begin{aligned} y_1 &= x_1^3 \pmod{n} \\ y_2 &= x_2^3 \pmod{n}. \end{aligned}$$

VÝSTUP: $x_1 = \frac{\beta(y_2 + 2\alpha^3 y_1 - \beta^3)}{\alpha(y_2 - \alpha^3 y_1 + 2\beta^3)} \pmod{n}$

7. Útok pri spoločnom n a nesúdeliteľných e_1, e_2 (Simmons):
Rovnaká správa sa pošle 2 účastníkom

$$y_1 = x^{e_1} \pmod{n}$$

$$y_2 = x^{e_2} \pmod{n}$$

Z EA existujú $\alpha, \beta, \alpha e_1 + \beta e_2 = 1$

$$x = x^{\alpha e_1 + \beta e_2} = y_1^\alpha y_2^\beta \pmod{n}$$

8. Útok pri spoločnom a malom $e = 3$, (1986), (predpokladáme nesúdeliteľnosť n_i):

$$\begin{aligned}y_1 &= x^e \pmod{n_1} \\y_2 &= x^e \pmod{n_2} \\y_3 &= x^e \pmod{n_3}\end{aligned}$$

a odtiaľ ($n = n_1 n_2 n_3$)

$$x^e(n_1 n_2 + n_1 n_3 + n_2 n_3) = y_3 n_1 n_2 + y_2 n_1 n_3 + y_1 n_2 n_3 \pmod{n}$$

8. Útok reťazovými zlomkami (1990) Hlavný trik:

$$\begin{aligned}ed &= k(p-1)(q-1) + 1 \\ \frac{e}{n} &= \frac{k}{d}(1 - \delta), \quad \text{kde } \delta = \frac{p+q-1-1/k}{n}\end{aligned}$$

Ak δ je malé, potom existuje technika, známa z reťazových zlomkov, ako z hodnoty $\frac{e}{n}$ nájsť $\frac{k}{d}$...

Odtiaľ podmienka: $p < q < 2p$, resp.

$$|n - \varphi(n)| = \dots = |p + q - 1| < 3\sqrt{n}.$$

Systémy s verejným kľúčom

RSA algoritmus

Výpočtové problémy pri použití RSA-algoritmu

Faktorizácia modulu

Rabinov algoritmus

Goldwasser-Micaliho algoritmus

Paillierov algoritmus

Hľadanie vhodných prvočísel

Je dosť veľa prvočísel?

Hľadanie náhodného prvočísla

Rýchle dešifrovanie

Voľba šifrovacieho exponentu

Navyše $e = 3, d = \frac{1+2(p-1)(q-1)}{3}$

Navyše $e = 3$, $d = \frac{1+2(p-1)(q-1)}{3}$

interval pre d ...

$$\frac{1+2n}{3} - d < 2^{1+0.5 \log_2 n}$$

Faktorizácia modulu

1. Je ekvivalentná so znalosťou $\varphi(n)$. Platí

$$\varphi(n) = (p-1)(q-1) = n + 1 - p - q,$$

a teda p, q sú riešením kvadratickej rovnice ...

2. Je ekvivalentná so znalosťou $\lambda(n)$. Platí

$$\frac{n}{\lambda(n)} - 2 < \gcd(p-1, q-1) < \frac{n}{\lambda(n)}$$

odkiaľ

$$\varphi(n) = \gcd(p-1, q-1)\lambda(p-1, q-1).$$

3. Je ekvivalentná so znalosťou dešifrovacieho exponentu d . Nech x je netriviálne riešenie $x^2 = 1 \pmod{n}$. Potom $n \mid (x+1)(x-1)$ a zároveň n nedelí žiadny z faktorov $x \pm 1$. preto $\gcd(x+1, n) = p$ alebo q . Tak dostávame Las Vegas algoritmus na faktorizáciu n , ak máme k dispozícii nejaký algoritmus A na výpočet d pre daný vstup e .

Let $w \in Z_n$, $x = \gcd(w, n)$

If $x > 1$ then $x = p$.

Else

$d = A(e)$, $ed - 1 = 2^s r$, r -nepárne.

For $i = 0$ upto s :

If $w^{2^i r} = \pm 1 \pmod{n}$ then quit.

Else

$x = \gcd(w^{2^i r} + 1, n) = p$

EndFor.

Pozn. $ed - 1 = 2^s r = 0 \pmod{\varphi(n)}$, $w^{\varphi(n)} = 1 \pmod{n}$.

3. Fermat (1643):

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

$$x = 1 + \lfloor \sqrt{n} \rfloor, 2 + \lfloor \sqrt{n} \rfloor, \dots$$

počítaj

$$y = \sqrt{x^2 - n}. \quad (1)$$

Ak je to celé číslo, potom $x - y = p$.

Vhodné, len ak je $|p - q|$ malé.

4. **Kraitchik (1920):** namiesto hľadania rozkladu $n = x^2 - y^2$, hľadal rozklad $kn = x^2 - y^2$, resp.

$$x^2 = y^2 \pmod{n}. \quad (2)$$

Ak n je nepárne a má aspoň dvoch prvočíselných deliteľov, potom aspoň polovica riešení je taká, že $x \not\equiv \pm y \pmod{n}$ a $\gcd(xy, n) = 1$. Potom $\gcd(x - y, n)$ je netriviálny faktor n .

5. Príklad. $n = 2041 = 13 * 157$, $\lfloor \sqrt{n} \rfloor = 45$.

Fermat: $y_i = \sqrt{(i + 45)^2 - 2041}$, $i = 1, 2, \dots$. Pre $i = 40$ dostaneme $x_{40} = 85$, $y_{40} = 72$, $x_{40} - y_{40} = p = 13$.

Kraitchik: $u_i = (i + 45)^2 - 2041$, $i = 1, 2, \dots$. Pre $i \leq 6$ dostaneme $u_i = \underline{75}, \underline{168}, 263, \underline{360}, 459, \underline{560}$. Pretože $u_1 u_2 u_4 u_6 = y^2$, našli sme riešenie rovnice (2):

$$x = 46 * 47 * 49 * 51 \equiv 311 \pmod{2041}$$

$$y = \sqrt{75 * 168 * 360 * 560} \equiv 1416 \pmod{2041}$$

$$\gcd(311 - 1416, 2041) = 13.$$

Podstata Kraitchikovej metódy spočíva v nájdení podpostupnosti postupnosti $x_i^2 - n$ pre x_i z okolia $\sqrt{n}$, z ktorej sa dá vytvoriť štvorec čísla.

6. Brillhart – Morrison (1975): Podstata všetkých moderných faktorizačných metód - nájdenie podpostupnosti predchádzajúcej metódy.

Každé číslo $m = \prod p_i^{\nu_i}$.

Každé číslo m má vektor $\nu(m) = (\nu_1, \nu_2, \dots)$

V našom príklade je $\nu(75) = (0, 1, 2, 0)$, $\nu(168) =$

$(3, 1, 0, 1)$, $\nu(360) = (3, 2, 1, 0)$, $\nu(560) = (4, 0, 1, 1)$.

My hľadáme štvorce, tj. stačí redukovať súradnice (mod 2).

Presnejšie, hľadáme také čísla, aby súčet ich vektorov

(mod 2) bol nulový vektor. Ak to všetko uvažujeme nad

vektorovým priestorom Z_2^4 , tak hľadáme také 4 vektory, ktoré

sú lineárne závislé...

Faktorové bázy sa dajú vopred pripraviť. Dokonca je možné

tieto vektory klastrovať do podskupín - podstata internetových

metód na faktORIZÁCIU...

Systémy s verejným kľúčom
 RSA algoritmus
 Výpočtové problémy pri použití RSA-algoritmu
FaktORIZÁCIA modulu
 Rabinov algoritmus
 Goldwasser-Micaliho algoritmus
 Paillierov algoritmus

RSA je multiplikatívny homomorfizmus
 Útok s vybranými zašifrovanými textami na PKCS#1
 Útok s postranným kanálom
 Kvázilineárne hľadanie GCD

dec(RSA)	bit(RSA)	dátum	MIPS-roky
100	332	apríl 1991	7
110	365	apríl 1992	75
120	398	jún 1993	830
129	428	apríl 1994	*5000
130	431	apríl 1996	500
140*	465	február 1999	2000
155**	512	august 1999	8400
160	530	apríl 2003	
174	576	december 2003	13200
200***	663	máj 2005	
232	768	dec. 2009	

1 MIPS-rok = jednoročnej práci procesora, ktorý vykonáva 10^6 /sec inštrukcií = za rok 3×10^{13} inštrukcií.

*1600PC/ 8 mesiacov; **2000PC/7 mesiacov; ***RSA200:

Šifrovanie RSA-2048 bitov za 8 rokov (2005)

Hardvérové riešenia 1024bit:

Shamir	TWINKLE	2000	200M	1r
Shamir, Tromer	TWIRL	2003	10M	1r
Franke,...	SHARK	2005	70K	1r

Predpokladá sa, že 1024 bitový modul môže byť faktorizovaný s pomocou 2^{80} operácií, a preto sila RSA 1024 je porovnávaná s 80-bitovou Vernamovou šifrou.

RSA je multiplikatívny homomorfizmus

1. $E(x_1 x_2) = E(x_1) E(x_2)$
2. Chosen ciphertext attack: Chceme dešifrovať $c = m^e \bmod n$. Požiadame o dešifrovanie $c_0 = cx^e \bmod n$. Dostaneme $c_0^d = c^d x^{ed} = mx = m_0 \bmod n \dots$
3. meet-in-the middle: $m = m_1 m_2, c = m^e \bmod n$. Vytvor tabuľku $(m'_1)^e \bmod n$, a pre všetky $((m'_2)^e)^{-1}$ porovnaj $c((m'_2)^e)^{-1}$ s tabuľkou. Ak nájdeš zhodu, potom $m'_2 = m_2$ a $c((m_2)^e)^{-1} = (m_1)^e \bmod n$ bude v tabuľke, $\rightarrow m_1 \dots$ úspešnosť 18%.

PKCS#1

Ak nekompetentná osoba má prístup ku oraculu tak, že toto mu odpovie, či zaslané $y^d \pmod n$ má, alebo nemá PKCS#1 formát, potom je schopná čítať, resp. podpisovať správy.

00	02	vložený reťazec PS	00	blok dát D
----	----	----------------------	----	--------------

Veľkosť n je k bytov, $2^{8(k-1)} \leq n \leq 2^{8k}$, $|PS| = k - 3 - |D|$ bytov,
 $|D| \leq k - 11$ bytov.

Samotný útok je založený na dvoch faktoch:

1. Podobne, ako pri metóde clonenia, môže NO čítať správu takto: zmení pôvodnú správu y na $y' \equiv yr^e \pmod{n}$ a snaží sa zachytiť $x' \equiv xr \pmod{n}$...

Samotný útok je založený na dvoch faktoch:

1. Podobne, ako pri metóde clonenia, môže NO čítať správu takto: zmení pôvodnú správu y na $y' \equiv yr^e \pmod{n}$ a snaží sa zachytiť $x' \equiv xr \pmod{n}$...
2. Algoritmus, kde oraculum zistí, či vyslaná správa má príslušný formát, alebo nie.

Postup pri dešifrovaní správy $E_e(x) = y$ je nasledovný:

1. Zvoľ číslo r a pošli správu $y' = yr^e \pmod{n}$.
2. Ak oraculum (server adresáta) oznámi (akceptuje), že správa má PKCS formát, potom nekompetentná osoba vie, že prvé dva byty správy mr sú 00 a 02. Navyše

$$2^{8(k-2)+1} \leq mr \pmod{n} < 32^{8(k-2)}.$$

3. Opakovaním vhodnej voľby r je možné tento interval zmenšovať približne na polovicu.

Zložitosť tohoto útoku je odhadnutá na 2^{20} .

Systémy s verejným kľúčom
RSA algoritmus
Výpočtové problémy pri použití RSA-algoritmu
Faktorizácia modulu
Rabinov algoritmus
Goldwasser-Micaliho algoritmus
Paillierov algoritmus

RSA je multiplikatívny homomorfizmus
Útok s vybranými zašifrovanými textami na PKCS#1
Útok s postranným kanálom
Kvázilineárne hľadanie GCD

Útok s postranným kanálom

1. už sme jeden mali pri monitorovaní umocňovania...
2. útok na implementáciu Open PGP, kedy sa "podstrčia" odosielateľovi slabé prvočísla. Podobne je to možné urobiť pre certifikovaný EP...
3. akustický, uzemňovací kolík,...

Systémy s verejným kľúčom

RSA algoritmus

Výpočtové problémy pri použití RSA-algoritmu

Faktorizácia modulu

Rabinov algoritmus

Goldwasser-Micaliho algoritmus

Paillierov algoritmus

RSA je multiplikatívny homomorfizmus

Útok s vybranými zašifrovanými textami na PKCS#1

Útok s postranným kanálom

Kvázilineárne hľadanie GCD

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Systémy s verejným kľúčom
RSA algoritmus
Výpočtové problémy pri použití RSA-algoritmu
FaktORIZÁCIA modulu
Rabinov algoritmus
Goldwasser-Micaliho algoritmus
Paillierov algoritmus

RSA je multiplikatívny homomorfizmus
Útok s vybranými zašifrovanými textami na PKCS#1
Útok s postranným kanálom
Kvázilineárne hľadanie GCD

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Dôkaz:

1. $\gcd(N_1, N_2, \dots, N_m) = g$

Systémy s verejným kľúčom
RSA algoritmus
Výpočtové problémy pri použití RSA-algoritmu
Faktorizácia modulu
Rabinov algoritmus
Goldwasser-Micaliho algoritmus
Paillierov algoritmus

RSA je multiplikatívny homomorfizmus
Útok s vybranými zašifrovanými textami na PKCS#1
Útok s postranným kanálom
Kvázilineárne hľadanie GCD

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Dôkaz:

1. $\gcd(N_1, N_2, \dots, N_m) = g$
2. $\gcd(N_1^2, N_1, N_2, \dots, N_m) = g \cdot N_1$

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Dôkaz:

1. $\gcd(N_1, N_2, \dots, N_m) = g$
2. $\gcd(N_1^2, N_1, N_2, \dots, N_m) = g \cdot N_1$
3. $\forall x \in \mathbb{Z} \quad \gcd(N_1^2, N_1, N_2, \dots, N_m + xN_1^2) = gN_1$

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Dôkaz:

1. $\gcd(N_1, N_2, \dots, N_m) = g$
2. $\gcd(N_1^2, N_1, N_2, \dots, N_m) = g \cdot N_1$
3. $\forall x \in \mathbb{Z} \quad \gcd(N_1^2, N_1, N_2, \dots, N_m + xN_1^2) = gN_1$
4. $\gcd(N_1^2, N_1, N_2, \dots, N_m \bmod N_1^2) = g \cdot N_1$

Kvázilineárne hľadanie GCD

Lemma:

$$\gcd(N_1, N_2, \dots, N_m) = \gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right)$$

Dôkaz:

1. $\gcd(N_1, N_2, \dots, N_m) = g$
2. $\gcd(N_1^2, N_1, N_2, \dots, N_m) = g \cdot N_1$
3. $\forall x \in \mathbb{Z} \quad \gcd(N_1^2, N_1, N_2, \dots, N_m + xN_1^2) = gN_1$
4. $\gcd(N_1^2, N_1, N_2, \dots, N_m \bmod N_1^2) = g \cdot N_1$
5. $\gcd\left(N_1, \frac{N_1 N_2 \dots N_m \bmod N_1^2}{N_1}\right) = g$

Systémy s verejným kľúčom

RSA algoritmus

Výpočtové problémy pri použití RSA-algoritmu

Faktorizácia modulu

Rabinov algoritmus

Goldwasser-Micaliho algoritmus

Paillierov algoritmus

RSA je multiplikatívny homomorfizmus

Útok s vybranými zašifrovanými textami na PKCS#1

Útok s postranným kanálom

Kvázilineárne hľadanie GCD

Strom súčinov množiny S je strom, kde množina S je na spodnom stupni. Pre všetky prvky stromu x , ktorého deti sú l a r platí:
 $x = l.r$

Obr.: Efektívny výpočet všetkých párov GCD

Využitie pri generovaní pseudonáhodných bitov.

- ▶ Vstupom je okrem parametrov RSA aj tajná hodnota y_0 .
- ▶ Generátor počíta hodnoty

$$y_{i+1} = (y_i^e \bmod n) \bmod 2.$$

- ▶ Výstupom je najnižší významový bit z každej iterácie.
- ▶ Tento generátor je tak bezpečný, ako samotné RSA a je ho možné používať už pri $e = 3$.

Rabinov algoritmus

1. Každý účastník siete zverejní tzv. **verejný** (šifrovací) kľúč $e = (n, B)$, kde $n = pq$ je súčinom dvoch veľkých Blumových prvočísel ($p \equiv q \equiv 3 \pmod{4}$) a $B \in Z_n$.
2. **Tajný** dešifrovací kľúč $d = (p, q)$, tj. oproti RSA sa nič nepočíta.
3. Otvorený text (správa) je $x \in Z_n$. Šifrovanie a dešifrovanie je dané vzťahmi
 - ▶ šifrovanie $E(x) \equiv x(x + B) \pmod{n}$
 - ▶ dešifrovanie $D(y) = \sqrt{\frac{B^2}{4} + y} - \frac{B}{2}$

1. Sila algoritmu spočíva vo výpočte odmocniny $(\text{mod } n)$ bez znalosti faktorizácie.

1. Sila algoritmu spočíva vo výpočte odmocniny $(\text{mod } n)$ bez znalosti faktorizácie.
2. Faktorizácia je ekvivalentná výpočtu odmocniny $(\text{mod } n)$.

1. Sila algoritmu spočíva vo výpočte odmocniny $(\text{mod } n)$ bez znalosti faktorizácie.
2. Faktorizácia je ekvivalentná výpočtu odmocniny $(\text{mod } n)$.
3. Rabinov algoritmus je dokázateľne odolný voči pasívnemu oponentovi za predpokladu, že faktorizácia je ťažký problém.

1. Sila algoritmu spočíva vo výpočte odmocniny $(\text{mod } n)$ bez znalosti faktorizácie.
2. Faktorizácia je ekvivalentná výpočtu odmocniny $(\text{mod } n)$.
3. Rabinov algoritmus je dokázateľne odolný voči pasívnemu oponentovi za predpokladu, že faktorizácia je ťažký problém.
4. Text musí obsahovať nejakú redundantnú informáciu... Takže prenosový pomer $R = \frac{1024}{1024-\ell}$.

Dešifrovanie je založené na nasledovných tvrdeniach:

1. Nech ω je ľubovoľné zo 4 riešení $x^2 \equiv 1 \pmod{n}$. Potom platí

$$E_e \left(\omega \left(x + \frac{B}{2} \right) - \frac{B}{2} \right) = E_e(x),$$

kde $1/2 = 2^{-1} \pmod{n}$. Takže pre každé $y \in Z_n$ existujú 4 možné správy: $x, -x - B, \pm \omega(x + B/2) - B/2$.

2. Dešifrovať správu znamená vyriešiť rovnicu

$$x^2 + Bx \equiv y \pmod{n}. \quad (3)$$

Legitímny príjemca ju vyrieši v dvoch krokoch

- Najprv zavedie substitúciu $x_1 = x + B/2$, čím prevedie (3) na

$$x_1^2 \equiv \frac{B^2}{4} + y \equiv C \pmod{n}.$$

- Tým sa úloha redukuje na riešenie sústavy kongruencií

$$C_p^2 \equiv C \pmod{p}, \quad C_q^2 \equiv C \pmod{q}.$$

To je v prípade Blumových prvočísel jednoduché. Ak

$$C_p \equiv \pm C^{(p+1)/4} \pmod{p}, \quad C_q \equiv \pm C^{(q+1)/4} \pmod{q},$$

potom podľa čínskej zvyškovej vety nájde 4 riešenia

$$x_1^{(i)} \equiv C_p v q + C_q u p \pmod{n},$$

kde $u \equiv 1/p \pmod{q}$ a $v \equiv 1/q \pmod{p}$.

- Na záver vypočíta $x^{(i)} = x_1^{(i)} - B/2$ a vyberie zaslanú správu.

Nech $n = 77 (= 7 \times 11)$, $B = 9$ a správa je $y = 22$. Nájdeme správu x ako legitímny príjemca.

Nech $n = 77 (= 7 \times 11)$, $B = 9$ a správa je $y = 22$. Nájdeme správu x ako legitímny príjemca.

1. Každý môže vyrátať $1/2 \pmod{77} = 39$,
 $1/4 \pmod{77} = 58$, $x_1^2 = B^2/4 + y \equiv 23 \pmod{77}$.

Nech $n = 77 (= 7 \times 11)$, $B = 9$ a správa je $y = 22$. Nájdeme správu x ako legítimny príjemca.

1. Každý môže vyrátať $1/2 \pmod{77} = 39$,
 $1/4 \pmod{77} = 58$, $x_1^2 = B^2/4 + y \equiv 23 \pmod{77}$.
2. Ďalší postup je možný len pre legítimneho príjemcu. Nájdeme 2 odmocniny z $23 \pmod{7}$ a 2 odmocniny z $23 \pmod{11}$:

$$C_7^2 \equiv 23 \pmod{7}, \quad C_7 \equiv 23^{(7+1)/4} \equiv \pm 4 \pmod{7}$$

$$C_{11}^2 \equiv 23 \pmod{11}, \quad C_{11} \equiv 23^{(11+1)/4} \equiv \pm 1 \pmod{11}$$

Nech $n = 77 (= 7 \times 11)$, $B = 9$ a správa je $y = 22$. Nájdeme správu x ako legítimny príjemca.

1. Každý môže vyrátať $1/2 \pmod{77} = 39$,
 $1/4 \pmod{77} = 58$, $x_1^2 = B^2/4 + y \equiv 23 \pmod{77}$.
2. Ďalší postup je možný len pre legítimneho príjemcu. Nájdeme 2 odmocniny z $23 \pmod{7}$ a 2 odmocniny z $23 \pmod{11}$:

$$C_7^2 \equiv 23 \pmod{7}, \quad C_7 \equiv 23^{(7+1)/4} \equiv \pm 4 \pmod{7}$$

$$C_{11}^2 \equiv 23 \pmod{11}, \quad C_{11} \equiv 23^{(11+1)/4} \equiv \pm 1 \pmod{11}$$

3. $u \equiv 1/7 \equiv 8 \pmod{11}$, $v \equiv 1/11 \equiv 2 \pmod{7}$,

$$x_1^{(i)} \equiv C_p v q + C_q u p \equiv \pm 10, \pm 32 \pmod{77}$$

Nech $n = 77 (= 7 \times 11)$, $B = 9$ a správa je $y = 22$. Nájdeme správu x ako legítimny príjemca.

1. Každý môže vyrátať $1/2 \pmod{77} = 39$,
 $1/4 \pmod{77} = 58$, $x_1^2 = B^2/4 + y \equiv 23 \pmod{77}$.
2. Ďalší postup je možný len pre legítimneho príjemcu. Nájdeme 2 odmocniny z $23 \pmod{7}$ a 2 odmocniny z $23 \pmod{11}$:

$$C_7^2 \equiv 23 \pmod{7}, \quad C_7 \equiv 23^{(7+1)/4} \equiv \pm 4 \pmod{7}$$

$$C_{11}^2 \equiv 23 \pmod{11}, \quad C_{11} \equiv 23^{(11+1)/4} \equiv \pm 1 \pmod{11}$$

3. $u \equiv 1/7 \equiv 8 \pmod{11}$, $v \equiv 1/11 \equiv 2 \pmod{7}$,

$$x_1^{(i)} \equiv C_p v q + C_q u p \equiv \pm 10, \pm 32 \pmod{77}$$

4. $x \equiv x_1^{(i)} - B/2 \pmod{77}$. Možné správy: $x = 44, 24, 66, 2$.

Goldwasser-Micaliho algoritmus

Definícia algoritmu.

1. Účastník si zvolí $p, q, n = pq$ a w tak aby
 $J(\frac{w}{n}) = 1, L(\frac{w}{p}) = L(\frac{w}{q}) = -1$
2. (n, w) je VK.
3. Šifrovanie binárnej správy $x_1, x_2, \dots$ kde u_i je náhodne zvolené číslo

$$y_i = w^{x_i} u_i^2 \bmod n.$$

4. Dešifrovanie binárnej správy $y_1, y_2, \dots$. Ak $L(\frac{y_i}{p}) = 1$, potom $x_i = 0$ inak $x_i = 1$
5. Prenosový pomer $R = 1/\log_2 n \dots$

Paillierov algoritmus

Zjednodušená verzia

1. platí: $|Z_{n^2}^*| = \varphi(n^2) = n\varphi(n)$, $\lambda(n^2) = n\lambda(n)$, $c \in Z_{n^2}^*$, $c^{\lambda(n)} = 1 \bmod n$, $c^{n\lambda(n)} = 1 \bmod n^2$, $(n+1)^m = 1 + mn \bmod n^2$,
 $(n+1)^{mn} = 1 \bmod n^2$
2. $n = pq$, $\gcd(pq, \varphi(pq)) = 1$, $g = n+1$, $\mu = \varphi(pq)^{-1} \bmod n$.
3. šifrovanie VK = (n, g) :
 - ▶ $m \in Z_n$, $r \in Z_n^*$
 - ▶ $c = g^m r^n \bmod n^2 \in Z_{n^2}^*$
4. dešifrovanie SK = $\varphi(pq)$:
5. $L(u) = \frac{u-1}{n}$
6. $m = L(c^{\varphi(n)} \bmod n^2) \mu \bmod n$

Aditívne homomorfný kryptosystém: $E(m_1 + m_2) = E(m_1)E(m_2)$

vhodný pre voľby, prahové schémy, watermarking,