PARAMETRLI ALGEBRA ASOSIDA YARATILGAN NOSIMMETRIK SHIFRLASH ALGORITMINING TAHLILI

Qarshiboyev Nizomiddin Abdumalik o‘g‘li
JizPI “ICHJA va B” kafedrasi, v.b., dotsent
Email: wolkswagen1991@gmail.com

Annotatsiya*: Parametrli funksiyaning tamoyilli xossalari safida quyidagilarni sanab o‘tish mumkin. Xossa. Parametri R≥1 bo‘lgan har qanday parametrli funksiya uchun, agar R bilan p_1, p_2 o‘zaro tub bo‘lib, modul nqp, $nqp_1 p_2$ bo‘lsa, unda Eyler pi-funksiyasi φ(n) qiymati mos tarzda p-1, $(p_1-1)(p_2-1)$ larga teng va Eyler pi-funksiyasi qo‘llanildi.*

Kalit so‘zlar*: Murakkab modul RSA kriptotizimi, shaxsiy kalit, parametr, diskret lagorifm, dastlabki matn, shifr matn, shifrlash, deshifrlash, identifikatsiya, autentifikatsiya.*

Аннотация: *Среди основных свойств параметрической функции можно назвать следующие. Свойство. Для любой параметрической функции с параметром R≥1, если R простое с p1, p2 и по модулю nqp, nqp1 p2, то пи-функция Эйлера φ(n) соответственно равна p- 1, равна (p1-1)(p2 -1) и использовалась пи-функция Эйлера.*

Ключевые слова: *Комплексно-модульная криптосистема RSA, закрытый ключ, параметр, дискретный логарифм, открытый текст, зашифрованный текст, шифрование, дешифрование, идентификация, аутентификация.*

Abstract: *Among the principle properties of a parameter function, the following can be listed. Property. For any parametric function with parameter R≥1, if R is prime to p1, p2 and modulo nqp, nqp1 p2, then the Euler pi-function φ(n) is correspondingly p- 1, equal to (p1-1)(p2-1) and the Euler pi-function was used.*

Keywords: *Complex modulus RSA cryptosystem, private key, parameter, discrete logarithm, plaintext, ciphertext, encryption, decryption, identification, authentication.*

-Modul nqp_1p_2 bo‘lib, agar R bilan faqat p_2 o‘zaro tub bo‘lsa, unda Eyler pi-funksiyasi $\varphi(n)$ qiymati $p_1(p_2-1)$ ga teng;

-agar R bilan faqat p_1 o‘zaro tub bo‘lsa, unda Eyler pi-funksiyasi $\varphi(n)$ qiymati $p_2(p_1-1)$ ga teng.

Xossa. $Ra^{g'x} \ (mod\ n) \equiv (1QRa)^x - 1 \ (mod\ n)$.

Xossa. Agar $y \equiv a^{g'x} (modn)$, n – tub (p) yoki murakkab modul , $n>a, x \geq 1$, $Rq\ \varphi(p)$ yoki q bo‘lsa, unda daraja ko‘rsatkichi: $xqyA^{-1} \ (mod\ R)$, bu yerda $AqaQkn$, $a \in \{1, 2,..., n-1\}$, $k \in \{0, 1, 2,..., n-1\}$, $q>x$.

Mazkur xossa asosida diskret logarifmlash va RSA kriptotizimida shaxsiy kalit x ni topish masalalari asos A ni topishga keltiriladi.[4]

Xossa. Agar n – tub yoki murakkab modul, $n>a, x \geq 1$, $x < Rq2^i$ bo‘lsa, unda $y \equiv a^{g'x} (mod\ n)$ ga mos shunday $Y\ qyQbn$ mavjudki, $x \equiv \pm Y \ (modR)$, bu yerda $b \in \{0, 1, 2, ..., R-1\}$.

Mazkur xossa asosida diskret logarifm va faktorlash masalalari b ni topishga keltiriladi.[5]

Parametrli funksiyaning ayrim xossalari asosida o‘xshashi yo‘q quyidagi shifrlarni tuzish mumkin. *Xossa.* Agar d, e $\varphi(p)$ bilan o‘zaro tub bo‘lib, $\varphi(p)$ moduli bo‘yicha o‘zaro teskari juftlik bo‘lsa, unda $(a^{g'd})^{g'e} \equiv a \ (mod\ p)$, bu yerda $a \in \{1,2,..., n-1\}$, g' - parametr R bilan darajaga oshirish ramzi, $R > aQ2^{160}$;

Misol:

oshkora parametr $(pq107, eq37, dq43)$

1-tomon: kalit $(Rq7)$, dastlabki matn $aq4$,

Shifrmatn $(sh \equiv 4^{g'43} \ (mod\ 107) q19)$,

2-tomon: kalit $(Rq7)$,

dastlabki matn $a \equiv 19^{g'37} \ (mod\ 107) q4$.

Xossa. Agar $R_1 \neq R_2 < n$, d_1, d_2 va e_1, e_2 mos tarzda $\varphi(n)$ bilan o‘zaro tub bo‘lib, $\varphi(n)$ moduli bo‘yicha o‘zaro teskari juftlik bo‘lsa, unda $(a^{g'd1})^{g'g'd2} \equiv sh \ (mod\ n)$, $(sh^{g'g'e2})^{g'e1} \equiv a \ (mod\ n)$, bu yerda $a, sh \in \{1,2,..., n-1\}$, d_1, d_2, $e_1, e_2 \in \{1,2,..., \varphi(n) -1\}$,

g' - parametr R_1 bilan darajaga oshirish ramzi, $g'g'$ - parametr R_2 bilan darajaga oshirish ramzi, $R_i > aQ2^{160}{}_i$, $iq1,2$.

Misol:

oshkora parametr $(nq107, e_1\ q67, e_2\ q11, d_1 q19, d_2 q29)$.

1-tomon: kalit $(R_1 q17, R_2 q37)$, dastlabki matn $aq3$, shifrmatn $(sh \equiv (a^{g'd1})^{g'g'd2} \ (mod\ 107) q38)$,

2-tomon: kalit $(R_1 q17, R_2 q37)$, dastlabki matn $a \equiv (sh^{g'g'e2})^{g'e1} \ (mod\ 107) q3$.

Xossa. Agar $n \in \{p, p_1 p_2\}$ – modul, $n > a \geq 1$, $R > d > 1$, $1 < R \leq \varphi(n)$, $y \equiv a^{g'd} \ (mod\ n)$, $y_1 \equiv a^{g'd-1} \ (mod\ n)$, (ay_1) bilan n o‘zaro tub, $R > aQ2^{160}$ bo‘lsa, unda $R \equiv (y - y_1 - a)(ay_1)^{-1} \ (mod\ n) \rightarrow a \equiv (y - y_1)(1QRy_1)^{-1} \ (mod\ n)$.

Misol:

oshkora parametr $nq107$.

1-tomon: kalit *(Rq51, d q23)*, dastlabki matn *aq5*, shifrmatn *($y \equiv a^{g'd} \pmod n$)q57*, *($y_1 \equiv a^{g'd-1} \pmod n$)q42);*

2-tomon: qismkalit *(Rq51)*, dastlabki matn *$a \equiv (57 - 42)*(1Q51*42)^{-1} \pmod n$)q5*.

Xossa. Ro‘yxatga olish Markazi (ROM)ning yagona RSA kriptotizimi analogidan va simmetrik kalit sifatida parametrdan foydalangan holda har bir mushtariy uchun himoyalangan axborot almashish kanali yaratish imkoniyati mavjudligi.

ROM bilan mushtariy orasida himoyalangan axborot almashish kanali yaratish uchun ROMda ham, har bir mushtariyda ham alohida RSA tizimi mavjud bo‘lishi lozim. Agar RSA tizimini loyihalash mushkulliklarini ehtiborga olinsa, yuqorida keltirilgan xossaning ahamiyati ulkanligi ayon bo‘ladi.[6]

EECh tenglamasidan parametrli EECh (PEECh) tenglamasiga o‘tish.

Xossa. Agar *$y^{g'2} \equiv x^{g'3} QaxQB \pmod p$* va *$y_0^2 \equiv x_0^3 Qax_0Qb \pmod p$* lar o‘zaro izomorf bo‘lsa, u holda *$B \equiv (aQb)\ R^{-1} \pmod p$*, *$y \equiv (y_0\text{-}1)\ R^{-1} \pmod p) \equiv (x^{g'3} QaxQB)^{g'0.5} \pmod p$*, *$y - \equiv -(y_0Q1)\ R^{-1} \pmod p) \equiv - (yQ2R^{-1}) \pmod p$*, *$y^{g'2} \equiv (y_0^2\text{-}1)\ R^{-1} \pmod p$*, *$x \equiv (x_0\text{-}1)\ R^{-1} \pmod p$*, *$x^{g'3} \equiv (x_0^3\text{-}1)\ R^{-1} \pmod p$*).[7]

Parametrli EECh nuqtasining chekli additiv gruppa elementiga mosligi.

Xossa. Agar *$y^{g'2} \equiv x^{g'3} QaxQB \pmod p$) PEECh* taqqoslamasi bo‘lib, *Yq(x,y)qd*$^{g'}$G* nuqta shu taqqoslamani qanoatlantirsa, u holda *PEECh* nuqtasi *x*-, *y*- koordinatalariga chekli *q* tartibli additiv gruppa *(GF(p);”Q”)* ning elementlari *$xq\ d*g_1 \pmod q$*, *$y\ q\ d*g_2 \pmod q$* o‘zaro mos keladi, bu yerda “*$^{g'}$” - parametrli ko‘paytirish, ”Q” - qo‘shish, ”*” - ko‘paytirish amallari ramzlari, *Gq(g_1, g_2)*.

PEECh nuqtasining chekli *q* tartibli additiv gruppa elementiga mosligi xossasidan foydalanish *EECh*larda diskret logarifmlash masalasini chekli additiv gruppaning bazis elementini topish asosida hal etishga yo‘l ochadi.[6]

Parametrli algebra amallari xususiyatlari mavjud murakkabliklarni kompozitsiyalari negizida takomillashgan yangi nosimmetrik algoritmlar yaratish imkoniyatlarini beradi.

Xulosa: O‘zbekiston davlat standartlarini ishlab chiqishga asos bo‘lgan parametrli funksiya amallari keltirilgan. Parametrli algebraik strukturalar va ularning yangi algoritmlarni ishlab chiqishdagi o‘rni o‘rganildi.

1. Parametrli funksiyaning ayrim xossalari tadqiq etildi. Parametrli funksiyalarning chekli gruppa va halqada diskret darajaga oshirish funksiyasi xossalariga o‘xshash xossalari tahlil etildi.

2. Parametrli algebra asosida yaratilgan nosimmetrik shifrlash algoritmining tahlili keltirildi. Parametrli algebra amallari xususiyatlari mavjud murakkabliklarni kompozitsiyalari negizida takomillashgan yangi nosimmetrik algoritmlar yaratish imkoniyatlarini berishi yoritildi.

Foydalanilgan adabiyotlar ro‘yxati

1. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. “O‘zbekiston markasi “, 2009. - 432 b.

2. O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari».

5. Брюс Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ - Москва: ТРИУМФ, 2002.

3. Тавбоев С. А., Каршибоев Н. А. МЕТОДЫ УЛУЧШЕНИЯ КОНТРАСТА ИЗОБРАЖЕНИЙ ПРИ НЕЧЕТКОЙ ИСХОДНОЙ ИНФОРМАЦИИ //Экономика и социум. – 2021. – №. 3-2. – С. 427-432.

4. Tovbaev Sirojiddin Karshiboev Nizomiddin International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

5. Tavboyev Sirojiddin Akbutayevich, Qarshiboyev Nizomiiddin Abdumalikovch Application of the theory of indistinct sets in the estimation of quality of educational process // Journal of Critical Reviews ISSN-2394-5125 Vol 7, Issue 12.2020

6. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). Image contour separation algorithms based on the theory of fuzzy sets. International Journal of Contemporary Scientific and Technical Research, 120-125.

7. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). Tasvirlardan ma’lumot olishda matlab muhitining intellektual tashkil etuvchilaridan foydalanish. International Journal of Contemporary Scientific and Technical Research, 247-250.

8. Akhbutayevich, T. S., & Abdumalikovich, K. N. (2022). Algorithms for Selecting the Contour Lines of Images Based on the Theory of Fuzzy Sets. Texas Journal of Engineering and Technology, 15, 31-40.

9. Савурбаев, А. Дангалов, Н.А., Шертойлоков, Г.М., & Эшонкулов, Ш.У. (2014). Алгоритм расчета переходного процесса при ударе цилиндрического