VOLUME-3, ISSUE-6

RSA ALGORITMINING OCHIQ KALITI YORDAMIDA MAXFIY KALITINI ANIQLASH ALGORITMI

Jomg'irova N.A.,
Musurmonqulova M.M
Termiz davlat universiteti Axborot texnologiyalari fakulkteti 2-kurs talabalari

Annotatsiya. Mazkur maqolada asimmetrik shifrlash algoritmlar turkumiga kiruvchi RSA shifrlash algoritmining ochiq kaliti yordamida maxfiy kalitini aniqlash algoritmi taklif qilingan. Taklif qilingan algoritmning samaradorligi (a, b) oraliqni imkoni boricha kichik oraliqlarga ajratish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlash murakkabligiga bog'liq. Mazkur algoritm shu kungacha ma'lum bo'lgan ko'pgina algoritmlardan samaradorligi bo'yicha ajralib turadi.
Kalit so'zlar. RSA, Eyler funksiyasi, matematik murakkablik, tub sonlar, faktorizatsiya

Kirish: Faktorlash muammosini hal etishda n modulni faktorlash masalasini yechishda birinchi navbatda hayolga keladigan usul, bu $\sqrt{n}$ dan oshmaydigan tub sonlarni tanlab ularga bo'lib ko'rishdir. Boshqa tanlash usuli Fermaga tegishli bo'lib, n ni kvadratlar ayirmasi ko'rinishida ifodalashga asoslangan [1,2]:

$$n = a^2 - b^2 = (a + b)(a - b).$$

Ferma eng katta umumiy bo'luvchi - $EKUB(n, a - b)$ ni, ya'ni n ning natural bo'luvchisini topishga harakat qilishni hamda bunga imkon beruvchi usulni ham taklif etgan. Agar n ning ko'paytuvchilari bir-biridan katta farq qilmasa, bu usul oddiy tanlash usuliga nisbatan tez yechim beradi va uning murakkabligi $O(\sqrt{n})$ ko'rinishida ifodalanadi, ammo hozirgi kunda kriptografik tizimlarda amalda foydalaniladigan hollar uchun ahamiyatga ega emas. Lejandr mazkur yondashuvda
$a^2 \equiv b^2 \ (mod\ n)$ ga ega bo'lish lozimligiga e'tibor qaratgan. Ammo, keltirilgan taqqoslama har qanday n uchun yetarli emasligini ham ko'rsatgan va ko'zlangan maqsadga erishish uchun uzluksiz kasrlardan foydalanish yo'lini taklif etgan.
RSA shifrlash algoritmi va uning murakkabligi bo'yicha ko'plab tadqiqot ishlari olib borilgan [1-10].

Asosiy qism

RSA shifrlash algoritmida ikkita p va q tub sonlardan foydalaniladi. $n = p * q$, $\varphi(n) = (p - 1) * (q - 1)$ Eyler funksiyasi hisoblanadi. $EKUB(d, \varphi(n)) = 1$ (1) shartni qanoatlantiruvchi e soni va $e * d = 1\ mod\ \varphi(n)$ (2) shartni qanoatlantiruvchi d soni hisoblanadi.
$(2, \varphi(n))$ oraliqda (1) shartni qanoatlantiruvchi bir qancha e sonlar va aniqlangan e sonlar bilan birgalikda (2) shartni qanoatlantiruvchi shuncha d sonlar mavjud.
$C = M^e\ mod\ n$ ifoda bilan M ochiq ma'lumotni shifrlash jarayoni amalga oshirilsa, $M = C^d\ mod\ n$ ifoda bilan esa shifrmatndan ochiq ma'lumotni hosil qilish jarayoni amalga oshiriladi.
Teorema. Har qanday (a, b) intervalda tanlab olingan p va q tub sonlar va ularning ko'paytmasi n soni uchun uchun quyidagi tenglik o'rinli:

$$\varphi(n) = 2 \cdot (\left[\frac{n}{2}\right] - \left[\sqrt{n}\right] - r) \qquad (3)$$

bu yerda $r \in [\frac{2\cdot(\left[\frac{n''}{2}\right]-[\sqrt{n''}])-\varphi''(n'')}{2}, \frac{2\cdot(\left[\frac{n'}{2}\right]-[\sqrt{n'}])-\varphi'(n')}{2}]$, $n' = p_{min}\cdot q_{max}$, $\varphi'(n') = (p_{min}-1)\cdot(q_{max}-1), n'' = p_{min}\cdot q_{min}$, $\varphi''(n'') = (p_{min}-1)\cdot(q_{min}-1)$ $p_{min}, p_{max}, q_{min}, q_{max}$ sonlar (a,b) intervaldagi eng kichik va eng katta qiymatlar.

Bizga 11 bitli ikkita p va q tub sonlarning ko‘paytmasi bo‘lgan $e = 17$ va $n = 3\ 202\ 751$ sonlari berilgan bo‘lsa (1) ifodaga $r \in [0{,}85]$ intervaldagi sonlarni ketma-ket qo‘yib chiqish va $m^e\ mod\ n = m^{e+\varphi(n)}\ mod\ n$ tenglikni qanoatlantirishini tekshirish orqali $\varphi(n)$ sonini aniqlash mumkin. Bu esa sonni faktorlashda keng tarqalgan usul $\sqrt{n} = 1789$ gacha bo‘lish amalidan ancha samarali hisoblanadi.

Albatta mazkur usulni yanada optimallashtirish ham mumkin. Buning uchun quyidagi amallar bajarish zarur. $t = \frac{p_{min}+q_{max}}{2}$ sonni aniqlab olinadi va $t^2 = (\frac{p_{min}+q_{max}}{2})^2$ ifoda hisoblanadi. Bizning holatimizda $p_{min} = 1031$, $q_{max} = 2039$ sonlari uchun $t^2 = (\frac{p_{min}+q_{max}}{2})^2 = (\frac{1031+2039}{2})^2 = 1490^2 = 2\ 220\ 100$ soni bilan n soni solishtiriladi agar mazkur aniqlangan natija n sonidan katta bo‘lsa n bo‘luvchilari bo‘luvchilari bo‘lgan p va q tub sonlarning hech bo‘lmaganda bittasi aniqlangan 1490 sondan kichik ekanligini, agar kichik bo’lsa p va q sonlar bu sondan katta ekanligini bildiradi. Bizning holatimizda $n > t^2$ $(3\ 202\ 751 > 2\ 220\ 100)$ ekanligidan izlanayotgan p va q sonlarimiz uchun $p > 1490$ va $q > 1490$ shartlar o‘rinli ekan. (3) ifodadan r ning maksimal qiymatini hisoblash amalga oshirilsa bu qiymat 21 ga teng ekanligini aniqlash mumkin. Demak, Bizga 11 bitli ikkita p va q tub sonlarning ko‘paytmasi bo‘lgan $n = 3\ 202\ 751$ soni berilgan bo‘lsa (3) ifodaga $r \in [0{,}21]$ intervaldagi sonlarni ketma-ket qo‘yib chiqish va aniqlangan $\varphi(n)$ sonining $m^e\ mod\ n = m^{e+\varphi(n)}\ mod\ n$ tenglikni qanoatlantirishini tekshirish yetarli ekan.

Natijalar va muhokamasi

RSA shifrlash algoritmida berilgan ochiq kalit e va $n = p * q$ sonlari yordamida $p, q \in (a,b)$ $\varphi(n) = (p-1)*(q-1)$ $(p, q \in (a,b))$ maxfiy kalitni aniqlash algoritmining umumiy tavsifi quyida keltirilgan.

1. (a,b) intervalni kichik qismlarga ajratiladi;
2. p, q sonlari ajratilgan qismlarning qaysi biriga tegishli bo‘lishi mumkinligi aniqlanadi;
3. 2-qadamda aniqlangan qismlar uchun $r \in [\frac{2\cdot(\left[\frac{n''}{2}\right]-[\sqrt{n''}])-\varphi''(n'')}{2}, \frac{2\cdot(\left[\frac{n'}{2}\right]-[\sqrt{n'}])-\varphi'(n')}{2}]$, $n' = p_{min}\cdot q_{max}$, $\varphi'(n') = (p_{min}-1)\cdot(q_{max}-1), n'' = p_{min}\cdot q_{min}$, $\varphi''(n'') = (p_{min}-1)\cdot(q_{min}-1)$ p_{min}, q_{max} oraliqlar hisoblanadi;
4. r ning 3 – qadamda aniqlangan oraliqdagi qiymatlari yordamida hisoblangan $\varphi(n) = 2\cdot(\left[\frac{n}{2}\right] - \left[\sqrt{n}\right] - r)$ uchun $m^e\ mod\ n = m^{e+\varphi(n)}\ mod\ n$ tenglik o‘rinli bo‘lsa hisoblashlar to‘xtatiladi;
5. 4-qadamdagi tenglikni qanaoatlantiruvchi $\varphi(n)$ izlanayotgan maxfiy kalit sifatida e’lon qilinadi.

Algoritmning samaradorligi (a,b) oraliqni imkoni boricha kichik oraliqlarga ajratish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlashga bog‘liq.

Quyidagi 1-9 rasmlarda r sonining $p-q$, n, $\varphi(n)$ sonlariga bog’liqligi bo’yicha tadqiqot natijalari keltirilgan ((256, 512) oraliqdagi tub sonlar misolida).

Ushbu rasmlardagi bog’liqliklardan r sonining qiymati n va $\varphi(n)$ sonlariga nisbatan $p-q$ ayirmaning qiymatiga bevosita bo’g’ligini ko‘rish mumkin.

(a, b) oraliqni kichik oraliqlarga bo‘lish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlashning optimal usuli aniqlansa, yuqorida keltirilgan algoritmning samaradorligi anchagina ortadi.

Xulosa

Mazkur maqolada RSA shifrlash algoritmida ochiq kalitlar yordamida maxfiy kalitni aniqlashning yangi algoritmi taklif qilingan. Taklif qilingan algoritmning samaradorligi (a, b) oraliqni imkoni boricha kichik oraliqlarga ajratish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlash murakkabligiga bog‘liq. (a, b) oraliqni kichik oraliqlarga bo‘lishning va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlashning optimal usuli aniqlansa, yoki r sonining n soniga bog‘liqligi aniqlansa mazkur algoritmning samaradorligi anchagina ortadi.

Foydalanilgan adabiyotlar

1. Talbot, John and Dominic Welsh. Complexity and Cryptography. Cambridge: Cambridge University Press, 2006.
2. Rothe, Jörg. Complexity Theory and Cryptology. Berlin: Springer, 2005.
3. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
5. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.