ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

ELEKTRON RAQAMLI IMZO ALGORITMLARINING QIYOSIY TAHLILI (RSA, ELGAMAL, DSA)

Yuldash Abdullayevich Kuralov
Toshkent viloyati Chirchiq davlat pedagogika instituti o‘qituvchisi
ykuralov89@mail.ru

ANNOTATSIYA

Mazkur ish kriptografiyaning muhim vazifalaridan biri - elektron raqamli imzoga bag’ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o’rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta’minlovchi oddiy imzoning analogidir. Ushbu ishda RSA, ElGamal va DSA algoritmlarining afzalliklari va kamchiliklari qarab chiqilgan

Kalit so‘zlar: shifrlash algoritmlari, elektron raqamli imzo, RSA, ElGamal, DSA.

COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE ALGORITHMS (RSA, ELGAMAL, DSA)

ABSTRACT

This paper deals with one of the most important tasks of cryptography - the electronic digital signature. Electronic digital signature (EDS) is needed to uniquely establish the author of any document. EDS is the analog of a common signature that authenticates any document or contract. In this paper we look at the advantages and disadvantages of the algorithms RSA, ElGamal and DSA.

Keywords: encryption algorithms, electronic digital signature, RSA, ElGamal,DSA.

KIRISH

So’nggi vaqtlarda axborot texnologiyalari kundalik hayotimizga kirib, muhim hukumat loyihalaridan tortib oddiy maishiy muammolarni yechishni ham qamrab olmoqda. Yangi texnologiyalar cheksiz imkoniyatlar va kata foyda keltirishi bilan birgalikda yangi muammolarni ham paydo qilmoqda. Ulardan biri axborotni olishi mumkin bo’lmagan shaxslar qo’liga tushishidan himoyalash muammosidir.

Axborotni himoyalashning ko’plab usullari mavjud, shunday bo’lsada ularni har birini quyidagi ikki usuldan biriga keltirishimiz mumkin: axborotni raqiblardan jidmoniy himoyalash va axborotni shifrlash.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

Mazkur ish kriptografiyaning muhim vazifalaridan biri – elektron raqamli imzoga bag'ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o'rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta'minlovchi oddiy imzoning analogidir[1]. Elektron raqamli imzo quyidagilarni amalga oshirish imkonini beradi:

– Yaxlitlik nazorati;
– Hujjatni o'zgartirishlardan (soxtalashtirish) himoyalash;
– Mualliflikni inkor etish imkoniyatini yo'q qilish;
– Hujjatning muallifligini isbotlab tasdiqlash.

ERI ning ushbu xususiyatlari uni yuridik qiymatga ega elektron hujjat aylanishini tashkil etishda qo'llaniladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Elektron raqamli imzo qurish sxemalari

Raqamli imzo qurishning bir necha sxemalari bor:

– Simmetrik shirfrlash algoritmi asosida. Ushbu sxema tizimda ikkala tomon ishonchidan foydalanuvchi uchinchi shaxs – arbitr borligini qaraydi. Hujjatni mualliflashtirish yopiq kalit bilan shifrlash va uni arbitrga jo'natishdan iborat.

– Assimmetrik shifrlash algoritm asosida. Hozirgi vaqtda ERI ning bunday sxemalari nisbatan ko'p tarqalgan va keng qo'llanilmoqda.

Bundan tashqari, yuqoridagi sxemalarning modifikatsiyasi bo'lgan raqamli imzoning boshqa usullari bor.

Yetarlicha kata hajmli hujjatlarni imzolashda ERI hujjatning o'ziga emas, balki uning heshiga qo'yiladi. Ixtiyoriy uzunlikdagi kiruvchi massiv berilganlarini fiksirlangan uzunlikdagi bit satrga hesh deyiladi.

Hesh-funksiyalardan foydalanish quyidagi imkoniyatlarni yaratadi:

– Hisoblashdagi qiyinchiliklarni kamaytiradi;
– Moslik bilan bog'liq muammolar yo'qligi;
– Berilganlar yaxlitligini tekshirish imkoniyati.

Simmetrik sxema.

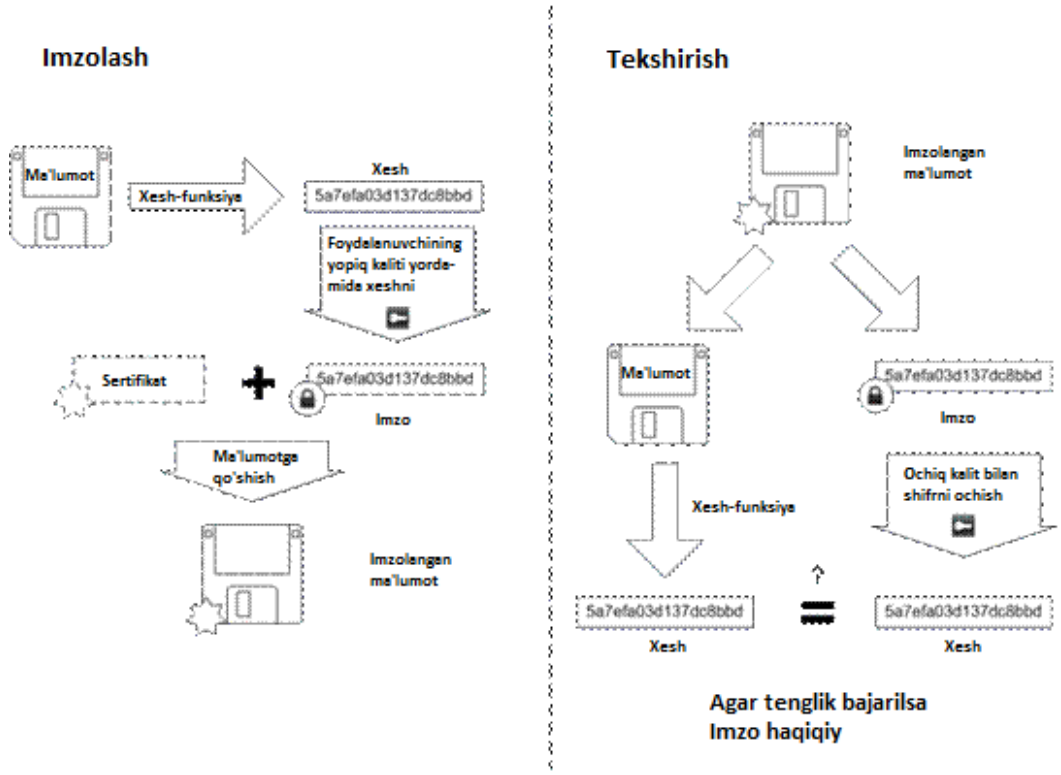
Simeetri ERI lar asimmetriklariga nisbatan kam tarqalgan, chunki raqamli imzo konsepsiyasi paydo bo'lgandan so'ng, o'sha vaqtlarda ma'lum bo'lgan simmetrik shifrlarga asosan imzoning effektiv algoritmlarini shakllantirib bo'lmadi. Raqamli imzoning asimmetrik sxemalari, hisoblash qiyin bo'lgan, isbotlanmagan masalalarga asoslanadi va shuning uchun yaqin yillarda ushbu sxemalarni buzish mumkin yoki yo'qligini aytib bo'lmaydi. Bundan tashqari, kriptobardoshlilikni oshirish uchun kalitlar

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

uzunligini oshirish kerak, bu esa ba’zan asimmetrik sxema dasturini qayta yozishga, ba’zida esa qurilmalarni qayta loyihalash zaruriyatini keltirib chiqaradi[2]. Simmetrik sxemalar keng o’rganilgan blokli shifrlarga asoslangan.

Asimmetrik sxema.

ERI ning asimmetrik sxemalari ochiq kalitli kriptotizimlar turiga kiradi. Raqamli imzo sxemalarida imzolash yopiq kalitni qo’llash orqali, tekshirish esa – ochiq kalit yordamida amalga oshiriladi.



1-rasm. Xesh-funksiya qo’llash orqali imzolash va uni tekshirish sxemasi

Umumiy qabul qilingan raqamli imzo sxemasi uch jarayonni o’z ichiga oladi:

– Kalit juftligini tanlash. Kalitni tanlash algoritmi yordamida yopiq kalit tanlanadi, keyin esa unga mos ochiq kalit hisoblanadi;

– Imzoni shakllantirish. Berilgan electron hujjat uchun yopiq kalit yordamida imzo hisoblanadi;

– Imzoni tekshirish. Ochiq kalit yordamida hujjat berilganlari va imzoning haqiqiyligi tekshiriladi.

NATIJALAR

ERI ning keng tarqalgan algoritmlari tahlili

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

Kalitlar juftligini (yopiq va ochiq) hosil qilish uchun ERI algoritmlarida bir yo'nalishli funksiyalarga asoslangan turli matematik sxemalardan foydalaniladi. Bu sxemalar ikki guruhga ajratiladi. Ushbu ajratishning asosida ma'lum murakkab hisoblanadigan masalalar yotadi:

– katta butun sonlarni faktorialini hisoblash maslasi;
– diskret logarifmlash masalasi.

RSA (Rivest, Shamir va Adleman familiyalarining bosh harflaridan olingan)

Birinchi va dunyoda mashhur muayyan ERI tizimi bu AQSh Massachuset texnologiya institutida 1977 yilda matematik sxemasi ishlab chiqilgan RSA tizimidir. Algoritmning ishonchliligi kata sonlarni faktorialini hisoblash murakkabligiga asoslangan[4].

RSA ning ochiq va yopiq kalitlarini hosil qilish algoritmi

Amalning ta'rifi	Misol
Ixtiyoriy p va q tub sonlar tanlanadi	p=11, q=7
Ularning moduli n=p*q hisoblanadi	n=11*7=77
Quyidagi formula bo'yicha Eyler funksiyasining n dagi qiymati hisoblanadi: $\varphi(n)=(p-1)(q-1)$	$\varphi(n)=(11-1)*(7-1)=60$
$\varphi(n)$ qiymati bilan o'zaro tub bo'lgan $e(1<e<\varphi(n))$ butun soni tanlanadi. Odatda e sifatida tub son tanlanadi.	$1<7<60$ $e=7$
Quyidagi shartni qanoatlantiruvchi d soni tanlanadi: $de\equiv 1(\mathrm{mod}\,\varphi(n))$. d soni e soniga $\varphi(n)$ modul bo'yicha multiplikativ teskaridir.	$7*d\equiv 1 \mathrm{mod}\ 60$ $d=43$
(e) ochiq kalit hisoblanadi. $P=(e,n)$ to'plam e'lon qilinadi.	(7,77)
(d) yopiq kalit vazifasini bajaradi va maxfiy saqlanadi.	(43)

Habarni raqamli imzolash algoritmi

Faraz qilaylik, A tomon B tomonga raqamli imzolangan pt=15 habarni jo'natishi kerak bo'lsin.

Jo'natuvchi algoritmi

Amal ta'rifi	Misol
Dastlabki matn pt olinadi	$pt=15$

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

$S, \sigma = pt^d \bmod n$ to'plam yordamida σ raqamli imzoni hosil qilinadi	$S = (43,77)$ $\sigma(15) = 15^{42} \bmod 77 = 64$
Habar va imzo juftligini (pt, σ) jo'natiladi	$(15,64)$

Qabul qiluvchi algoritmi

Amal ta'rifi	Misol
(pt, σ) juftlik qabul qilinadi	$(15,64)$
A tomonning P ochiq to'plami olinadi	$P = (7,77)$
Imzoning haqiqiyligi tekshiriladi: $\sigma^e \bmod n \equiv pt \rightarrow imzo\ haqiqiy$	$64^7 \bmod 77 = 15 = 15 \rightarrow imzo\ haqiqiy$

MUHOKAMA

Raqamli imzo RSA ning kamchiliklari

– Raqamli imzo tizimi RSA uchun n modul, e va d kalitlarni hisoblashda amalda bajarish qiyin bo'lgan katta sondagi qo'shimcha shartlarni tekshirish zaruriyati tug'iladi. Ushbu shartlardan ixtiyoriy birining bajarilmasligi, ushbu kamchilikni aniqlagan tomonidan raqamli imzoning soxtalashtirilishiga olib keladi[5].

– RSA raqamli imzoning soxtalashtirilishiga kriptobardoshliligini ta'minlash uchun hisoblashga katta xarajatlar talab qiladi (masalan, AQSh milliy shifrlash standarti (DES algoritmi) darajasida ya'ni 1018 bo'lishi uchun, n, d va e ni hisoblashda har biri uchun 2512 dan kam bo'lmagan butun sonlardan foydalanish kerak), bu esa boshqa algoritmlar yordamida xuddi shu darajadagi kriptobardoshli raqamli imzoni yaratishga ketuvchi xarajatdan 20-30% ko'pdir.

– Raqamli imzo RSA multiplikativ hujumlar bilan bog'liq. Boshqacha aytganda, RSA raqamli imzo algoritmi buzg'unchiga d yopiq kalitni bilmagan holda avval imzolangan hujjatlar xeshlarining ko'paytmasini hisoblagan holda imzoni aniqlash imkonini beradi.

ElGamal (El-Gamal sxemasi)

Shaxsiy kompyuterlarda hosil qilinishi qulay va nisbatan ishonchliroq ERI algoritmi 1984 yili arab millatiga mansub amerikalik Tohir El Gamal tomonidan ishlab chiqilgan va ElGamalSignatureAlgorithm(EGSA) nomini olgan.

EGSA ning g'oyasi katta butun sonni ko'paytuvchilarga ajratishdan ko'ra hisoblanishi qiyinroq masala diskret logarifmlash masalasida ERI ni soxtalashtirishning amaliy imkoni yo'qligiga asoslangan. Bundan tashqari, ElGamal RSA ERI

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

algoritmining oshkor kamchiligi yopiq kalitni bilmagan holda ba'zi xabarlaryordamida ERI ni soxtalashtirish bilan bog'liq kamchilikni bartaraf eta olgan[3].

ElGamal ochiq va yopiq kalitlarini hosil qilish algoritmi

Amal ta'rifi	Misol
Tasodifiy p tub son tanlanadi	$p = 23$
p modul bo'yicha ildiz bo'lgan ixtiyoriy butun g soni tanlanadi.	$g = 5$
$1 < x < p$ ni qanoatlantiruvchi tasodifiy x butun son tanlanadi	$x = 7$
$y = g^x \bmod p$ hisoblanadi	$y = 5^7 \bmod 23 = 17$
(p, g, y) uchligi ochiq to'plam bo'ladi	$(23,5,17)$
(x) yopiq kalit vazifasini bajaradi va maxfiy saqlanadi.	(7)

Habarni raqamli imzolash algoritmi

Faraz qilaylik, A tomon B tomonga raqamli imzolangan pt=15 habarni jo'natishi kerak bo'lsin.

Jo'natuvchi algoritmi

Amal ta'rifi	Misol
Dastlabki matn pt olinadi	$pt = 15$
$p-1$ bilan o'zaro tub bo'lgan tasodifiy $1 < k < p-1$ son tanlanadi	$k = 5$
$r = g^k \bmod p$ hisoblanadi	$r = 5^5 \bmod 23 = 20$
Kengaytirilgan Evklid algoritmi yordamida quyidagi shartni qanoatlantiruvchi s hisoblanadi: $pt = (x*r + k*s) \bmod p-1$	$15 = (1*20 + 5*s) \bmod 22$ $s = 19$
Habar va imzo juftligini (r, s) jo'natiladi	$(20,19)$

Qabul qiluvchi algoritmi

Amal ta'rifi	Misol
(r, s) juftlik qabul qilinadi	$(20,19)$
Quyidagi shartlar bajarilishi tekshiriladi:	Quyidagi shartlar bajarilsa keying qadamga o'tamiz $0 < 20 < 23$ va

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

$0 < r < p$ va $0 < s < p-1$. Agarda ushbu shartlardan hech bo'lmaganda bittasi bajarilmasa imzo soxta hisoblanadi.	$0 < 19 < 22$.
Quyidagi taqqoslama bajarilsa, imzo haqiqiy hisoblanadi $y^r \cdot r^s \equiv g^m \bmod p$	Chap tomonini 23 modul bo'yicha hisoblaymiz: $17^{20} \cdot 20^{19} \bmod 23 = 19$ O'ng tomonini 23 modul bo'yicha hisoblaymiz: $15^8 \bmod 23 = 19$

El Gamal raqamli imzo sxemasi RSA raqamli imzo sxemasiga nisbatan bir qator afzalliklarga ega:

1) Belgilangan bardoshlilik darajasidagi raqamli imzo algoritmida hisoblashlarda qatnashadigan butun sonlar 25% ga kam va bu hisoblashni deyarli ikki barobarga kamaytiradi.

2) p modulni tanlagan vaqtda uning tub ekanligini va p-1 ko'p sondagi tub ko'paytuvchilari borligini tekshirish yetarli.

3) El Gamal sxemasi bo'yicha imzoni shakllantirish protsedurasi yopiq kalitni bilmagan holda habarlar yordamida raqamli imzoni hisoblashga (RSA dagi kabi) yo'l qo'ymaydi.

Biroq, raqamli imzo algoritmi El Gamal ham RSA raqamli imzo sxemasi bilan taqqoslaganda ba'zi kamchiliklarga ega. Xususan, raqamli imzo uzunligi 1,5 barobar kata bo'ladi, bu esa uni hisoblashga ko'proq vaqt talab qiladi[4].

DSA (DigitalSignatureAlgorithm) – raqamli imzolash algoritmi (DSA) 1991 yili AQSh standart raqamli imzo DSS(DigitalSignatureStandart) da foydalanish uchun taklif qilingan. DSA algoritmi ERI EGSA ning rivojlantirilganidir. ERI EGSA bilan taqqoslaganda DSA algortimi bir qancha afzalliklarga ega: xotira hajmi va hisoblashlar vaqti qisqartirilgan. Imzolash va tekshirishda katta sonli modul bo'yicha bo'lish zaruriyati va bu amalning murakkabligi mazkur algoritmning kamchiligidir.

Habarni raqamli imzolash algoritmi

Faraz qilaylik, A tomon B tomonga raqamli imzolangan pt=15 habarni jo'natishi kerak bo'lsin.

DSA ochiq va yopiq kalitlarini hosil qilish algoritmi

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

Amal ta'rifi	Misol
$H(x)$ – xesh-funksiya hisoblanadi. Algoritmdan foydalanish uchun imzolanuvchi habar raqamlardan iborat bo'lishi kerak	Bizning holatda pt habar 15, xesh-funksiyadan foydalanish shart emas.
Bitlardagi o'lchami xesh-funksiya $H(x)$ yoki habarning bitlardagi o'lchamiga teng bo'lgan q tub son tanlanadi .	$q = 13$
Shunday p tub soni tanlanadiki, $p-1$ soni q ga bo'linadi	$p = 27$
p modul bo'yicha multiplikativ tartibi q ga teng g soni tanlanadi. Uni hisoblash uchun $g = h^{(p-1)/q} \bmod p$ formuladan foydalanish mumkin, bu yerda $h-$ ixtiyoriy son, $h \in (1; p-1)$, $g \neq 1$.	$h = 2$ $g = 2^{\frac{26}{13}} \bmod 27 =$
$x \in (0, q)$ shartni qanoatlantiruvchi x yopiq kalit tanlanadi. (x) maxfiy saqlanadi.	$x = 8; 8 \in (0,13)$
$y = g^x \bmod p$ formula bo'yicha ochiq kalit hisoblanadi. (p, q, g, y) to'plam jo'natiladi.	$y = 4^8 \bmod 27$

Jo'natuvchi algoritmi

Amal ta'rifi	Misol
Tasodifiy $k \in (0, q)$ soni tanlanadi	$k = 3$
$r = (g^k \bmod p) \bmod q$ hisoblanadi	$r = (4^3 \bmod 27) \bmod 13 = 10 \bmod 13 = 10$
$s = (k^{-1}(H(m) + xr)) \bmod q$ hisoblanadi	$s = (3^{-1}(15 + 8*10)) \bmod 13 = (8*4) \bmod 13 =$ $= 32 \bmod 13 = 6$
Agar $r = 0$ yoki $s = 0$ bo'lsa boshqa k tanlanadi.	$r \neq 0$, $s \neq 0$
(r, s) sonlar juftligi imzo bo'ladi	$(10,6)$

Qabul qiluvchi algoritmi

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

Amal ta'rifi	Misol
$\omega = s^{-1} \bmod q$ hisoblanadi	$\omega = 6^{-1} \bmod 13 = 11$
$\mu_1 = (pt * \omega) \bmod q$ hisoblanadi	$\mu_1 = (15 * 11) \bmod 13 = (2 * 11) \bmod 13$ $= 22 \bmod 13 = 9$
$\mu_2 = (r * \omega) \bmod q$ hisoblanadi	$\mu_2 = (10 * 11) \bmod 13 = 110 \bmod 13 = 6$
$\gamma = ((g^{\mu_1} * y^{\mu_2}) \bmod p) \bmod q$ hisoblanadi. Agar $\gamma = r$ bo'lsa, imzo haqiqiy.	$\gamma = ((4^9 * 7^6) \bmod 27) \bmod 13 =$ $= (1 * 10 \bmod 27) \bmod 13 = 10$ $10 = 10$ – imzo haqiqiy.

Raqamli imzo El Gamal bilan taqqoslaganda, DSA algoritmi quyidagi afzalliklarga ega:

1) Bardoshlilikning ixtiyoriy darajasida, ya'ni ixtiyoriy g va p sonlar juftligi (512 dan 1024 gacha), q,x,r,s sonlari 160 bit uzunlikka ega va imzo uzunligini 320 bitgacha qisqartiradi.

2) Imzoni hisoblash vaqtida K,r,s,x sonlari bilan bajariladigan ko'plab amallar uzunligi 160 bit bo'lgan q modul bo'yicha hisoblanadi va sarflanadigan vaqt qisqaradi.

3) Imzoni tekshirish jarayonida μ_1, μ_2, γ , ω sonlari bilan ham ko'plab amallar uzunligi 160 bit bo'lgan q modul bo'yicha hisoblanadi va sarflanadigan vaqt hamda xotira hajmini qisqaradi.

XULOSA

DSA algoritmining kamchiligi shundan iboratki, imzolashda va imzoni tekshirishda q modul bo'yicha bo'lish amali qiyinchilik tug'diradi va maksimal tezlikda ishlash imkoniyati yo'qotiladi.

ERI algoritmlari taqqoslash

Algoritm	Kalit uzunligi	Imkoniyati	Algoritmlar tahlili
RSA	4096 bitgacha	Shifrlash va imzolash	Katta sonlari faktorialini hisoblashning qiyinligiga asoslangan; dastlabki asimmetrik algoritmlardan biri. Ko'plab standartlar tarkibiga kiritilgan.
ElGamal	4096 bitgacha	Shifrlash va imzolash	Chekli maydonda diskret logarifmni hisoblash masalasining qiyinligiga asoslangan; bardoshlilikni kamaytirmagan holda kalitlarni qisqa vaqtda hosil qilish imkonini beradi. DSA elektron raqamli imzo algoritmining DSS standartida

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

			qo'llaniladi.
DSA	1024 bitgacha	Faqat imzolash	Chekli maydonda diskret logariflash masalasining qiyinligiga asoslangan; AQSh ning milliy standarti sifatida qabul qilingan; maxfiy va maxfiy bo'lmagan aloqalar uchun qo'llaniladi; AMB tomonidan ishlab chiqilgan.

REFERENCES

1. Kuralov, Y. A., (2020). Development Of Geometric Creativity Of Secondary Scholl Students By Computer. International Journal of Scientific & Technology Research - (IJSTR) Volume-9 Issue-2, February 2020 Edition, 4572-4576.
2. Kuralov, Y. A., Makhmudova, D. M., (2020). METHODOLOGY OF DEVELOPING CREATIVE COMPETENCE IN STUDENTS WITH PROBLEMATIC EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol. 8 No. 4, 2020, Part IIISSN 2056-5852, 142-146.
3. Akhmedov, B. A., Majidov, J. M., Narimbetova, Z. A., Kuralov, Yu. A. (2020). Active interactive and distance forms of the cluster method of learning in development of higher education. Экономика и социум, 12(79), 805-808.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М., 2002 – 816 с.
6. Жўраева, Н. В., Султанов, Р. О., Абдуллаева, С. А., Рахимжонова, В. А. (2020). Systematization of word combinations in the uzbek language. Наука и Мир, 2(6), 65-68.
7. Sultanov R. O., Yusupov M. R. (2020). Ta'limda matematika fanini o'qitishdagi muammolar va ularning yechimida axborot kommunikatsiya texnologiyalarining ahamiyati. O`zMU xabarlari, 2(1/2/1), 144-147.
8. Султанов, Р. О. (2020). Idea блокли шифрлаш алгоритмини такомиллаштириш методлари. Academic Research in Educational Sciences, 1(3), 397-404.
9. Kamolov, E. R., Raximov, S. M., Sultanov, R. O., Maxmudov, M.A., (2021). Innovative method of developing creative thinking of students. Экономика и социум, 1(80).
10. Хуррамов, А. Ж., Комолов, Э. Р., Разработка алгоритма управления с

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-00907

учетом трудноформализуемой информации // Academic research in educational sciences, (2020). Volume 01, Issue 03, -pp: 240-247.

11. Khurramov, A. J., Makhmudova, D. M., Improvement of Technique of Designing and Teaching Learning Process in the course “Methods of Teaching Mathematics”. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019. Volume-9 Issue-2, pp: 5244-5249.
12. Хуррамов, А. Ж., Ражабов, О. Т., Ядгарова, Н. Н., Умумий ўрта таълим мактабларида математика фанини ўқитишда таълим технологияси инновацион моделининг ўрни. Academic research in educational sciences, 2021. Volume 2 special issue 2, pp: 59-67.
13. Боймуродов, А. Х. Таълим жараёнида ахборот технологиялари ва интерфаол методлар интеграцияси. Academic research in educational sciences, 2021. volume 2 ISSUE 3, pp: 406-412.