www.wordlyknowledge.uz Volume: 2, Issue: 2, 2023

DSA ERI standarti. ГОСТ Р 34.10-94 elektron raqamli imzosi

Sharopova Muxayyo Muxtor qizi
Osiyo Xalqaro Universiteti
“Umumtexnik fanlar” kafedrasi o’qituvchisi
muxayyosharopova4@gmail.com

ANNOTATSIYA: Ushbu maqolada elektron raqamli imzo haqida tushunchalar va undan foydalanishdan ko’zlangan asosiy maqsadlar ko’rsatilgan.Bundan tashqari elektron imzoning asosini tashkil qilgan fan “Kriptografiya ” fani haqida hamda bu fanning dastlabki shifrlash algoritmlari keltirilgan , ularga doir misollar ko’rsatib o’tilgan. DSA va ГОСТ Р 34.10-94 shifrlash algoritmiga asoslangan elektron raqamli imzo tavsiflangan.

Kalit so’zlar: shifrlash **,** DES, ГОСТ Р 34.10-94

ANNOTATION: In this article, the concepts of electronic digital signature and the main goals of its use are shown. In addition, the science "Cryptography", which forms the basis of electronic signature, and the initial encryption algorithms of this science are given, and examples of them are shown. An electronic digital signature based on DSA and GOST R 34.10-94 encryption algorithm is described.

Key words: shifrlash,RSA ,El-Gamal, Cryptography

Kirish:1991 yilda NIST (National Institute of Standard and Technology) tomonidan DSA (Digital Signature Algorithm) algoritmiga asoslangan DSS (Digital Signature Standard) ERI standartining loyihasi muhokamaga qo‘yildi. Ushbu algoritm bardoshliligi yetarli katta tub xarakteristikaga ega bo‘lgan chekli maydonda diskret logarifmlash masalasining murakkabligiga asoslangan Quyida algoritm qadamlari ketma-ketligi keltirilgan.

Imzoni shakllantirish

1. Ma’lumot jo‘natuvchi M -ma’lumotni va quyidagi parametrlarni keng doiradagi tizim foydalanuvchilariga ochiq e’lon qiladi:

p – tub son, $2^{512} < p < 2^{1024}$, bit uzunligi 64 ga karrali;

q - tub son, $2^{159} < q < 2^{160}$, p-1 ning bo‘luvchisi;

$g = h^{(p-1)/q} \bmod p$, bu yerda h ushbu $0 < h < p$ va $h^{(p-1)/q} \bmod p > 1$ shartlarni qanoatlantiruvchi butun son;

y – ochiq kalit bo‘lib, $y = q^x \bmod p$ formula orqali aniqlanadi. Bu yerda x – maxfiy kalit bo‘lib, $0<x<q$ oraliqdan olingan va faqat imozolovchining o‘zigagina ma’lum;

$H(M)$ – M ma’lumotdan $[1;q]$ oraliqdagi butun sonni generatsiya qiluvchi xesh-funksiya.

2. Ma’lumot jo‘natuvchi $0<k < q$ oraliqdan tasodifiy k sonni tanlaydi, uni maxfiy tutadi va imzo generatsiyasidan keyin darhol yo‘qotadi.

3. Ma’lumot jo‘natuvchi r va s qiymatlarni quyidagi qonuniyat orqali hisoblaydi:

$$r = g^k \bmod p \bmod q,$$

$$s = k^{-1}(xr + H(M)) \bmod q.$$

www.wordlyknowledge.uz Volume: 2, Issue: 2, 2023

M - ma'lumotga qo'yilgan imzo (r, s) sonlar juftligidan iborat.

Imzoni tekshirish. Qabul qiluvchi M' ma'lumotni va (r', s') imzoni qabul qilib oladi. U M va M' ma'lumotlarning mos kelishini tekshirishi lozim. Buning uchun u quyidagi qadamlar ketma-ketligini bajaradi:

1. $0 < s' < q$ yoki $0 < r' < q$ shartlardan birortasi bajarilmasa, imzo qalbaki deb hisoblanadi va imzoni tekshirish tugatiladi.
2. $v = (s')^{-1} (mod\ q)$ topiladi.
3. $z_1 = H(M')\ v \bmod q,\ z_2 = r'\ v \bmod q$ hisoblanadi.
4. Keyin $u = g^{z_1} y^{z_2} \bmod p \bmod q$ hisoblanadi.
5. Agar $r' = u$ tenglik o'rinli bo'lsa, u holda imzo haqiqiy va $M = M'$ tenglik to'g'ri.

Algoritmning to'g'riligi. $M = M',\ s' = s$ va $r' = r$ bo'lsin. U holda $r = u$ tenglik o'rinli bo'lishi ko'rsatiladi.

Demak, $v = (s')^{-1} \bmod q,\ z_1 = H(M')\ v \bmod q,\ z_2 = r'\ v \bmod q$ ekanligidan, quyidagini yozish mumkin:

$$u = g^{z1}\ y^{z1} \bmod p \bmod q = g^{H(M)s-1}\ g^{xrs-1} \bmod p \bmod q =$$

$$= g^{k(xr+H(M))-1(xr+H(M))} \bmod p \bmod q = g^k \bmod p \bmod q = r.$$

Bundan ko'rish mumkinki, $r = u$ tenglik o'rinli. Shunday qilib, algoritm to'g'riligi isbotlandi.

ГОСТ Р 34.10-94 elektron raqamli imzosi

2000-yilgacha Rossiya standarti hisoblangan ГОСТ Р 34.10–94 ERI algoritmi qarab chiqiladi. Bu algoritm DSA algoritmiga o'xshash va quyidagi boshlang'ich ochiq parametrlardan foydalanadi:

1) Uzunligi L bo'lgan katta p tub son tanlanadi, bu yerda L son 509 bitdan 512 bitgacha yoki 1020 bitdan 1024 bitgacha oraliqdan tanlanadi, ya'ni $2^{509} < p < 2^{512}$ yoki $2^{1020} < p < 2^{1024}$.

2) Uzunligi L_1 bo'lgan katta q tub son tanlanadi, bu yerda L_1 son 254 bitdan 256 bitgacha oraliqdan tanlanadi, ya'ni $2^{254} < p < 2^{256}$.

3) $g^q \bmod p = 1$ shartni qanoatlantiruvchi $0 < g < p - 1$ oraliqdagi g son tanlanadi.

4) $y = g^x \bmod p$ dan y - ochiq kalit hisoblanadi, bu yerda $0 < x < q$ oraliqdan olingan x -maxfiy kalit.

5) $H(M)$ - xesh-funksiya berilgan M - ma'lumot bo'yicha hisoblangan butun son bo'lib, 1 dan q gacha oraliqdagi qiymatlarni qabul qiladi, ya'ni $1 < H(M) < q$.

Imzoni generatsiya qilish algoritmi. Boshlang'ich ma'lumotlar: M - ma'lumot, berilgan parametrlar va maxfiy kalit. Natija: imzo - (r, s).

1) 1 k q intervaldan tasodifiy k soni olinadi, u maxfiy saqlanadi va imzo qo'yilgandan keyin darhol yo'qotiladi.

www.wordlyknowledge.uz Volume: 2, Issue: 2, 2023

2) $r = (g^k \bmod p)(\bmod q)$ hisoblanadi.

3) Jo‘natilayotgan M - ma’lumotning $e := H(M)$ - xesh qiymati hisoblanadi.

4) Agar $r = 0$ yoki $H(M) \bmod q = 0$ bo‘lsa, u holda 1- qadamga o‘tilib, boshqa k tanlanadi.

5) $s = (xr + kH(M)) \bmod q$ hisoblanadi, bu yerda maxfiy kalit x faqat imzo qo‘yuvchining o‘zigagina ma’lum.

6) Agar $s = 0$ bo‘lsa, u holda 1-qadamga boriladi.

7) M ma’lumot imzosi - (r, s) juftligidan iborat.

Imzoni tekshirish algoritmi. Boshlang‘ich ma’lumotlar: M ma’lumot, berilgan parametrlar, imzoni tekshirish kaliti va M ma’lumot imzosi. Natija: imzo haqiqiyligi yoki qalbakiligi haqidagi tasdiq.

1) Agar 1 r, s $n-1$ shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi. Bu shartlar bajarilsa keyingi qadamga o‘tiladi.

2) $e := h(m)$ hisoblanadi.

3) $w := H(M)^{(q-2)} \bmod q$ hisoblanadi.

4) $u_1 := sw \bmod q$ hisoblanadi.

5) $u_2 := (q - r)w \bmod q$ hisoblanadi.

6) $u := (g^{u_1} y^{u_2} \bmod p)(\bmod q)$ hisoblanadi.

7) Agar $u = r$ shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.

ГОСТ Р 34.10-94 imzo algoritmining to‘g‘riligi. ГОСТ Р 34.10-94 elektron raqamli imzo generatsiyasi algoritmidan olingan r parametrning qsiymatini imzoni tekshirish algoritmidagi u parametr qiymati bilan tengligini ko‘rsatishimiz kerak.

Haqiqatan, $u = (g^{u_1} y^{u_2} \bmod p)(\bmod q) = g^{sw \bmod q} \cdot g^{x(q-r)w \bmod q} \bmod p \bmod q =$

$= g^{(s+xq-xr)w \bmod q} \bmod p \bmod q = g^{(xr+kH(M)+xq-xr)w \bmod q} \bmod p \bmod q =$

$= g^{(kH(M)+xq)w \bmod q} \bmod p \bmod q =$

$= g^{kH(M)w \bmod q} \bmod p \cdot (g^q \bmod p)^{xw \bmod q} (\bmod q) =$

$= /\ (g^q \bmod p) = 1$ shartga ko‘ra, $(g^q \bmod p)^{xw \bmod q} (\bmod q) = 1$ tenglik o‘rinli/=

$= g^{kH(M)w \bmod q} \bmod p\ (\bmod q) = /\ w = H(M)^{(q-2)} \bmod q$, $0 < H(M) < q$ (q –tub) shartga va Eylera – Ferma teoremasiga ko‘ra $H(M)^{(q-2)} \bmod q = H(M)^{-1}$ ekanligi kelib chiqadi, shunga ko‘ra g ning darajasini $kH(M)w = kH(M)H(M)^{q-2} \bmod q = kH(M)H(M)^{-1} = k$ kabi ifodalash mumkin / $= g^k \bmod p\ (\bmod q) = r$. Shunday qilib talab qilingan shart ko‘rsatildi.

Adabiyotlar ro’yxati

1. qizi Sharopova, M. M. (2023). RSA VA EL-GAMAL OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDA ELEKTRON RAQMLI IMZOLARI. RSA OCHIQ KALITLI

SHIFRLASH ALGORITMI ASOSIDAGI ELEKTRON RAQAMLI IMZO. *Educational Research in Universal Sciences*, *2*(10), 316-319.

2. Jalolov, T. S. (2023). PSIXOLOGIYA YO ‘NALISHIDA TAHSIL OLAYOTGAN TALABALARGA SPSS YORDAMIDA MATEMATIK USULLARNI O ‘RGATISHNING METODIK USULLARI. Educational Research in Universal Sciences, 2(10), 323-326.
3. Jalolov, T. S. (2023). PYTHON INSTRUMENTLARI BILAN KATTA MA’LUMOTLARNI QAYTA ISHLASH. Educational Research in Universal Sciences, 2(10), 320-322.
4. Sadriddinovich, J. T. (2023). Capabilities of SPSS Software in High Volume Data Processing Testing. American Journal of Public Diplomacy and International Studies (2993-2157), 1(9), 82-86.
5. Jalolov, T. S., & Usmonov, A. U. (2021). “AQLLI ISSIQXONA” BOSHQARISH TIZIMINI MODELLASHTIRISH VA TADQIQ QILISH. Экономика и социум, (9 (88)), 74-77.
6. Турсунов, Б. Ж., Гайбуллаев, С. А., & Жумаев, К. К. (2020). Влияние технологических параметров на гликолевую осушку газа. Sciences of Europe, (55-1 (55)), 33-36.
7. Турсунов, Б. Ж., & Алланазаров, Г. О. (2019). Перспективные технологии производства по улучшению качества бензина. Теория и практика современной науки, (3 (45)), 305-308.
8. Турсунов, Б. Д., & Суннатов, Ж. Б. (2017). Совершенствование технологии вторичного дробления безвзрывным методом. Молодой ученый, (13), 97-100.
9. Турсунов, Б. Ж., & Шомуродов, А. Ю. (2021). Перспективный метод утилизации отходов нефтеперерабатывающей промышленности. TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI, 1(6), 239-243.
10. Bakhodir, T., Bakhtiyor, G., & Makhfuza, O. (2021). Oil sludge and their impact on the environment. Universum: технические науки, (6-5 (87)), 69-71.
11. Турсунов, Б. Ж. (2021). АНАЛИЗ МЕТОДОВ УТИЛИЗАЦИИ ОТХОДОВ НЕФТЕПЕРЕРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ. Scientific progress, 2(4), 669-674.
12. Турсунов, Б. Ж., Ботиров, Т. В., Ташпулатов, Д. К., & Хайруллаев, Б. И. (2018). ПЕРСПЕКТИВА ПРИМЕНЕНИЯ ОПТИМАЛЬНОГО ПРОЦЕССА РУДООТДЕЛЕНИЯ В КАРЬЕРЕ МУРУНТАУ. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 160-164).
13. ТУРСУНОВ, Б., & ТАШПУЛАТОВ, Д. (2018). ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ПРЕДВАРИТЕЛЬНОГО ОБОГАЩЕНИЯ РУД В КАРЬЕРЕ КАЛЬМАКИР. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 165-168).
14. Турсунов, Б. Ж., Ботиров, Т. В., Ташпулатов, Д. К., & Хайруллаев, Б. И. (2018). ПЕРСПЕКТИВА ПРИМЕНЕНИЯ ОПТИМАЛЬНОГО ПРОЦЕССА РУДООТДЕЛЕНИЯ В КАРЬЕРЕ МУРУНТАУ. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 160-164).
15. Axmedova, Z. I. (2023). LMS TIZIMIDA INTERAKTIV ELEMENTLARNI YARATISH TEXNOLOGIYASI. Educational Research in Universal Sciences, 2(10), 368-372.
16. Jurakulov, S. Z. (2023). NUCLEAR ENERGY. *Educational Research in Universal Sciences*, *2*(10), 514-518.
17. Oghly, J. S. Z. (2023). PHYSICO-CHEMICAL PROPERTIES OF POLYMER COMPOSITES. *American Journal of Applied Science and Technology*, *3*(10), 25-33.

www.wordlyknowledge.uz Volume: 2, Issue: 2, 2023

18. Zafarjon o'g'li, Z. S. (2023). PHYSICAL-MECHANICAL PROPERTIES OF INTERPOLYMER COMPLEX FILM BASED ON SODIUM CARBOXYMETHYL CELLULOSE AND POLYACRYLAMIDE.

19. Jurakulov Sanjar Zafarjon Oghly. (2023). THE RELATIONSHIP OF PHYSICS AND ART IN ARISTOTLE'S SYSTEM. *International Journal of Pedagogics*, *3*(11), 67–73.