1) Guruch va sabzi teng degani uchun, sabzidan 8 kg

2) Go‘sht 2 marta kam degani. Demak: 8 : 2 = 4 kg

3) Yog’ 4 marta kam degani uchun: 8 : 4 = 2 kg

4) Piyoz esa 8 marta kam degan, yani: 8 : 8 = 1 kg

Javobi: Guruch 8 kg, sabzi 8 kg, go‘sht 4 kg, yog’ 2 kg, piyoz 1 kg sotib olish kerak.

Bundan ko‘rinadiki, o‘quvchilarda masalani yechish algortimi hosil bo‘ladi.

Foydalangan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Prezidentining 2019 yil 29 apreldagi “O‘zbekiston Respublikasi Xalq ta`limi tizimini 2030 yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g’risida”gi PF – 5712 – sonli Farmoni. https://lex.uz/docs/4312785

2. Lapchik, M.P.Informatika o‘qitish metodikasi [Matn] / M.P.Lapchik. – M.Akademiya, 2010. – 624b.

3. Gazeikina, A.I. Pedagogika unversiteti talabalariga fikrlash uslublari va dasturlashni o‘rgatish [Elektron resurs] – Kirish rejimi:

http://ito.edu.ru/2013/Moscow/I/1/I - 1 -6371.html

4. Matematika: 3 – sinf uchun darslik / S.Burxonov, O‘.Xudoyorov, Q.Norqulova; mas’ul muharrir A.Bahromov.–Toshkent: “SHARQ”, 2016.–37 b.

RAQAMLI JAMIYATDA RSA SHIFRLASH ALGORITMINING AHAMIYATI

Xasanova Mohichexra Farxod qizi

Chirchiq davlat pedagogika universiteti

Matematika va informatika fakulteti 2-kurs talabasi

E-mail: xasanovamohichehra668@gmail.com

ANNOTATSIYA:

Ushbu tezisda kriptografiyaning katta qismini egallashga ulgurgan, maxfiylikni taminlashda keng qo‘llaniladigan RSA shifrlash algoritmining

aniqlanishi ,axborotning himoyalanishi va uning raqamli jamiyatimizdagi ahamiyati haqida so‘z yuritiladi.

Kalit so‘zlar: Kriptografiya, shifrlash dekodlash, RSA shifrlash algoritmi, raqamli jamiyat

Axborot kommunikatsiya texnologiyalari bugungi kunda ma’lumot almashishda va insonlar orasidagi aloqalarni o‘rnatishda shiddat bilan rivojlanib borayotgan muhim omillardan biridir.Hozirgi kunda kriptografiya atamasi tez-tez qulog’imizga chalinadi.Kriptografiya bu axborot kommunikatsiyalari va ma’lumotlarni himoya qilish ,ularni to‘g’ridan-tog’ri o‘qimaslik uchun xizmat qiladigan texnologik usuldir.Kriptografiya yordamida malumotlar maxfiy ravishda yuboriladi va faqat maxfiy kalitlar bilan uni o‘qish mumkin.Uning ahamiyati elektron imzolar ,bank hisob-kitoblari va shaxsiy malumotlarni himoya qilishda katta rol o‘ynaydi.Kriptografiya malumotlarni shifrlash va dekodlash orqali xavsizlikni taminlash uchun matematik asoslaridan foydalanadi.Shifrlash algoritmlari- ma’lumotlarni shifrlash uchun matematik asoslar asosida yaratilgan algoritmlaridir. Jahonda kiberxavfsizlik , ma’lumotlar himoyasi va shifrlash sohasida keng qo‘llaniladigan algoritmlar RSA (Rivest-Shamir-Adleman) ,AES(Advanced Encryption Standart), 3DES(Triple Data Encryption Standart),Blowfish ,Twofish kabilardir. Ushbu tezisda RSA shifrlash algoritmida foydalanish haqida fikr mulohazalar yuritilgan.RSA ,Ron Rivest ,Adi Shamir va Leonard Adleman tomonidan 1977-yilda ishlab chiqilgan algortim. Bu shifrlash uchun ochiq kalitni va shifrni ochish uchun shaxsiy kalitni yaratadi, shuning uchun ma’lumotlarni shifrlash jarayoni juda oddiy va tez ish hisoblanadi[1].Raqamli imzolar va alektron imzolar RSA algoritmi asosida ishlaydi.Algoritm quyidagi ketma-ketlikda aniqlanadi:

1.Ikkita katta bir-biriga teng bo‘lmagan tub sonlar (p,q) tanlab olinadi.k

2.Kalitning ochiq tashkil etuvchisi n hosil qilinadi: $n = p \cdot q$

3.Eyler funksiyasi quyidagi formula bo‘yicha topiladi: $k = (p-1) \cdot (q-1)$

4. k qiymati bilan o‘zaro tub bo‘lgan katta tub son e tanlab olinadi.

5.Quyidagi shartni anoatlantiruvchi d soni aniqlanadi: $d = e^{-1} \bmod k$

Bu shartga binoan $e \cdot d$ ko‘paytmaning k qiymatga bo‘lishdan qolgan qoldiq 1 ga teng. e soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi. Yopiq kalit sifatida d soni ishlatiladi.

6. d quyidagicha aniqlanadi: $d = e^{-1} \bmod k$

Bu shartga binoan $e \cdot d$ ko‘paytmani k qiymatga bo‘lishdan qolgan qoldiq 1 ga teng. e soni esa ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi.Yopiq kalit sifatida d soni ishlatiladi.

7. Dastlabki axborot uning fizik tabiatidan qat‘iy nazar raqamli ikkilik ko‘rinishida ifodalanadi.Bitlar ketma-ketligi L bit uzunligidagi bloklarga ajratiladi ,bu yerda blok sifatida $L < \log_2(n+1)$ shartni qanoatlantiruvchi eng kata butun sonni olish tavsiya etiladi.Har bir blok $[0, n-1]$ oraliqqa taaluqli butun musbat son kabi ko‘riladi.Shu tarzda dastlabki axborot M_i , $i = \overline{1, I}$ sonlarning ketma-ketligi orqali ifodalanadi. I ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

8.Shifrlangan axborot quyidagi formula bo‘yicha aniqlanuvchi C_i sonlarning ketma-ketligi ko‘rinishida olinadi:[2]

$$C_i = M_i^e \bmod n$$

Masala: $n = 1517$, $e = 11$ ochiq kalit ,shifrlanadigan matn $M = BESH$ so‘zi va matn uzunligi $L = 8$ bit berilgan.Berilgan so‘zni shifrlang.

Shifrlash: $n = p \cdot q = 1517 \quad p = 41, q = 37$

1-qadam *BESH* so‘zini ASCII jadvali yordamida bit ko‘rinishiga o‘tkazib olamiz: 01000010 01000101 01010011 01001000

2-qadam. Bitlardan iborat matnni 8 bitdan iborat bloklarga ajratamiz va har bir blokni o‘nlik sanoq sistemasiga o‘tkazamiz:

$$M_1 = 66,\ M_2 = 69,\ M_3 = 83,\ M_4 = 72$$

3-qadam. $C_i = M_i^e \bmod n$ formula yordamida shifrlanadi:

$$C_1 = M_1^e \bmod n = 66^{11} \bmod 1517 = 763$$
$$C_2 = M_2^e \bmod n = 69^{11} \bmod 1517 = 1441$$
$$C_3 = M_3^e \bmod n = 83^{11} \bmod 1517 = 1441$$
$$C_4 = M_4^e \bmod n = 72^{11} \bmod 1517 = 1097$$

Hosil bo‘lgan shifrtekstimiz quyidagi $C = \{763,1441,821,1097\}$ ko‘rinishga ega bo‘ladi.

Raqamli jamiyatda xavfsizlikni taminlashda RSA shifrlash algoritmi kritik ahamiyatga ega. Bugungi kunda turli tizimlar RSA shifrlashidan foydalanadi ,jumladan OpenSSL, wolfCrypt ,cryptlib va boshqa kriptografik kutubxonalar[3].RSA algoritmidan Windows Server,Active Directory va Exchange Server kabi Microsoftning mahsulotlari va Cisco Systems xavfsizlikning murakkab sozlashlarida foydalanadi.

Xulosa: Internet va elektron tizimlar yordamida axborot almashish jadal rivojlanmoqda.Bu esa maxfiylik va xavfsizlik talablarini yanada oshiradi.RSA algoritmi esa bu talablarni qondiradi.Ammo kvant kompyuterlari paydo bo‘lishi bilan RSA shifrlash algoritmini buzishga olib kelishi mumkin shu sababdan bugungi raqamli jamiyatda yangi shifrlash algoritmini o‘ylab topish dolzarbdir.Ushbu tezisda RSA shifrlash algoritmi tarixi, uni amalga oshirish va uning dolzarbligi haqida bayon etilgan.

Foydalanilgan adabiyotlar:

1. M.Aripov ,A.S.Matyakubov, “Axborotlarni himoyalash usullari”,. Toshkent “Universitet”-2014.- 61-64-betlar

2. D.Y.Akbarov, P.F.Xasanov,O.P.Axmedova,I.U.Xolimtayeva “Kriptografiyaning matematik asoslari”, o‘quv qo‘llanma ,Toshkent-2018

3. Гулямов С.С. Основы информационной безопасности. Ташкент, 2004.

4. https://www.veritas.com

5. 2024-yil Xasanova ,M.F(2024) “Eyler va Ferma teoremalariga oid masalalar va ularning isbotlari” . “Ilm-fan muammolari magistrantlar talqinida” 143-146-betlar

6. **https://poe.com**

BOSHLANG’ICH SINFLARDA TEXNOLOGIYA DARSLARINI TASHKIL ETISHDA INNOVATSION TEXNOLOGIYALARDAN FOYDALANISH

Begaliyeva Mohichexra Axmatali qizi
Chirchiq Davlat Pedagogika Universiteti
2-kurs Texnologik ta’lim yo‘nalishi talabasi
e-mail: begaliyevamohichrxra@gmail.com

“Texnologiya” darsligi insonlar hayotida muhim o‘rin tutuvchi amaliy mehnat faoliyatiga tayyorgarlik ko‘rishda muhim o‘rin tutadi. Voyaga yetib, qaysi kasbni egallamang, kim bo‘lmang, “Texnologiya” fanidan olgan bilim va ko‘nikmalaringiz sizga hayotda, albatta kerak bo‘ladi. Boshlang’ich sinflarda “Texnologiya” darslarida oziq-ovqat, metallarga ishlov berish, materialshunoslik, asbob-uskunalar, moslamalar va ulardan foydalanishga oid bilimlarni o‘zlashtiradi. Mahsulot ishlab chiqarish va uyro‘zg‘or buyumlarini ta’mirlashga oid ko‘nikma va malakalarga ega bo‘ladi. Bu maqolada o‘quvchilarning turli materiallarga ishlov berish usullarini egallashida kerak bo‘ldigan qobiliyatlar va ularni shakllantirishga doir jihatlar keltirib o‘tilgan. Zero, materiallarga ishlov berish bilan bog‘liq umummehnat ko‘nikmalari har bir inson hayotida muhim o‘rin tutadi.

Jamiyatimizning har bir a’zosining bilim va salohiyatini to‘la ro‘yobga chiqarishga qaratilgan bozor munosabatlarining rivojlanib borayotganligi bu ko‘nikmalarning zaruratini yanada oshirmoqda. **Ijodkorlik** – bu yangi g‘oyaga asoslangan moddiy va ma’naviy boyliklarni yaratishdir. Ijodiy faoliyat tufayli hayotimiz yanada qulay va qiziqarli bo‘lib bormoqda. Bizni o‘rab turgan barcha