O'ZBEKISTON RESPUBLIKASI
OLIY VA O'RTA MAXSUS
TA'LIM VAZIRLIGI

BUXORO DAVLAT UNIVERSITETI
1930

O'ZBEKISTON RESPUBLIKASI
INNOVATSION
RIVOJLANISH VAZIRLIGI

МАТЕМАТИКА, ФИЗИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИНИНГ ДОЛЗАРБ МУАММОЛАРИ

МАВЗУСИДАГИ РЕСПУБЛИКА МИҚЁСИДАГИ ОНЛАЙН ИЛМИЙ-АМАЛИЙ АНЖУМАНИ

ТЕЗИСЛАР ТЎПЛАМИ

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

БУХОРО ДАВЛАТ УНИВЕРСИТЕТИ

ФИЗИКА-МАТЕМАТИКА ФАКУЛЬТЕТИ

“МАТЕМАТИКА, ФИЗИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИНИНГ ДОЛЗАРБ МУАММОЛАРИ”

мавзусидаги

Республика миқёсидаги онлайн илмий-амалий анжумани

ТЕЗИСЛАР ТЎПЛАМИ

Бухоро, 2020 йил 15 апрель

Бухоро- 2020

4. Mathematica - 7|8. *Vazifasi va imkoniyatlari:*

1)Universitetlarning yuqori bosqich talabalari va ilmiy texnik hisoblashlarga mo'ljallangan

2) Turli platformadagi EHMlarga mo'ljallanganligi

3)Tovushlarni sintez qilish imkoniyatining mavjudligi

4) Ma'lumotlar tizimi juda qulay shaklda tashkil etilgan

5) Hujjatlarni yuqori saviyada formatlash mkoniyati mavjud

Kamchiliklari:

1)Katta hajmda EHM resurslarini talab qilinishi

2)Yuqori malakali mutaxassislarga va matematiklarga mo'ljallanganligi.

Shunday qilib, yuqoridagi ma'lumotga qo'shimcha ravishda shuni aytish mumkinki, Mathematica 8.0 tizimida barcha bajariladigan ishlar bloknot (hujjat) sifatida tashkil qilinib, muloqot interaktiv rejimda amalga oshiriladi.

Yuqoridagi tavsiflari keltirilgan dasturiy tizimlardan foydalanishning *ommaviylashuviga* quyidagi faktorlar:

-kompyuterlar odatdagi uy elektr jihozlari qatoridan o'rin olayotganligi;

-hozirgi zamon talabasi, ilmiy xodimi va mutaxassisi hayotida Internet tarmog'idan foydalanish kundalik ehtiyojga aylanganligi;

-o'quvchi va talabalarga bilim berishda dasturiy tizimlardan o'qitish vositasi sifatida foydalanish darajasining oshishi;

-dasturiy tizimlardan foydalanishga doir maxsus adabiyotlarni ko'payganligi asosiy sabab bo'lmoqda.

Holbuki rivojlangan mamlakatlarda bu tizimlar o'qitish jarayonining ajralmas qismiga aylanib qolgan. Masalan, AQSh, Xitoy, Yaponiya va Germaniya davlatlarida bu tizimlardan nafaqat o'qitish jarayonida, balki ilmiy-texnik hisoblashlarda unumli foydalanilmoqda. MDH mamlakatlari orasida bu borada Belorussiya respublikasining professor o'qituvchilari, muhandislari va olimlari peshqadamlikni qo'ldan bermay kelmoqdalar. Bizning nazarimizda, ushbu maqolada respublikamizda birinchi marta, o'zbek tilida Mathematica paketining imkoniyatlari qisqacha bayon qilingan. Shuning uchun, ushbu maqola, ba'zi xatoliklardan holi bo'lmasligi mumkin. Bizning keyingi tadqiqotlarimiz Mathematica sistemasining boshqa imkoniyatlarini yanada batafsil yoritishga hamda bu sistema vositalarini aniq fanlarini o'qitishga tatbiq etishdan iborat bo'ladi.

FOYDALANILGAN ADABIYOTLAR.

1.Yusupbekov N.R., Muxitdinov D.P., Bazarov M.B, Xalilov A.J. Boshqarish sistemalarini kompyuterli modellashtirish asoslari: O'quv qo'llanma.- Navoiy: «Navoiy Gold Servis».- 2008. - 184 bet.

2. Базаров М. Б. Основы системы Mathematica .// Навои. –НГГИ.-2004.

3. Mo'minov.B. Informatika.Toshkent 2012.

4. Дьяконов В.П. Mathematica 4: учебный курс. // СПб.: Питер, 2001.

5. Qurbonov B., To'rayev M. Mathematica 8 dasturi. Uslubiy qo'llanma. Buxoro-2013.

6.Семененко Н.Г. Введение в математическое моделирование. Maple, Mathematica, MATLAB.// М.: СОЛОН, 2002.

9. Воробьев Е.М. Введение в систему MATEMATICA.// М.:"Финансы и статистика", 1998.

10. Mathematica 8 ning ma'lumotlar tizimi(help menyusi).

Internet rusurslari:

1. http://wolfram.com/.

2. http://www.exponenta.ru/.

3. http://www.mathematica.com/.

MATHEMATICA SISTEMASINING TUZILISHI VA INTERFEYS OYNASINING TARKIBI.

To'rayev Mardonjon Farmonovich,

BuxDU Axborot texnologiyalari kafedrasi o'qituvchisi

Maqolada rivojlangan davlatlarda keng qo'llaniladigan mathematica sistemasining tuzilishi va interfeys oynasining tarkibi hamda menyu qisimlari bayon etilgan.

В статье описывается структура системы mathematica и структура окна интерфейса, а также пункты меню, которые широко используются в развитых странах.

In the article has described the structure of the mathematica system and the structure of the interface window, as well as the menu items, which are widely used in the developed countries.

Mathematica tizimini, boshqa shu turdagi tizimlarga nisbatan ustunliklaridan biri –uni turli kompaniyalar(firma)larning (Macintosh, Apple va x.k) EHM lari uchun bir xilligi, ya`ni barcha shaxsiy EHM lar uchun moslashtirilganligidir.

Uning ishlash prinsipi, **asosiy qismlari**: Yadro;· Interfeys; Amaliy dasturlar majmuasi(paketi), Kutubxona; Ma'lumotlar(Help)

Ma'lumotlar tizimlarining quyidagi o'zaro aloqasi (bog'liqligidan) ko'rish mumkin, bunda asosiy o'rinni Yadro (Kernel) tashkil etadi. Yadro aniq bir EHM tuzilishiga bog'liq bo'lmasdan, u asosan matematik hisob-kitoblarni bajarishga mo'ljallangan. Bu tizimni aniq bir EHM platformasiga moslashtirish (yo'naltirish) uchun Interfeys protsessori (Front End) xizmat qiladi. Kutubxona (Library) esa Yadroga biriktirilgan mavjud funksiyalar safini kengaytirish uchun mo'ljallangan. Sonli analiz usullarining algoritmlarini hamda amaliy masalalarni yechish algoritmlarini va dasturlari Amaliy dasturlar majmuasi (ADM) (Paketы rasshireniye-AAD-ON-Paskages) da mujassamlashtirilgan. Bu dasturlar Mathematica dasturlash tilida tuzilgan bo'lib, bu majmuani foydalanuvchi tomonida kengaytirish imkoniyati ham ko'zda tutilgan, ya`ni foydalanuvchining o'zi ham ma'lum bir sinfdagi masalalarning yechish dasturlarini tuzib, ushbu majmuaga qo'shib quyishi mumkin. Bundan tashqari, Mathematica dasturiy tizimi, tizimga biriktirilgan Ma'lumotlar tizimi (Help)ga egadir. Bu ma'lumotlar o'zida elektron darslikni jamlagan bo'lib, bu elektron kitoblarda "jonli" misol va ko'rsatmalar jamlangan. Ya`ni, foydalanuvchi elektron darsliklardan foydalanganda, ularda keltirilgan qoida va namunaviy ko'rsatmalarni, o'zining ma'lumotlari yordamida tekshirib ko'rishi mumkin.

Interfeys oynasining tarkibi. Ixtiyoriy dasturiy tizimdan foydalanish uchun uning foydalanuvchilar bilan muloqot muhiti (interfeysi) ni bilish zarur. Mathematica 8.0 tizimining Windows operatsion muhitida joriy qilingan interfeysi bilan tanishamiz. Mavjud dasturiy tizimlar: Maple, Mathcad va h.k ham Windows operatsion muhitida ishlagani sababli, ularning interfeyslari Microsoft Office muhitidagi dasturlar (Word, Excel, Power Paint) interfeyslariga o'xshashdir.

Shunday qilib, Mathematica tizimining ko'rinish interfeysi, umumiy holda, quyidagicha: Oyna sarlavhasi , Menyular satri ,Prokrutka chizg'ichlari ,Ishchi soha :

Interfeys oynasining ko'rinishi.

Sarlavhada Mathematica tizimining belgisi va joriy "ishchi soha"dagi hujjatning nomi ko'rsatiladi. E'tibor berilsa, Mathematica paketida, boshqa dasturlardagidek, "Vositalar paneli", "Formatlash paneli" va shunga o'xshash satrlar mavjud emas. Tizim mualliflari tomonidan, bu yordamchi vositalar - panellarining o'rniga turli matematik belgilar funksiyalar, tizimni boshqarish buyruqlarining (ularning soni 700 dan ortiq) piktogrammalarini o'zida mujassamlashtirgan palitralar kiritilgan.

Prokrutka chizg'ichlari. Bu chizg'ichlar tizim oynasining o'ng va ostki qismlarida joylashgan. Ular ishchi sohadagi matnni vertikal va gorizontal yo'nalishlarga siljitish uchun ishlatiladi. Har bir chizg'ichda "yugurdak"(begunok) o'rnatilgan bo'lib, u orqali oyna hujjatning qaysi joyiga kelganini bilib olish mumkin.

Menyular satri. Matematica tizimida ham boshqa dasturlardagi kabi, bajarilayotgan amallar menyu qismlari orqali tartibga solinadi.

Menyular satrining ko'rinishi

Menyular satri quyidagi qismlardan: Fayl (File), Tahrir (Edit), Qo'shish(Insert), Format (Format), Yacheyka (Cell), Grafiklar (Graphics), Evalution, Palitra(Paletters), Oyna (Window), Yordam(Help). Bu qismlarning orasida "Fayl" va "Tahrir"ning ko'pgina bandlari Windowsning barcha amaliy dasturlaridagi (Fayl va Tahrir) kabidir.

Fayl (File) menyusi. Bu menyuda fayllar bilan ishlash, yangi hujjatlar uchun oyna yechish, oldingi saqlangan hujjatlarni xotiradan chaqirish, joriy hujjatni yopish, tayyorlangan hujjatni diskga yozish, yangi oynadagi hujjatga nom berib saqlash, matnni hujjatga qanday joylashganini oldindan ko'rish, hujjatlarni chop etish hamda tizimdan chiqish kabi bir qator ishlarni amalga oshirish mumkin.

Fayl menyusining ba'zi bir bandlari bilan tanishamiz:

-Yangi (Notebook-Ctrl+N) - yangi hujjat uchun oyna hosil qilish;

-Ochish (Open-Ctrl+Q) - mavjud oynani yuklash;

-Saqlash (Save-Ctrl+S) - hujjatni yozish , saqlash

-Yopish (Close-Ctrl+F4) - joriy oynani yopish;

-Kabi saqlash (Save as-Shift +Ctrl+S)- hujjatni nomini o'zgartirib yozish;

- Open Special- fayllarni maxsus formatlarda ochish;

-Printing Settings- chop etish parametrlarini o'rnatish;

-Chop etish (Print - Ctrl+P)- joriy hujjatni chop etish

-Chiqish(Exit-Alt+F4)- tizim ishini yakunlash.

Fayl, bloknot tushunchalari. Ma'lumki, fayl tushunchasi har qanday dasturiy muhitning asosiy vositalaridan biridir. Mathematica tizimida fayllar ham ikkita katta sinfga: sistemali fayllar va foydalanuvchi tomonidan tuzilgan fayllarga bo'linadi.

Dastlabki paytlarda Mathematica tizimida tuzilgan hujjatlarning fayllari ***.ma*** (Mathmatical-applications-so'zlarining bosh harflari) kengaytma bilan foydalanilgan. Bunday kengaytmali fayllarni muharrirlash oynasiga chaqirib to'ldirish, tahrirlash yoki bajarish mumkindir. Bunday fayllarni tizimga yozib qo'yish jarayonida, tizimning resurslari tomonida, bir vaqtning o'zida, .mb kengaytmali binar fayllar ham hosil kilinadi. Bu faylning ***.mb*** kengaytmasida hujjatning, berilgan matnning grafik obrazi hosil qilinadi.

Mathematica tizimining 3/4 - versiyalaridan hujjatlarni "Bloknot" yoki "Zapisnaya knijka" (rus tilida) yoki Notebook (ingliz tilida) atash qabul qilinadi. O'zbek tilidagi bayonlarimizda esa bunday bloknotlarni " Hujjat" deb atashga kelishib olamiz. Shunday qilib, bloknot - hujjatlarda oddiy matn yoki grafik yoki boshqa ma'lumotlarni saqlash mumkin. Bloknot- hujjatlar **.nb** kengaytmali matnli fayllar sifatida foydalaniladi. Bunday kengaytmali fayllarni ASCII formatli ixtiyoriy matn muharriri tomonidan o'qish va tahrirlash mumkin.

Taxrir (Edit) menyusi. Hujjatlarni tahrirlashning barcha amallari Redaktirovat menyusida keltirilgan. Ushbu menyuning ba'zi bandlarini tavsiflarini keltiramiz:

-Qaytish (Undo – Ctrl+z)- amallarni rad etish;

-Qirqish(Cut - Ctrl+x) – yacheykadagi matnni qirqib buferga o'tkazish;

-Nusxa olish(Copy - Ctrl+c) – yacheykadagi ma'lumotni nusxasini olish;

-Joylashtirish(Paste - Ctrl+v) – buferdagi ma'lumotni yacheykaga joylashtirish;

-Kabi joylashtirish(Paste as) – buferdagi ma'lumotni berilgan formatda yacheykaga joylashtirish;

-Barchasini belgilash(Sellect all - Ctrl+a) –barcha yacheykalarni belgilash(tanlash);

- Insert Object- ob'ektlarni joylashtirish;

-Chek Spelling– orgrofiya nuqta- nazaridan tekshirish;

-Sozlash (Prefereces) – tizimni sozlash oynalarini chaqirish.

Insert menyusi. Insert menyusi yordamida hujjatimizga jadval, mavjud fayllarni, ranglarni, obyektlarni qo'shish mumkin. Input from above(ctrl+l) (ishga tushirish yuqorida ko'rsatilgan)-oxirgi natijani satr bo'yicha, Output from above(xulosa yuqorida ko'rsatilgan)- ustun bo'yicha qo'shadi.

Naytida matnlardagi va ifodalardagi qism matnlarni izlab topish yoki almashtirish amallarini bajaradigan qism menyular keltirilgan.

Find – berilgan satrlarni (oldinga va orqaga qarab) almashtirmasdan izlash; Enter Selection – tanlangan satrni izlash; Find Next – oldinga qarab hujjat bo'yicha izlash;

Find Previous- orqaga qarab hujjat bo'yicha izlash.;

Find in Cell Tags – berilgan etiketkali(tegli) yacheykani izlash;

Replace All – berilgan hujjatda almashtirishni bajarish.

Format(Format) menyusi. Mathematica tizimida kiritish va chiqarish yacheykalarining formatlashni turli imkoniyatlari mavjud. Bu imkoniyatlarga yacheykalarni o'lchamlarini, simvollarning ranglarini, Shriftlarni tanlash va h.k. lar kiradi. Format menyusi bir necha bandlardan tashkil topganini ko'rish qiyin emas. Bu buyruqlar odatda nashriyot masalalarini qulay va tez hal qilish uchun qo'llaniladi.

Yacheyka(Cell) menyusi. Hujjatlardagi barcha ma'lumotlar yacheykalarda saqlanadi. Yacheykalarning xarakteri ular bajaradigan funksiyalarga hamda ulardagi ma'lumotlarning turiga bog'liqdir. Yacheykalarni o'ng tomonidagi ko'k rangdagi kvadrat qavs (o'rta qavs -]), ularning o'lchovini , stili(uslubi)ni, xarakterini anglatadi. Shu o'ng tomondagi o'rta qavslardagi ortiqcha belgilarga ko'ra uning atributi (xossasi)ni aniqlash mumkin.

Shunday qilib, har bir yacheyka ma'lum bir maqsad uchun yo'naltiriladi va foydalaniladi. Masalan, hujjatning sarlavhasi – nomi yozilgan yacheyka faollashmagan ("inactive" - neaktivnaya) deb ataladi. Faollashmagan yacheyka hisoblashlarda foydalanilmaydi. Hisoblash natijalarini chiqarish (Chop etish) ga mo'ljallangan yacheyka formatlangan («formatted» - formatirovannaya) deb ataladi. Bu yacheyka ham tahrirlanmaydi. Kiritish ma'lumotlarini o'zida aks ettiruvchi yacheyka esa formatlanmagan («unformatted» - neformatirovannaya) deb atalib u tahrirlanadi. Faollashmagan yacheyka oxiridagi o'rta qavs **(]** ning yuqori qismida gorizontal chiziqcha belgisi turadi. Bundan tashqari, yopilgan , initsializatsiya qilingan (initsializirovannaya) yacheyka tushunchalari ham mavjud. Yopilgan yacheykaning o'ng tomonidagi o'rta qavsning yuqori qismida «**x**» belgisi turadi. "Locked" buyrug'i orqali yoki sichqonchani *x]* belgisiga

keltirib chap tugma ikki marta bosib, yopilgan yacheykani ochish mumkin. Odatda tashqaridagi turli tasodifiy aralashishlardan yacheykani himoyalash maqsadida, yacheyka yopib qo'yiladi. Har bir yacheyka hujjatda o'zining aniq bir stili (uslubi) ga egadir. Ya`ni, yacheykadagi matnnning shrifti, o'lchami, rangi bo'lishi mumkin.

Yacheykalar hujjatlarning asosiy qismlari hisoblanadi. Yacheyka bir – biridan statusi (maqomi) bilan farq qilib, uning tipi va turli holatlardagi ko'rinishlari – ularning asosiy xarakteristikasi hisoblanadi. Yacheyka menyusida yacheykalar ustida amallar bajarishni tashkil etadigan buyruqlar joylashtirilgan. Ushbu menyuning ba'zi buyruqlarining tavsiflari quyidagicha:

-Convert to – yacheyka formatini almashtirish;

-Display As – yacheyka kœrinishini formatini almashtirish;

-Cell Properties – yacheykalarni xossalarini o'rnatish;

- Cell Groupping - yacheykalarni guruhlash;

- Cell Size Statistics – yacheykalarning o'lchamlari haqida ma'lumotlarni olish va h.k.

Graphics (bo'yoqsiz rasm solish**) menyusi** grafiklar va har xil shaklar chizish imkoniyatini beradi. New Graphic (ctrl+1) bandi yangi grafik soha hosil qiladi, Grafic Tools(crtl+d) – grafiklar bilan ishlash uskunalar oynasini ekranga chiqaradi.

Ma'lumki hisoblarni bajarishdan oldin hisoblashlar uchun kerakli ma'lumotlarni va matematik ifodalarni kiritish zarur. Ushbu masalalar Graphic menyusi orqali hal qilinadi. Menyudagi ba'zi buyruqlarning bajarilish qoidalari bilan tanishaylik. Ma'lumki, ikki o'lchovli grafiklar yordamida chiziqsiz algebraik tenglamalarni qulay usullar bilan yechish mumkin. Mathematica tizimida ikki o'lchovli grafiklarning nuqtalarini koordinatalarini Get Graphics Coordinates buyrug'i yordamida olinadi.

Jadval qiymatlarni kiritish menyuning Greate Table/Matrix/Palette buyrug'i orqali amalga oshiriladi.

Hisoblash (Evaluation) menyusi. Evaluation menyusida ishchi sohaga yuklangan (chaqirilgan) hujjatning yacheykalari ustida Yadro tomonidan bajariladigan amallarning ro'yxati keltirilgan. Bu qism menyular hisoblash jarayonini boshqarish uchun xizmat qiladi. Menyuning ayrim bandlari bilan qisqacha tanishamiz:

Evaluation Cells – tanlangan yacheykalarni hisoblash;

Evaluation Notebook – hujjatni barcha yacheykalarini hisoblash.

Hujjatlarda kiritish va chiqarish satrlari mos ravishda In[n] va Out[n] ko'rinishida belgilanadi. Ba'zan bu belgilar hujjatlarni rasmiylashtirishda xalaqit beradi. Shuning uchun, Yadro menyusidagi Show In/Out Names qism menyusi bu In[n] va Out[n] larni hujjatlarda ko'rsatmaslik imkonini beradi.

Palitra (Paletters) menyusi. Palitralarni ishchi sohaga chaqirish. Har xil funksiya, operatorlarni ishlatganda ularni yozib o'tirmay qoliplaridan foydalanish imkonini beradi.

Oyna (Window) menyusi. Mathematica tizimi ham ko'p oynali dasturlar sinfiga tegishli bo'lib, bir vaqtning o'zida bir necha hujjatlar bilan ishlash mumkin. Okno menyusidagi qism menyular ro'yxati bilan tanishamiz:

Stack Windows – oynalarni kaskadli joylashtirish;

The Windows Wide – oynalarni balandlik bo'yicha ustma-ust joylashtirish;

The Windows Tall – oynalarni yonma-yon joylashtirish.

Har bir hujjat o'zining oynasiga ega bo'lishi tabiiydir. Foydalanuvchi o'ziga qulay shaklda oynalarni joylashtirib ularda kerakli amallarni bajarishi mumkin.

Yordam (Help) menyusi. Mathematica tizimi juda ham boy ma'lumotlar tizimiga egadir. Help menyusida juda qulay usulda kerakli ma'lumotlarni topish mexanizmi ishlab chiqilgan.

Ma'lumotlar tizimining The Mathematica Book(F1) bo'limida esa katta hajmdagi ma'lumotlar (formulalar, grafiklar, turli xarakterdagi hisoblashlarning namunalari) jonli misollar yordamida keltirilgan. Boshqa ma'lumotlar bo'limida esa tizimning interfeysi haqidagi barcha ma'lumotlar va h.k. lar keltirilgan.

FOYDALANILGAN ADABIYOTLAR.

1.Yusupbekov N.R., Muxitdinov D.P., Bazarov M.B, Xalilov A.J. Boshqarish sistemalarini kompyuterli modellashtirish asoslari: O'quv qo'llanma.- Navoiy: «Navoiy Gold Servis».- 2008. - 184 bet.

2. Базаров М. Б. Основы системы Mathematica .// Навои. –НГГИ.-2004.

3. Mo'minov.B. Informatika.Toshkent 2012.

4. Дьяконов В.П. Mathematica 4: учебный курс. // СПб.: Питер, 2001.

5. Qurbonov B., To'rayev M. Mathematica 8 dasturi. Uslubiy qo'llanma. Buxoro-2013.

6.Семененко Н.Г. Введение в математическое моделирование. Maple, Mathematica, MATLAB.// М.: СОЛОН, 2002.

9. Воробьев Е.М. Введение в систему MATEMATICA.// М.:"Финансы и статистика", 1998.

10. Mathematica 8 ning ma'lumotlar tizimi(help menyusi).

Internet rusurslari:
1. http://wolfram.com/.
2. http://www.exponenta.ru/.
3. http://www.mathematica.com/.

AXBOROTLARNI SHIFRLASHDA RSA ALGORITMI.

Jalolov Ozodjon Isomidinovich
(BuxDU, axborot texnologiyalari kafedrasi dotsenti)
Jo'rayev Qo'ldosh Ismatullo o'g'li
(BuxDU, 1- bosqich maristranti)

Hozirgi kunda bilamizki axborot eng muhim tushunchalardan biri hisoblanadi. Axborotlarni turli xil hujumlardan himoyalashda axborotlarni shifrlash muhim ahamiyat kasb etadi Shifrlash 2 xil usulda amalga oshiriladi: simmetrik shifrlash va asimmetrik shifrlash. Ushbu maqolada RSA algoritmi tushuntirib berilgan RSA algoritmi asimmetrik shifrlash usuliga kiradi. Bunda axborotlarni himoyalashda 2 ta kalit ishlatiladi: ochiq kalit yordamida axborotlar shifrlanadi, maxfiy (yopiq) kalit yordamida shifrlangan axborot dastlabki holatiga qaytariladi, ya'ni shifrlangan axborot rasshifrovka qilinadi.

RSA algoritmi faqat sonlarni shifrlashga mo'ljallangan bo'lib, tub sonlar yordamida shifrlash amalga oshiriladi. RSA algoritmini tushunish uchun dastlab quyidagi matematik ifoda va funksiyani bilish talab qilinadi:

1) $m \bmod n = x$

Yuqoridagi ifoda m sonini n soniga bo'lgandagi qoldiq x ga teng demakdir. Masalan: $26 \bmod 7 = 5$.

2) Eyler funksiyasi o'zaro tub sonlar juftligini aniqlaydi. $\phi(n) = n - 1$

Bu funksiya orqali n sonigacha bo'lgan o'zaro tub sonlar nechtaligi topiladi. Bunda n tub son bo'lishi kerak, agar n tub son bo'lmasa uni tub sonlarning ko'paytmasi shaklida ifodalab olinadi. Agar $n = a * b$ ko'rinishida bo'lsa (a va b tub son), bunda quyidagi tenglik o'rinli bo'ladi:

$$\phi(a * b) = \phi(a) * \phi(b) = (a - 1)(b - 1)$$

Masalan: $\phi(7) = 7 - 1 = 6$ bundan 7 gacha 6 ta o'zaro tub sonlar juftligi borligi kelib chiqadi, ular quyidagilardir: $(1,7)$; $(2,7)$; $(3,7)$; $(4,7)$; $(5,7)$; $(6,7)$.

Eyler funksiyasi uchun quyidagi tenglik o'rinli: $m^{\phi(n)} \bmod n = 1$

RSA algoritmida biror m sonni shifrlash uchun dastlab 2 ta tub a va b sonlarni tanlaymiz. $n = a * b$ bo'lsin, u holda yuqoridagi Eyler funksiyasiga asosan $\phi(n) = (a - 1)(b - 1)$ bo'ladi. Keyin yana bitta e tub sonni tanlaymiz. Bunda $e < \phi(n)$ shart bajarilishi kerak. m sonini quyidagi formula yordamida shifrlaymiz:

$$m^e \bmod n = x$$

x – m sonining shifrlangani bo'ladi.

Endi RSA algoritmini Mathcad tizimida bajarib ko'ramiz:

1. *p* va *q* tub sonlari tanlanadi: p:=13 q:=19
2. Hisoblanadi: *n = p * q : n=247*
3. Hisoblanadi: *m = (p - 1) * (q - 1): m=216*
4. *m* ga nisbattan o'zaro tub bo'lgan *d* soni tanlanadi
5. *e* soni shunday tanlanadiki: *e * d = 1 (mod m): d:=5 e=0.2*

Bu algoritm [0; n-1] gacha bo'lgan sonlarni shifrlab beradi.
Masalan: a:=244
Shifrlash: *b:=mod(a^e,n)* *natija: b= 3.00246508138818*
Teskari shifrlash: a:=mod(bd,n) natija: a=244