

**O'ZBEKISTON RESPUBLIKASI AXBOROT  
TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI  
RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI  
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI  
SAMARQAND FILIALI**

**Zaynalov N.R.**

**KRIPTOGRAFIYADAN MISOL VA MASALALAR  
TO'PLAMI**

O'zbekiston Respublikasi Oliy va O'rta maxsus ta'lif vazirligi  
tomonidan o'quv qo'llanma sifatida tavsiya etilgan

**Samarqand – 2022 y.**

Zaynalov N.R. Kriptografiyadan misol va masalalar to‘plami. Elektron o‘quv qo‘llanma. – Samarqand.: ”TATU SF”, 2022 y.

Mazkur o‘quv qo‘llanma “Kriptografiya I” o‘quv fani dasturi asosida yozilgan, unda shifrlashga doir har xil murakkablikdagi masalalar yoritib berilgan. Asosiy maqsad qilib kriptografiyaga doir masalalarni har bir qadamini anglab olishga va uni batafsil tahlil qilishga qaratilgan. Ushbu masalalarni yechish uchun zaruriy ma’lumotlar to‘liq keltirilgan. Shu bois talabalar ushbu qo‘llanmada keltirilgan namunalar orqali masalaning mazmun-mohiyatini tushunib olishlari mumkin bo‘ladi va kelgusida mukammal usullarni yaratishlariga zamin bo‘lib xizmat qiladi.

O‘quv qo‘llanma “5330300-Axborot xavfsizligi” ta’lim yo‘nalishi talabalari uchun mo‘ljallangan bo‘lib, undan oliy o‘quv yurtlari, ixtisoslashtirilgan texnikum, maktab va litsey o‘qituvchilari, hamda shifrlash texnologiyalarini o‘rganayotganlar ham foydalanishlari mumkin bo‘ladi.

#### Taqrizchilar:

Urubaev E. – fizika-matematika fanlari doktori ( DSc ), Sharof Rashidov nomidagi Samarqand Davlat Universiteti, «Matematik modellashtirish» kafedrasи dotsenti.

Yaxshiboyev M.U. - fizika-matematika fanlari doktori ( DSc ), Muhammad al-Xorazmiy nomidagi TATU Samarqand filiali «Tabiiy fanlar» kafedrasи professori.

## Mundarija

KIRISH .....	5
1-bob. KRIPTOGRAFIYANING UMUMIY ASOSLARI .....	7
1.1. Kriptografiya tarixi .....	7
1.2. Kriptografiya tasnifi .....	8
2-bob. KRIPTOGRAFIYANING MATEMATIK ASOSLARI .....	14
2.1. Sanoq tizimlari va bitlar arifmetikasi.....	14
2.2. Butun sonlarning bo‘linish belgisi.....	28
2.3. Tub sonlar .....	31
2.4. Sonlarni ko‘paytuvchilarga yoyish .....	33
2.5. Eng katta umumiy bo‘luvchi .....	34
2.6. Taqqoslama arifmetikasi .....	39
2.7. O‘rin almashtirishlar .....	47
2.8. Matritsalar.....	55
3-bob. SIMMETRIK KALITLI SHIFRLASH TIZIMLARI .....	65
3.1. O‘rniga qo‘yish usuli.....	65
3.2. Monoalifboli o‘rniga qo‘yish usuli .....	68
3.2.1. Sezar usuli.....	72
3.2.2. Affin tizimidagi Sezar usuli.....	74
3.2.3. Tayanch so‘zli Sezar usuli.....	75
3.2.4. Polibiy kvadradi .....	77
3.2.5. Atbash usuli .....	81
3.2.6. Pleyfer usuli .....	84
3.2.7. Omofon usuli .....	90
3.2.8. Vernam usuli .....	95
3.3. Polialifboli o‘rniga qo‘yish usuli.....	98
3.3.1. Gronsfeld usuli .....	99
3.3.2. Vijiner jadvali .....	101
3.3.3. ADFGX usuli .....	104
3.4. O‘rin almashtirish usuli.....	106

3.4.1. Shifrllovchi jadval .....	109
3.4.2. Tayanch so‘zli shifrllovchi jadval.....	110
3.4.3. Matritsa usuli .....	112
3.4.4. Sehrli kvadrat .....	114
3.4.5.Gamilton usuli.....	115
3.5. Shifrlashning analitik usullari.....	117
3.5.1. Matritsalarni ko‘paytirish usuli .....	117
3.5.2. Xaltaga buyumlarni joylashtirish masalasi .....	121
3.6. Shifrlashning additiv usullari .....	127
3.6.1.Gammalashtirish usuli.....	128
3.6.2.Uitstonning “ikki kvadrat” usuli .....	130
3.6.3. To‘rt kvadrat usuli.....	133
3.6.4.Xill usuli .....	135
<b>4-bob. KODLASHGA DOIR ODDIY MISOLLAR .....</b>	<b>140</b>
4.1. Kodlashga doir usullar .....	140
4.2. Xaffman usuli .....	141
<b>5-bob. AMALIY MASHG‘ULOTLAR UCHUN KO‘RSATMALAR .....</b>	<b>148</b>
5.1. N bitli skremblerni qurish va takrorlanish davrini hisoblash.....	148
5.2. Blokli shifrlar yordamida ma’lumotlarni shifrlash.....	156
5.3. Psevdotasodifiy sonlar generatorini va uning dasturiy ta’mintonini yaratish .....	171
5.4. RC4 shifrlash algoritmi asosida ma’lumotni shifrlash va deshifrlash dasturini yaratish.....	187
5.5. OpenSSL kutubxonasidan foydalangan holda ma’lumotlarni xesh qiymatini hisoblash .....	201
<b>XULOSA .....</b>	<b>220</b>
Tayanch so‘zlar ko‘rsatkichi .....	221
Foydalilanilgan adabiyotlar ro‘yxati .....	223
Amaliy dasturlar .....	226
Masalalar javoblari.....	238

## KIRISH

Ushbu o‘quv qo‘llanma kriptografiya sohasida mavjud qo‘llanmalarini to‘ldirishga yo‘naltirilgan bo‘lib, bo‘lajak mashhur dasturlovchilarining o‘z mahsulotlarida kriptografiya usullaridan qanday foydalanishni misollarda tushuntirib berishga bag‘ishlangan.

Kriptografiyanı o‘rganish uchun faqatgina nazariy bilim yetarli bo‘lmaydi. Shu bois, shu kungacha ishlab chiqilgan usullarni chuqur o‘rganib chiqish muhim hisoblanadi, shundan so‘ng axborot tizimlarida axborot xavfsizligini ta’minlash maqsadga muvofiq bo‘ladi.

O‘quv rejaga binoan kriptografiya fani 2 qismiga bo‘lingan. Bu yerda “Kriptografiya 1” qismiga doir mavzular ko‘rib chiqilgan. Qo‘llanmada keltirilgan shifrlash usullarini bevosita dasturlash tillariga o‘girish uchun yetarlicha misollar keltirilgan. Kitobda keltirilgan usullarni chuqur o‘rganish uchun ularni mustaqil ravishda bajarish lozim bo‘ladi, shu bois har bir bobdagi paragraf oxirida topshiriqlar keltirilgan. Ular bir tartibda raqamlangan va javoblar kitobning oxirida keltirilgan.

Mazkur o‘quv qo‘llanmaning “Kriptografiyaning umumiy asoslari” nomli birinchi bobida kriptografiya sohasiga asos solgan islom dunyosidagi olimlar haqida so‘z yuritilgan. Keyinchalik ushbu sohaning rivojlanishi natijasida yuzaga kelgan usullar tizimli ravishda tasniflangan. Keyingi boblarda keltirilgan tasnif asosida materiallar uzviy ketma-ketlikda berilib borilgan. Bu yerda keltirilgan asosiy shifrlash usullari kriptografiyada qabul qilingan tartib asosida berilgan va undagi tushunchalar keyingi mavzularni bayon etishda qo‘llanilgan.

“Kriptografiyaning matematik asoslari” ikkinchi bobda bevosita butun va natural sonlar ustida bajariladigan amallar va hozirgi zamon algebrasining asosiy tushunchalari haqida boshlang‘ich ma’lumotlar berilgan. Shu bois bobning nomlanishida “arifmetika” so‘zini qo‘llash mumkin. Bu bilan beriladigan ma’lumotlar oddiyligi bilan ajralib turishini ta’kidlash mumkin.

Keyingi, “Simmetrik kalitli shifrlash tizimlari” nomli uchinchi bobda hozirgi kungacha ma’lum bo‘lgan oddiy kriptografiya usullarining asosiy qismi yoritilgan. Bu yerda keltirilgan usullar o‘zining g‘oyasi va qo‘llanishdagi imkoniyati bilan biri-biridan ajralib turadi. Ushbu usullarni bayon qilish mazkur bobning mazmunini tashkil etadi.

“Kodlashga doir oddiy misollar” nomli to‘rtinchi bobda keltirilgan yondashuv bevosita shifrlashdan mazmunan farq qiladi. Ammo, kodlash usullari mazmunan ma’lumotlarni yagona tizimga solishni o‘rgatadi va shu bois ham kitobdan o‘rin olgan. Hozirgi zamon kompyuterlarida keng tadbiqga ega bo‘lgan arxivlash texnologiyasi ham aynan kodlash jarayoni orqali amalga oshiriladi.

Beshinchi “Amaliy mashg‘ulotlar uchun ko‘rsatmalar” nomli bobda bevosita “Kriptografiya 1” fani bo‘yicha amaliy mashg‘ulotlarni o‘tkazish bo‘yicha to‘liq va batafsil tavsiyalar berilgan. Mavzularni to‘liq tushunib olish uchun barcha jarayonlar qadamba-qadam yoritib berilgan. Talabalardan keltirilgan jarayonlarni mustaqil bajarishlari talab etiladi. Keltirilgan algoritmlar juda murakkab bo‘lganligi sababli, ba’zida qisqartirilgan algoritmlar ham bayon etilgan.

Qo‘llanmada keltirilgan har bir usulning bayoni batafsil yechilgan misollar bilan mustahkamlangan. Bundan tashqari qaralayotgan mavzu bevosita matematika kursi bilan uzviy bog‘lab yozilgan. Qo‘llanmada talabalarning mustaqil ishlashi uchun topshiriqlar keltirilgan. Ularda mavjud misollar soni har xil bo‘lishiga qaramay, talabalarning bilimini mustahkamlash uchun yetarli hisoblanadi.

Qo‘llanmani yaratilishida va uni birlamchi qo‘lyozma holatida o‘qib, undagi bir qancha kamchiliklarni tuzatishda o‘z maslahatlarini bergen Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali dotsenti U.X.Narzullayev va Samarqand Davlat universitetining dotsenti G‘.M. Porsayevlarga samimi minnatdorchilik bildiraman.

## **1-bob. KRIPTOGRAFIYANING UMUMIY ASOSLARI**

Kriptografiya fani biz uchun umuman olganda yot fan emas, chunki uning shakllanishida ajdodlarimiz hissalari bor. Masalan, “shifr” so‘zining ushbu fanga kirib kelishiga bevosita buyuk ajdodimiz al-Xorazmiyning izlanishlari ham asos bo‘lgan. Hozirgi kunda kelib Internetda mavjud har bir jarayon bevosita kriptografiya bilan chambarchas bog‘liq bo‘lib, ularni chuqur o‘rganish bevosita va bilvosita matematikadan erishgan yutuqlarimiz bilan bog‘liq.

Shu bois, mazkur bobda kriptografiya fanining shakllanishi bilan bog‘liq bo‘lgan asosiy tushunchalar keltirilgan. Kriptografiya yo‘nalishining rivojlanishi natijasida ko‘plab usullar yaratilgan, ularning tasnifi ham ushbu bobdan o‘rin olgan, chunki mavjud usullarni qaysi ketma-ketlikda o‘rganish uchun asos bo‘lib xizmat qiladi.

### **1.1. Kriptografiya tarixi**

Islom dunyosida ilm-fanda o‘rta asrlarda erishilgan yutuqlar albatta kriptografiya sohasini chetlab o‘tib ketishi mumkin emas edi. Shifrlash sohasida yaratilgan va bizgacha yetib kelgan asarlardan biri Abu Bakr Axmad ibn Ali ibn Vaxshiya an-Nabati qalamiga mansub bo‘lib (olimlarning ismlari Internet manbalaridan olingan), u 855-yillarda yaratilgan va qadimiy qo‘lyozmalarni o‘qish muammolariga bag‘ishlangan. Ushbu kitobda ikki alifboli kriptografiya usullari ham yoritilgan va unda har xil shifrlash tizimlari keltirilgan va ular XIX asrlargacha qo‘llanilib kelingan.

Chastotali kriptotahlilga bag‘ishlangan asar 855-yilda yaratilgan va Abu Yusuf al-Kindi qalamiga mansub bo‘lib, unda kriptografik xabarlarni deshifrlash muammolari o‘rganib chiqilgan. Al-Kindining kriptotahlilga bag‘ishlangan qo‘lyozmasi bizgacha yetib kelgan va unda qadimiy xalqlarning alifbosiga asoslangan shifrlash usullari ham berilgan. Al-Kindi yaratgan algoritmlar XIX asrgacha qo‘llanilib kelingan.

Ushbu sohada to‘plangan ma’lumotlar misrlik matematik Shaxob Kalkashandi tomonidan 1412-yilda yozilgan 14 jildlik “Shauba al-Asha” asarida jamlangan. Unda shifrlashning 7 ta usuli bilan birga, deshifrlash masalalari ham ko‘rib chiqilgan. Shu bois Shaxob Kalkashandi kriptografik tahlilning asoschisi sifatida e’tirof etilgan, ammo milliy adabiyotlarda bu haqida nimagadir so‘z yuritilmaydi. Bunda arab tiliga xos statistika va lingvistika qonuniyatlariga asoslanib noma’lum shifrlangan xabarlarni o‘qish yo‘llari keltirilgan. Bu qomusiy asarning ajoyib jihatlaridan biri bu, ilk bor kriptotahlilda chastotali tahlilni qo‘llanilganligidur. Bunday usul orqali oddiy o‘rinlarini almash tirish usullari orqali shifrlangan matnlar o‘qilgan. “Shifr” so‘zining fandagi o‘rni ham ushbu asarlardan kelib chiqqan.

Maxfiy xatlarni o‘qishda qabul qilingan tartib qoidalariga asoslanib tayanch so‘zlar negizida matnni deshifrlash mumkinligiga ilk bor VIII asrda Xalil al-Faraxidi e’tibor bergen. Masalan, xatni biz “salom” so‘zidan boshlaymiz, demak matndagi beshta harfni qanday belgilab olinganligini aniqlash mumkin bo‘ladi. Bu g‘oyani Xalil al-Faraxidi “Kitab al-Maumma” asarida bat afsil yoritib bergen.

## **1.2. Kriptografiya tasnifi**

Kriptografiyaning umum e’tirof etilgan klassik masalasi – bu qandaydir boshlang‘ich matnni, qaysikim ochiq matn deb yuritiladi, qandaydir qoidalar asosida shifrlangan ko‘rinishga o‘tkazishdir. Bunda hosil bo‘lgan belgilarning tasodifiyga o‘xshagan ketma-ketligi shifrmattn yoki kriptogramma deb ataladi. Ochiq matnni oddiy inson tomonidan tushunarsiz holatga o‘tkazish jarayoni esa shifrlash, teskarisi esa deshifrlash atamalari bilan nomlangan. Boshqacha so‘zlar bilan aytganda, shifrlash deganda barcha tomonidan tushuniladigan ochiq ma’lumotlarni shifrlangan ma’lumotlarga (shifrlangan matnga) o‘zgartirishga aytlsa, deshifrlash deganda shifrlangan ma’lumotlarni ochiq ma’lumotlarga o‘zgartiruvchi teskari jarayonga aytildi. Kompyuter va internetning paydo bo‘lishi

ma'lumotlarni shifrlash-deshifrlashning ko'pgina yangi usullarini yaratilishiga olib keldi.

Kriptografiya nuqtayi nazaridan shifr – bu kalit demakdir va ochiq ma'lumotlar to'plamini yopiq (shifrlangan) ma'lumotlarga o'zgartirish algoritmlari majmuasidir. Umumiy holda shifrga quyidagicha ta'rif berish mumkin:

**Shifr** – bu kalitlardan foydalangan holda aniq qoidalar asosida amalga oshiriladigan ochiq (dastlabki) ma'lumotlar to'plamini shifrlangan ma'lumotlar to'plamiga o'girishga qaratilgan o'zgartirishlar majmuasidir.

Shifr bilan bog'langan kalitni esa quyidagicha ta'riflash mumkin:

**Shifrlash kaliti** – bu shifrlash va deshifrlash amallarini boshqaruvchi belgilar ketma-ketligi bo'lib, bevosita kriptografik o'zgartirishlar algoritmining ba'zi-bir parametrarinining maxfiy holati hisoblanadi va barcha algoritmlardan yagona variantni tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy ko'rsatgich bo'lib kriptomustahkamlik (ba'zi adabiyotlarda kriptobardoshlilik) hisoblanadi.

**Kriptomustahkamlik** – bu shifrning kriptotahlilga, ya'ni deshifrlashga bo'lgan bardoshliligi (turg'unligi va chidamliligi bular sinonim sifatida ko'riladi) shunday bo'lishi lozimki, uning fosh etilishi faqatgina kalitlarning to'liq saralash masalasini yechish orqaligina amalga oshirilishi mumkin bo'lsin.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo'yiladi:

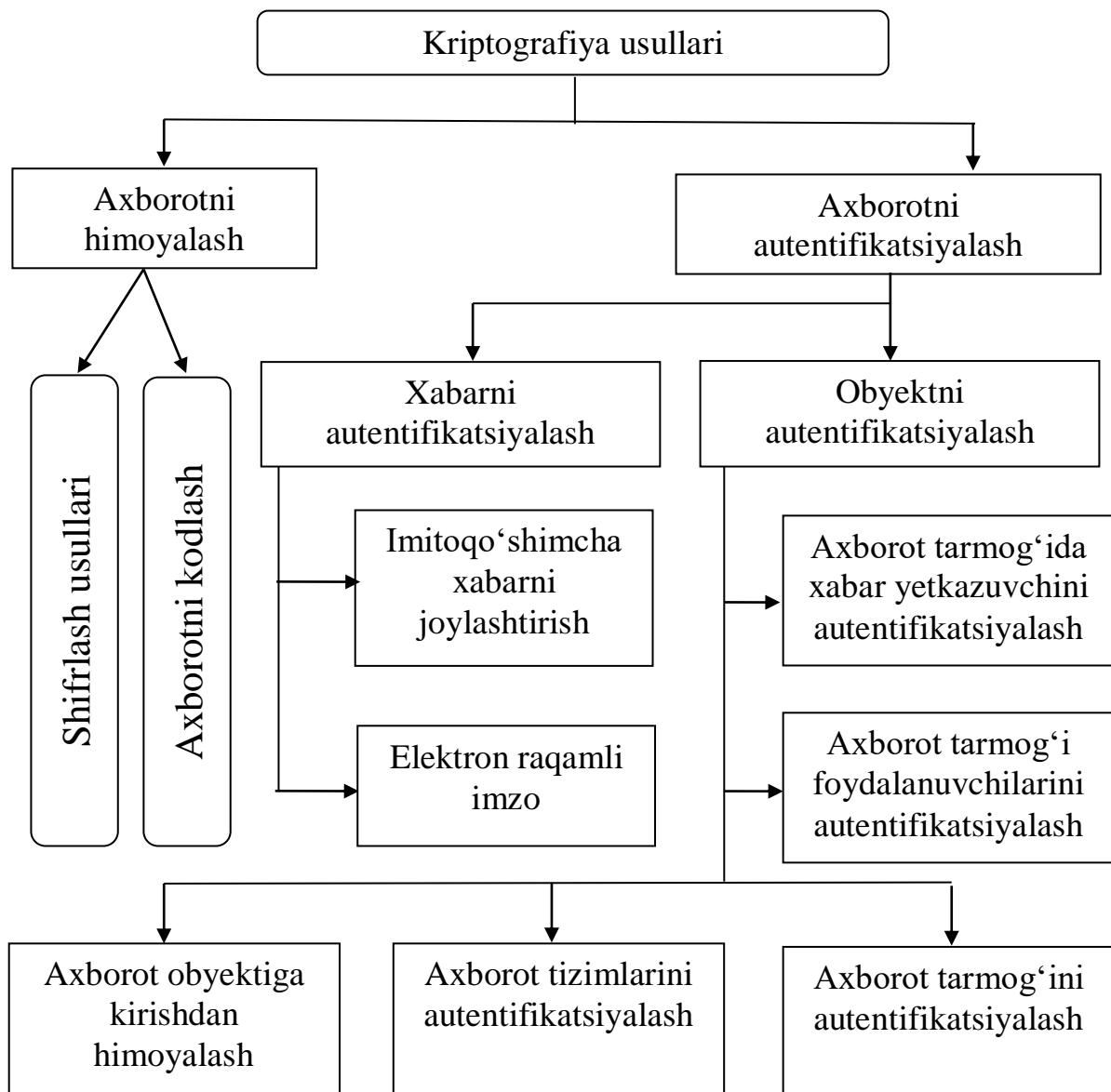
- yetarli darajada kriptomustahkamlik;
- shifrlash va qaytarish jarayonining oddiyligi va ko'p vaqt talab qilmasligi;
- axborotlarni shifrlash oqibatida ularning hajmi ortib ketmasligi;
- shifrlashdagi kichik xatolarga ta'sirchan bo'lmasligi, ya'ni xatoliklar axborotning buzilishiga va yo'qolishiga olib kelmasligi kerak.

Zamonaviy kriptografiya bevosita shifrlash algoritmining maxfiyligini emas, balkim kalitning maxfiyligini ta'minlashga qaratilgan.

Kriptografiya usullarining xilma-xilligi va ularning keng rivojlanishi bevosita ushbu usullarni tizimli o'rganishni talab qiladi. Hozirgi kunda ilk qadamlarni milliy adabiyotlarda ham uchratish mumkin, ammo tasnif to'liq berilmagan. Ma'lumki, tasniflash deyilganda ma'lum bir alomatlar bo'yicha obyektlarni

tartibga solish tushuniladi. Umumiyl holda bajariladigan vazifalaridan kelib chiqqan holda kriptografiya usullarini, bir-biridan keskin farqlanuvchi ikki toifaga ajratish mumkin (1-rasm):

- Axborotni himoyalash vazifasini ta'minlovchi usullar;
- Axborotni haqiqiyligini ta'minlovchi autentifikatsiya usullari.



1-rasm. Kriptografiya usullarining tasnifi.

Axborotni himoyalash vazifasini ta'minlovchi usullar o'z navbatida ikki yo'naliishga bo'linadi: axborotni shifrlash va kodlash usullari.

Axborotni shifrlash orqali yaratilgan shifrogramma bevosita qayta tiklanishi mumkin va bunda ushbu jarayon asosiy boshlang'ich axborotga bog'liq bo'lmaydi

va deshifrlash deb nomlanadi. Shifrlash usullarining tasnifini alohida keyinroq keltiramiz (2-rasm).

Axborotlarni maxfiyligini ta'minlash kriptografik kodlash tizimlari hisoblanadi. Umumiyl holda kriptotizimlar usullarida kalitdan foydalanib yaratilgan kriptogramma bevosita boshlang'ich axborotga bog'liq bo'ladi.

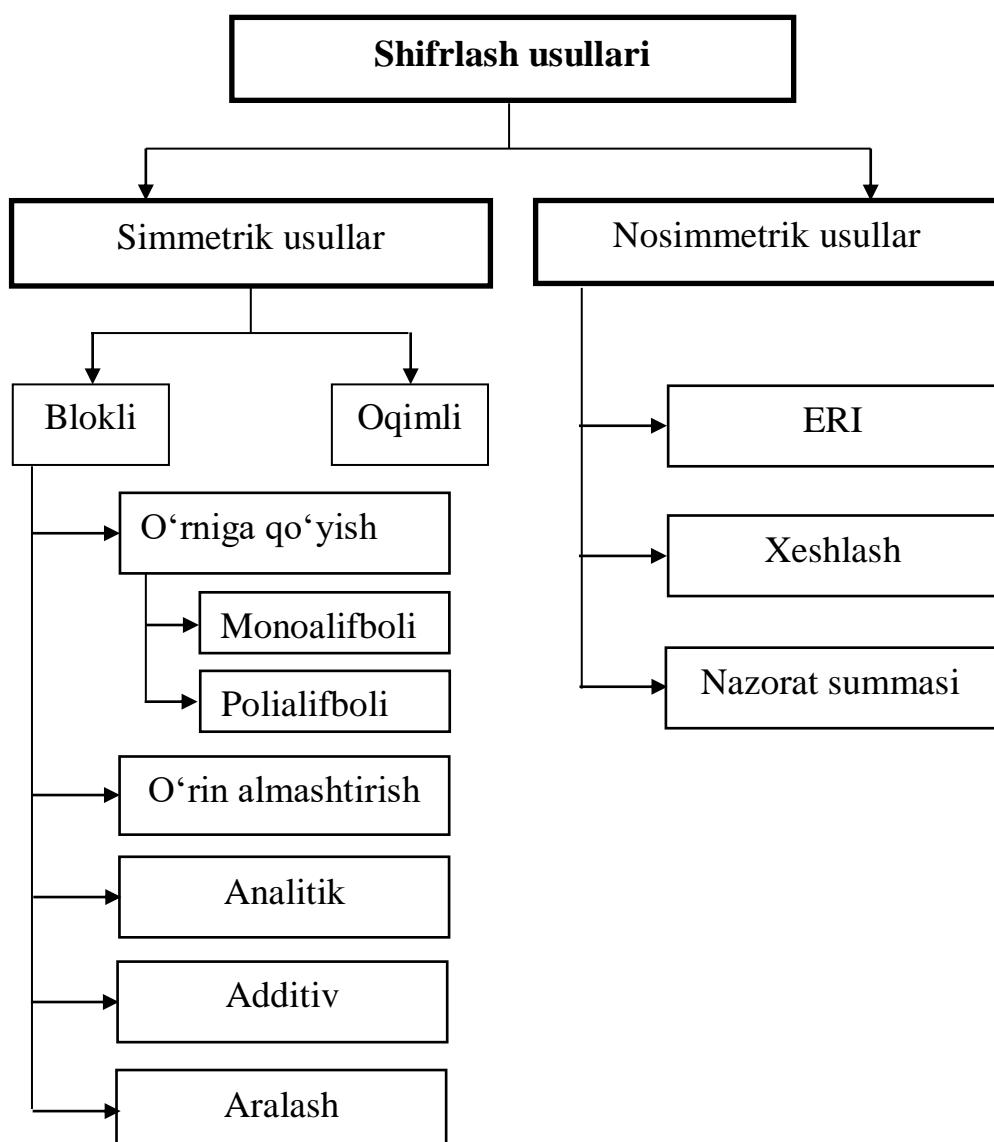
Axborotni autentifikatsiyalash kriptotizimlari bevosita axborotning haqiqiyligini nazorat qilishda qo'llaniladi. Shu bilan birga axborotni butunligini nazorat qilishda ham samarali hisoblanadi. Axborotni autentifikatsiyalash usullarini o'z navbatida ikki yo'nalishga ajratish mumkin. Qo'yilgan masaladan kelib chiqqan holda xabarni yoki obyektni autentifikatsiyalashga taqsimlanadi. Xabarni autentifikatsiyalash bevosita axborotni haqiqiyligini ta'minlashga qo'yilgan shartlarga bog'liq bo'ladi. Masalan, axborotni jo'natuvchi va qabul qiluvchilar bir-biriga shartsiz ishonch bildirgan bo'lsa, bunda faqatgina tashqi obyekt tomonidan xabarda o'zgarishlar sodir bo'lishi mumkin. Bunday vaziyatlarda shifrlangan xabarga qo'shimcha ma'lumot qo'shiladi. Qo'shimcha ma'lumot bevosita asosiy ochiq axborotdan va kalitdan maxsus qabul qilingan algoritm orqali shakllanadi va imitoqo'shimcha deb nomlanadi (ingl. imitoinsert). Rossiyada ushbu yondashuv GOST 28147-89 standartida amalga oshirilgan va imitovstavka deb nomlangan.

Shifrlangan xabarni qabul qiluvchi bevosita axborotni tiklaydi va kalitdan foydalanib imitoqo'shimchani tiklaydi, agar tiklangan ma'lumot unga ma'lum bo'lganiga mos kelsa, demak axborotga o'zgarishlar kiritilmaganligiga ishonch paydo bo'ladi. Ammo, axborotni jo'natuvchi va qabul qiluvchilar bir-biriga ishonch bildirishmasa, unda imitoqo'shimcha samarasiz bo'ladi. Bunda faqatgina elektron raqamli imzodan foydalanish tavsiya etiladi. Bunday usulda axborotni jo'natuvchi bajargan ishni uni qabul qiluvchi tomonidan bajarib bo'lmaydi va teskarisi, chunki ular har xil kalitdan foydalanishadilar. Shu bois bunday yondashuv har xil autentifikatsiya jarayonlarida keng qo'llaniladi.

Axborotga (obyektga) kirishdan himoyalashda ham umuman olganda yuqorida qayd qilingan usullar aralashmasidan foydalanish kuzatilmoxda. Shu bois uni alohida sinfga ajratish mumkin.

Shifrlash usullarini faqatgina sanab o‘tish yetarli emas, hozirgi kunda ushbu usullarni ikki toifaga ajratish qabul qilingan: simmetrik va nosimmetrik usullar. Shundan kelib chiqqan holda kriptografiya usullarini tasniflashda bevosita usullarning mohiyatidan kelib chiqqan holda bajarish maqsadga muvofiq bo‘ladi.

Shifrlash usullarini tasniflashda asosan simmetrik va nosimmetrik usullar ko‘rib chiqiladi, ammo bunda simmetriya alomati faqatgina kalit orqali belgilanadi. Bunday yondashuvda keltirilgan usullarni aniq tasniflash mumkin bo‘lmay qoladi.



2-rasm. Shifrlash usullarining tasnifi.

Birinchidan, umuman kalitsiz usullar ham mavjud, masalan, xeshlash usullarining kalitsiz va bir kalitli variantlari ham mavjud.

Ikkinchidan, nazorat summasini hisoblash orqali himoyalash usullari umuman chetda qolib ketadi. Shu bois, bu yerda tasniflash uchun simmetriya alomati faqatgina kalit orqali emas, balkim algoritmni qayta qo'llash orqali matnni tiklash mumkinligini asos qilib olamiz. Natijada, shifrlash usullarini turli alomatlar bo'yicha, yuqoridagi 2-rasmda keltirilgandek, tasniflanish mumkin bo'ladi.

Mazkur qo'llanmada faqatgina simmetrik usullar ko'rib chiqilishi sababli nosimmetrik usullar to'liq keltirilmagan.

Keltirilgan usullarga quyidagicha qisqa ta'riflar berish mumkin:

**O'rniga qo'yish** usullari – bu shifrlash usuli bo'yicha boshlang'ich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.

**O'rin almashtirish** usuli – bu shifrlash usuli bo'yicha boshlang'ich matn belgilarining matnning ma'lum bir qismi doirasida maxsus qoidalar yordamida o'rinlari almashtiriladi.

**Additiv** usullari bo'yicha boshlang'ich matn belgilari shifrlash gammasi belgilari, ya'ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

**Analitik** usullari bo'yicha boshlang'ich matn belgilari analitik formulalar yordamida o'zgartiriladi, masalan, vektorni matritsaga ko'paytirish yordamida. Bu usulda vektor matndagi belgilar ketma-ketligi bo'lsa, matritsa esa kalit sifatida xizmat qiladi.

Shunday qilib axborotni himoyalash masalasi bevosita kriptografiya usullari bilan bajarilishi mumkin. Kriptografiya sohasiga mansub usullar mazkur qo'llanmadan o'rin olgan. Har bir usul aniq misollar bilan tushuntirib berilgan va mustaqil ishlar uchun topshiriqlar keltirilgan.

## **2-bob. KRIPTOGRAFIYANING MATEMATIK ASOSLARI**

Kriptografiya fanining ustunlaridan biri bu, albatta, algebra hisoblanadi. Ushbu tushunchaning kelib chiqishi bevosita matematika bilan bog‘liq bo‘lib, hozirgi kunda keng ko‘lamli qo‘llanish sohalaridan iborat. Algebra fanining asoschisi IX asrda yashagan matematik va astronom Muhammad ibn Muso al-Xorazmiyning “Al-jabr va al-muqobala” asarining ta’sirida vujudga kelgan. “Algebra” atamasi ham aynan asarning nomidan olingan. Shu bilan birga “Algoritm” tushunchasi ham olimning ismlaridan kelib chiqqan. Bu ham hozirgi kunda eng keng qo‘llanilayotgan tushunchalardan biri hisoblanadi.

Keyingi vaqtarda kriptografiyada algebra usullaridan foydalanib muhim ixtiolar qilingan. Shu bilan birga algebraning boshqa fanlarda ham muhim tatbiqlari mavjud, masalan fizikada, informatikada va iqtisodiy izlanishlarda.

Mazkur bobda aynan matematikada mavjud tushunchalar bilan bog‘liq bo‘lgan ma’lumotlar o‘rganilgan va misollar bilan boyitilgan. Ammo, bu yerda keltirilgan tushunchalar oddiy bo‘lib, faqatgina “Kriptografiya 1” doirasida zarur bo‘lgan asosni belgilab beradi.

### **2.1. Sanoq tizimlari va bitlar arifmetikasi**

Sonlarni tasvirlashda ishlataladigan belgilar va qoidalar to‘plamiga sanoq tizimi deb ataladi. Belgilar to‘plami sanoq tizimining alifbosi deyiladi. Amaliyotda ikki xil, yani pozitsion va nopoziitsion sanoq tizimlari qo‘llaniladi.

Sonlarning qiymati undagi raqamlarining sonda joylashgan o‘rniga qarab belgilanadigan sanoq tizimi pozitsion sanoq tizimi deb ataladi. Masalan, o‘nlik sanoq tizimida o‘nta  $0,1,2,3,4,5,6,7,8,9$  raqamlaridan foydalaniladi, demak uning alifbosi  $T_{10}=\{0,1,2,3,4,5,6,7,8,9\}$  va  $52,25,255$  sonlarini tasvirlanishida 2 va 5 raqamlaridan foydalanilsada bu sonlarning qiymati turlichadir.

Raqamlarning qiymati ularni sonda joylashgan o‘rniga bog‘liq bo‘lmassa, bunday sanoq tizimi nopoziitsion sanoq tizimi deyiladi. Masalan, Rim sanoq tizimi nopoziitsion sanoq tizimiga misol bo‘la oladi. Misol uchun, 20 soni bu tizimda quyidagicha yoziladi **XX**, ya’ni tegishli belgi sonni qanday o‘rinda turishidan qat’iy nazar har doim bir xil qiymatni ifoda etadi. Ushbu sanoq tizimi

hozirgi paytda turli tarixiy sanalarni yozishda, kitob boblarini, soat raqamlarini belgilashda qo'llaniladi.

Pozitsion sanoq tizimining nopoziitsion sanoq tizimidan qulaylik tomoni shundaki, unda katta sonlarni qisqa qilib yozish mumkin. Pozitsion sanoq tizimida istalgan son raqamlar ketma-ketligida yoziladi, butun va kasr qismi vergul bilan ajratiladi. O'z navbatida pozitsion sanoq tizimi ham turli sanoq tizimlariga bo'linadi va ulardan ayrimlari kompyuterlarda keng qo'llaniladi.

Pozitsion sanoq tizimida sonni yozish uchun qo'llaniladigan turli raqamlarning soni  $d$ -sanoq tizimining asosi deb aytildi va aksincha sanoq tizimini  $d$  asosi shu sanoq tizimida qatnashadigan raqamlar sonini bildiradi. Biroq, hech bir sanoq tizimida uning asosi  $d$  ga teng bo'lgan raqam ( $A_i$ ) qatnashmaydi, ya'ni doimo quyidagi tengsizlikning bajarilishi shartdir:

$$0 \leq A_i < d,$$

bu yerda, masalan, agarda  $d = 2$  bo'lsa,  $A_i = 0$  yoki 1 bo'lishi mumkin.

Umumiy holda pozitsion sanoq tizimda  $d$ -asosli istalgan  $A$  sonni darajali qatorning yig'indisi ko'rinishida quyidagicha tasvirlash mumkin:

$$A_{(d)} = A_m d^m + A_{m-1} d^{m-1} + \dots + A_1 d^1 + A_0 d^0 + A_{-1} d^{-1} + \dots, \quad (*)$$

bu yerda

$d$  - sanoq tizimining asosi,  $m + 1$  – xonalar soni,  $A_m$  -  $m$ -xonada turuvchi koeffitsiyent.

$A_{(d)}$  yozuvida sanoq tizimining asosi  $d$  qavslarda indeks ko'rinishida yoziladi. O'nlik sanoq tizimi bundan mustasno.

$A_{(d)}$  sonini yuqoridagi formulaga mos keluvchi ko'rinishdagi qisqartirilgan yozuvini raqamlar ketma-ketligi ko'rinishida quyidagicha yozish qabul qilingan:

$$\mathbf{A}_{(d)} = A_m \mathbf{A}_{m-1} \dots \mathbf{A}_1 \mathbf{A}_0, \mathbf{A}_{-1} \dots \mathbf{A}_{-m}$$

Bu ketma-ketlikda sonning butun qismi bilan kasr qismi vergul bilan ajratiladi. Agar manfiy darajalar bo'lmasa vergul tushirib yuboriladi. Verguldan boshlab sanaladigan raqamlar o'rni xona deyiladi. Masalan, 811 soni uch xonali. Xonalar soni, masalan  $m$  uchun, unda ko'pi bilan nechta har xil sonni tasvirlash mumkinligi quyidagi formula orqali aniqlanadi:

$$N(m)=d^m.$$

Masalan, o‘nlik sanoq tizimida  $m=3$  bo‘lsa, demak  $N=10^3=1000$ . Haqiqatan ham, uch xonali sonlar 000 dan boshlanib 999 bilan tugaydi, demak hammasi bo‘lib 1000 ta har xil son mavjud bo‘ladi.

Pozitsion tizimda  $d$  asosli sonning har bir raqam qiymati undan o‘ng tomonda bo‘lgan qo‘shni xonadagi qiymatidan katta hisoblanadi.

Kompyuterlarda o‘nli bo‘lmagan pozitsion sanoq tizimlari: ikkilik, sakkizlik, o‘n otililiklar sanoq tizimlari ham qo‘llaniladi.

Ikkilik sanoq tizimida faqat ikkita 0 va 1 raqamlaridan foydalaniladi, demak uning alifbosi  $T_2=\{0,1\}$ .

Ikkilik sanoq tizimidan foydalanishga, misol sifatida, ASCII (American Standart Code for Information Interchange) jadvalini keltirish mumkin. Bunda ikkilik kodlash orqali har bir raqam va alifbodagi belgilar ikkilik belgilar ketma-ketligida ifodalanadi. ASCII jadvali yordamida ayrim lotin alifbosidagi bosh harf belgilarining ikkilik tizimidagi kodlarini misol sifatida keltiramiz:

A – 01000001	H – 01001000	O – 01001111	V – 01010110
B – 01000010	I – 01001001	P – 01010000	W – 01010111
C – 01000011	J – 01001010	Q – 01010001	X – 01011000
D – 01000100	K – 01001011	R – 01010010	Y – 01011001
E – 01000101	L – 01001100	S – 01010011	Z – 01011010
F – 01000110	M – 01001101	T – 01010100	
G – 01000111	N – 01001110	U – 01010101	

Kriptografiya usullari asosan ushbu alifbo misolida o‘rganib chiqiladi.

Kompyuterda o‘nli songa nisbatan ikkilik sonini tasvirlash uchun ko‘proq xonalar talab etiladi. Shunga qaramasdan ikkilik tizimini qo‘llash kompyuterni loyihalash va ishlatish uchun ko‘proq qulaylik tug‘diradi, chunki kompyuterda ikkilik sonini tasvirlash uchun istalgan sodda faqat ikki turg‘un holatdan birini ifodalovchi elementlardan foydalanishi mumkin. Ikkilik tizimini boshqa afzalligiga uning ikkilik arifmetikasining soddaligini aytish kifoyadir. Sakkizlik

sanoq tizimida sakkizta 0,1,2,3,4,5,6,7 raqamlari ishlataladi, demak  $T_8=\{0,1,2,3,4,5,6,7\}$ .

O‘noltilik sanoq tizimida sonni tasvirlash uchun 16 ta ya’ni 0 dan boshlab 15 gacha bo‘lgan raqamlar foydalaniladi. Ammo bitta raqamni ikkita belgi bilan ifodalamaslik maqsadida 9 dan katta sonlar uchun maxsus belgilar kiritiladi. Dastlabki o‘nta raqamni 0 dan 9 gacha bo‘lgan raqamlar bilan, so‘nggi katta sonlarni esa lotin harflari, ya’ni o‘nni - A, o‘n birni - B, o‘n ikkini - C, o‘n uchni - D, o‘n to‘rtni - E, o‘n beshni - F bilan belgilaymiz, demak  $T_{16}=\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$ .

Sanoq tizimining asosi kamayishi bilan bitta songa ajratilgan xonalar soni oshib boradi.

Odatda axborotlarni kompyuterda qayta ishlash uchun ular kompyuterga o‘nlik sanoq tizimida kiritiladi, natija ham o‘nlik sanoq tizimida chiqarib beriladi. Biroq axborotlar kompyuterda boshqa sanoq tizimlarida qayta ishlanadi.

Sonlarni bir sanoq tizimidan boshqasiga o‘tkazishni kompyuterning o‘zi quyida keltiriladigan qoidalarga muvofiq ravishda maxsus dasturlar asosida avtomatik tarzda bajaradi.

Sanoq tizimlari			
O‘nlik	Sakkizlik	Ikkilik	O‘n otililik
0	0	000	0
1	1	001	1
2	2	010	2
3	3	011	3
4	4	100	4
5	5	101	5
6	6	110	6
7	7	111	7
8	10	1000	8
9	11	1001	9
10	12	1010	A
11	13	1011	B
12	14	1100	C
13	15	1101	D
14	16	1110	E
15	17	1111	F

Sonni  $d_1$ -asosli sanoq tizimidan  $d_2$ -asosli sanoq tizimiga o'tkazishni ikki xil qoidasi bir-biridan farq qiladi.

Agar  $d_1 < d_2$  bo'lsa, u holda sonni  $d_1$  - asosli sanoq tizimidan  $d_2$ - asosli sanoq tizimiga o'tkazish uchun o'tkaziladigan son (\*) formulaga asosan yoyib chiqiladi va so'ng qator yig'indisi hisoblanadi. Ushbu jarayonda barcha arifmetik amallar  $d_2$ - asosli sanoq tizimining qoidalari bo'yicha amalga oshiriladi.

**Misol.** 100101<sub>(2)</sub> sonini o'nli sanoq tizimiga o'tkazamiz.

$$100101_{(2)} = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 32 + 4 + 1 = 37.$$

Natija: 100101<sub>(2)</sub> = 37.

Keltirilgan qoida asosida, juda osonlik bilan ikkilik va sakkizlik tizimidagi sonlarni o'nlik sanoq tizimiga o'tkazish mumkin. Biroq, yuqoridagi qoidadan farqli ravishda ikkilik tizimidagi sonni sakkizlik tizimiga ham o'tkazish mumkin. Buning uchun (\*) qator yig'indisini hisoblashni sakkizlik arifmetika qoidasiga asosan bajarish kerak bo'ladi.

Agar  $d_1 > d_2$  bo'lsa, u holda butun va kasr sonlarini bir sanoq tizimidan boshqasiga o'tkazishning quyidagi qoidalardan foydalaniladi. Ya'ni  $d_1$ -asosli sanoq tizimidagi butun sonni  $d_2$ -asosli sanoq tizimiga o'tkazish uchun u o'tkaziladigan sanoq tizimining asosi  $d_2$  ga ketma-ket bo'linadi. O'tkaziladigan son va bo'linmani bo'lish toki oxirgi qoldiq  $d_2-1$  dan kichik yoki unga teng bo'lguncha davom ettiriladi.  $d_2$ -tizimidagi yangi son bo'lish natijasida hosil bo'lgan qoldiq va oxirgi bo'linmalarni teskari yo'nalishida yozish bilan o'qiladi. Oxirgi bo'linma yangi sonning birinchi raqamini beradi. Barcha amallar dastlabki son berilgan  $d$  - asosli sanoq tizimida bajariladi. Yangi son asosi eski  $d_1$ - asosli tizim raqamlari bilan yoziladi.

Kasr sonlarni bir sanoq tizimidan boshqa sanoq tizimiga o'tkazish uchun o'tkaziladigan  $d_1$ - tizimidagi sonni o'tkazishimiz kerak bo'lgan  $d_2$ - tizimining asosiga ketma-ket ko'paytiramiz va har bir ko'paytirishimizdan so'ng uning butun qismini ajratamiz.  $d_2$ - tizimidagi yangi son (verguldan keyin) ko'paytmalarning butun qismlarining ketma-ketligi ko'rinishida yoziladi. Ko'paytirish to

ko‘paytmani kasr qismida nollar hosil bo‘lgunga qadar yoki oldindan ko‘zda tutilgan aniqlik bajarilgunga qadar davom ettiriladi. Kasr sonni yangi  $d_2$ -tizimidagi birinchi ajratilgan butun qismidan boshlab oxirgi butun qismiga pastga qarab o‘qiladi. Hisoblashlar o‘tkazilayotgan son yozilgan sanoq tizimida amalga oshiriladi.

**Misol :** 13 sonini o‘nlik sanoq tizimidan ikkilik sanoq tizimiga o‘tkazamiz.

$$\begin{array}{r}
 -\frac{13}{12} \quad | \quad \frac{2}{6} \\
 \underline{-\frac{12}{1}} \quad | \quad \underline{\frac{2}{3}} \quad | \quad \frac{2}{1} \\
 \underline{\underline{0}} \quad | \quad \underline{\underline{2}} \quad | \quad \underline{\underline{1}}
 \end{array}$$

Natija:  $13_{(10)} = 1101_{(2)}$ .

Sonni sakkizlik sanoq tizimidan ikkilik sanoq tizimiga o‘tkazish uchun sakkizlik raqamlarini ikkilikdagi sonlar bilan almashtirib yozish mumkin, chunki sakkizlik sanoq tizimining asosi 2 darajasi 3 ga teng. Ushbu texnologiya o‘noltilik sanoq tizimiga ham taaluqli. Bu yerda ko‘pincha triada va tetrada so‘zlari ishlatiladi. Triada deganda sakkizlik raqamini ifodalaydigan uch xonali ikkilik son tushuniladi. Tetrada deganda o‘nli raqamni ifodalaydigan to‘rt xonali ikkilik son tushuniladi. Bundan foydalananib, yuqorida keltirilgan sanoq tizimlari jadvali asosida juda osonlik bilan quyidagilarni bajarish mumkin

$$11\ 0111\ 1100_{(2)} = 37C_{(16)},$$

$$110\ 1111\ 1001_{(2)} = 4F9_{(16)},$$

$$10\ 100\ 010_{(2)} = 242_{(8)},$$

$$110\ 101_{(2)} = 65_{(8)}.$$

Ikkilik sanoq tizimida arifmetik amallarni bajarish tartibi quyidagi jadvalda keltirilgan:

$$0+0=0 \quad 0+1=1 \quad 1+0=1 \quad 1+1=10$$

$$0\cdot 0=0 \quad 1\cdot 0=0 \quad 0\cdot 1=0 \quad 1\cdot 1=1$$

Sakkizlik sanoq tizimida qo'shish arifmetik amalini bajarish tartibi esa quyidagi jadvalda keltirilgan:

0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	10
2	3	4	5	6	7	10	11
3	4	5	6	7	10	11	12
4	5	6	7	10	11	12	13
5	6	7	10	11	12	13	14
6	7	10	11	12	13	14	15
7	10	11	12	13	14	15	16

Arifmetik amallarni bajarishni yengillashtirish maqsadida maxsus kodlar ham kiritilgan: teskari kod va qo'shimcha kod. Teskari kod ikkilik sonda 0 ni 1 ga va 1 ni 0 ga almashtirish yo'li bilan olinadi. Qo'shimcha kod esa teskari kodga 1 ni qo'shish bilan topiladi. Misol :

$$01111_{(2)} \rightarrow (\text{teskari}) \ 10000_{(2)} + 1 \rightarrow (\text{qo'shimcha}) \ 10001_{(2)}$$

Ko'pgina amaliy masalalarda uchlik va to'qqizlik sanoq tizimlaridan foydalanishga to'g'ri keladi. Shu bois ushbu tizimdagagi o'zaro bog'liqliknini quyidagi jadvalda keltiramiz

O'nlik	Uchlik	To'qqizlik
0	00	0
1	01	1
2	02	2
3	10	3
4	11	4
5	12	5
6	20	6
7	21	7
8	22	8
9	100	10

Yuqorida keltirilgan ma'lumotlar asosida bevosita bitlar bilan arifmetik amallarni bajarish mumkin bo'ladi. Ammo kompyuter arifmetik amallardan

tashqari mantiqiy amallarni ham bajarish imkoniga egadir. Kriptografiya fanida bu amallarni ishini va ularning qo'llanilishini bilish foydalidir. Ularning soni dasturlash tillariga bog'liq bo'lib, bu yerda asosan quyidagilarni to'laroq o'rGANIB chiqamiz.

- **And** – mantiqiy ko'paytirish;
- **Not** – mantiqiy inkor;
- **Or** – mantiqiy qo'shish;
- **Xor** – mantiqiy qo'shishni inkor etish.

**And** amali ikkita ifodani mantiqiy ko'paytirish uchun ishlatiladi. Bu yerdan quyidagi ta'rifni berish mumkin. Mantiqiy ko'paytirish bu ikki ifoda bir paytda rost bo'lgandagina natija rost bo'ladigan amaldir.

**And** amali sonning bitlarini tekshirish uchun ham ishlatilishini unutmaslik lozim. Bitlar uchun **And** amalining ishlashi quyidagi jadvaldagi qonuniyatlarga amal qiladi:

1-bit	2-bit	Natija
0	0	0
0	1	0
1	0	0
1	1	1

**And** amaliga doir misollar quyida keltirilgan:

A	B	C	Mantiqiy ifoda	Natija
			$A > B \text{ And } B > C$	True
			$B > A \text{ And } B > C$	False
10	8	6	$A \text{ And } B$	8

Birinchi misolni ko'rib chiqamiz. Bu yerda  $A > B$  va  $B > C$  tengsizliklar bajarilayapti, shu bois ularning qiymatlari **True** bo'ladi va o'z navbatida natija ham **True** bo'ladi. Xuddi shu yo'l bilan ikkinchi misol natijasi ham isbotlanadi. Lekin 3-misoldagi natijani aniqlash uchun A va B larni ikkilik sanoq tizimiga o'tkazamiz va yuqoridagi jadval bo'yicha har bir bit uchun amallarni bajaramiz

A	10	1010
B	8	1000
<b>And</b>		1000

Bu yerdagi natija  $1000_{(2)}$  o‘nlik sanoq tizimida 8 ga teng bo‘ladi.

Mantiqiy qo‘shish **Or** amali ikkita ifodani mantiqiy qo‘shish uchun ishlataladi. Bunda quyidagi ta’rif berilgan: Mantiqiy qo‘shish bu ikki ifodadan kamida bittasi rost bo‘lganda natija rost bo‘ladigan amaldir.

**Or** amalining ishlashi quyidagi jadvaldagi qonuniyatlarga amal qiladi:

1-bit	2-bit	Natija
0	0	0
0	1	1
1	0	1
1	1	1

**Or** amaliga doir misollar quyida keltirilgan.

A	B	C	Mantiqiy ifoda	Natija
10	8	6	$A > B \text{ Or } B > C$	True
10	8	6	$B > A \text{ Or } B > C$	True
10	8	6	$A \text{ Or } 5$	15

Birinchi misolni ko‘rib chiqamiz. Bu yerda  $A > B$  va  $B > C$  tengsizliklar bajarilayapti, shu bois ularning qiymatlari **True** bo‘ladi va o‘z navbatida yuqoridagi jadvalga binoan natija ham **True** bo‘ladi. Xuddi shu yo‘l bilan ikkinchi misol natijasi ham isbotlanadi. Lekin 3-misoldagi natijani aniqlash uchun A va B larni ikkilik sanoq tizimiga o‘tkazamiz va yuqoridagi jadval bo‘yicha har bir bit uchun amallarni bajaramiz:

A	10	1010
B	5	0101
<b>Or</b>		1111

Mantiqiy qo‘shishni inkor etish **Xor** amali ikkita ifodani mantiqiy inkor etish uchun ishlataladi. Bunda quyidagi ta’rif beriladi: Mantiqiy qo‘shishni inkor etish bu ikki ifodadan faqatgina bittasi rost bo‘lsa, natija rost bo‘ladigan amaldir.

**Xor** amalini qanday ishlashi quyidagi jadvalda keltirilgan:

1-bit	2-bit	Natija
0	0	0
0	1	1
1	0	1
1	1	0

**Xor** amali **Or** dan shu bilan farq qiladiki, unda ikkala bit ham bir bo‘lsa, **Xor** amali **0** natijani beradi. **Xor** amali yana shu bilan qiziqarlik, agar u ikki marta qo‘llanilsa, berilgan sonni natija sifatida chiqaradi. **Xor** amaliga doir misollar quyida keltirilgan:

A	B	C	Mantiqiy ifoda	Natija
10	8	6	$A > B \text{ Xor } B > C$	False
10	8	6	$B > A \text{ Xor } B > C$	True
10	8	6	$B > A \text{ Xor } C > B$	False
10	8	6	$A \text{ Xor } B$	2

Bu yerda ham keltirilgan misollar deyarli tushunarli, faqatgina oxirgi misolni batafsil ko‘rib chiqamiz

A	10	1010
B	8	1000
<b>Xor</b>		0010

Ikkita sonli o‘zgaruvchilarning qiymatlarini almashtirishda **Xor** amalining qo‘llanilishi misoli juda qiziqarli hisoblanadi:

```

A:=4
B:=7
A:=A xor B
B:=A xor B
A:=A xor B

```

Bu amallar ketma-ket bajarilishi natijasida A o‘zgaruvchi B o‘zgaruvchining qiymatiga ega bo‘ladi va aksincha, ya’ni  $A=7$  va  $B=4$  bo‘ladi.

Mantiqiy inkor **Not** amali bu berilgan ifoda rost bo‘lganda yolg‘on, yoki ifoda yolg‘on bo‘lganda natija rost bo‘ladigan amaldir.

**Not** amali «ifoda»ning barcha bitlarini teskarilashtiradi, ya’ni 0 ni 1 ga va 1 ni 0 ga aylantiradi. **Not** operatoriga doir misollar quyida keltirilgan:

A	B	C	Mantiqiy ifoda	Natija
10	8	6	Not ( $A > B$ )	False
10	8	6	Not ( $B > A$ )	True
10	8	6	Not A	-11

Shunday qilib, barcha bitlar bilan bajariladigan amallarni yagona jadvalda joylashtiramiz.

A	B	$A \text{ or } B$ $A \vee B$	$A \text{ and } B$ $A \wedge B$	$A \text{ xor } B$ $A \oplus B$	$\text{not } A$ $\neg A$
0	0	0	0	0	1
1	0	1	0	1	0
0	1	1	0	1	1
1	1	1	1	0	0

Shu o‘rinda ushbu amallar bilan bog‘liq ifodalarda ma’lum-bir qonuniyatlar mavjud bo‘lib, ularni quyidagi jadvalda jamlab keltiramiz:

Qonuniyat	Formula
Kommutativlik qonuni	$A \vee B = B \vee A$ $A \wedge B = B \wedge A$
Assotsiativlik qonuni	$(A \vee B) \vee C = A \vee (B \vee C)$ $(A \wedge B) \wedge C = A \wedge (B \wedge C)$
Distributivlik qonuni	$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$ $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
Qarama-qarshilik qonuni	$A \wedge \neg A = 0$
Uchinchisi istisno qonuni	$A \vee \neg A = 1$
Ikka karra inkor qonuni	$\neg(\neg A) = A$
de Morgan qonuni	$\neg(A \vee B) = \neg A \wedge \neg B$ $\neg(A \wedge B) = \neg A \vee \neg B$

### Topshiriqlar

- Quyidagi  $100000_{(2)}$  sonini o‘noltilik sanoq tizimiga o‘tkazing.
- Quyidagi  $10001011_{(2)}$  sonini sakkizlik sanoq tizimiga o‘tkazing.
- Quyidagi  $ABCD_{(16)}$  sonini ikkilik sanoq tizimiga o‘tkazing va birlar sonini aniqlang.

4. Quyida keltirilgan ikkilik sanoq tizimida yozilgan juft songa 0 va toq songa 1 qiymat berish natijasidan hosil bo‘lgan sonni aniqlang:

$$11101_{(2)} \quad 1000_{(2)} \quad 1010_{(2)} \quad 111_{(2)} \quad 101010_{(2)}$$

5. Quyidagi  $888_{(9)}$  sonini uchlik sanoq tizimiga o‘tkazing.

6. Quyidagi  $723_{(8)}$  sonini o‘noltilik sanoq tizimiga o‘tkazing.

7. Ushbu ketma-ketlikdagi 12, 21, 100, 102 sonlarni nima birlashtiradi?

8. Qaysi sanoq tizimida quyidagi  $21+24=100$  tenglik bajarilishini aniqlang.

9. Agar ikki xonali  $N$  natural soni  $x$  asosli sanoq tizimiga mansub bo‘lsa va  $M$  o‘nlik sanoq tizimidagi son bo‘lsa, unda quyidagi  $N_{(x)}=M$  tenglamani yechimini toping.

10. Quyidagi  $3FFFF_{(16)}$  sonini ikkilik sanoq tizimiga o‘tkazing va birlar sonini aniqlang.

11. Quyida keltirilgan uchlik sanoq tizimida yozilgan son uchga bo‘linsa 0 va aksincha 1 qiymat berish natijasida hosil bo‘lgan sonni aniqlang:

$$1102_{(3)} \quad 1020_{(3)} \quad 1011_{(3)} \quad 201_{(3)} \quad 11010_{(3)}$$

12. Quyidagi  $1111111_{(2)}$  sonini o‘noltilik sanoq tizimiga o‘tkazing.

13. Quyidagi  $1357_{(9)}$  sonini uchlik sanoq tizimiga o‘tkazing.

14. Quyida keltirilgan yettilik sanoq tizimida yozilgan son 7 ga bo‘linsa 0 va aksincha 1 qiymat berish natijasida hosil bo‘lgan sonni aniqlang:

$$502_{(7)} \quad 1123_{(7)} \quad 4012_{(7)} \quad 250_{(7)} \quad 10006_{(7)}$$

15. Quyida keltirilgan beshlik sanoq tizimida yozilgan son 5 ga bo‘linsa 0 va aksincha 1 qiymat berish natijasida hosil bo‘lgan sonni aniqlang:

$$401_{(7)} \quad 1103_{(7)} \quad 4010_{(7)} \quad 320_{(7)} \quad 1004_{(7)}$$

16. Quyidagi  $512_{(8)}$  sonini o‘noltilik sanoq tizimiga o‘tkazing.

17. Quyidagi ketma-ketlikdagi 1, 1, 10, 11, 101, 1000 sonlarni nima birlashtiradi?

18. Qaysi sanoq tizimida quyidagi  $20+3+22 = 100$  tenglik bajarilishini aniqlang.

19. Quyidagi  $11011011_{(2)}$  sonini sakkizlik sanoq tizimiga o‘tkazing.

20. Qaysi sanoq tizimida quyidagi  $22+44 = 110$  tenglik bajarilishini aniqlang.

21. Quyidagi berilgan mulohazalar  $A=$ ”8 bit 1 baytga teng” va  $B=$ ”1024 bayt 1 Kb ga teng” qanday qiymatga ega va ular ustidagi quyidagi amalni bajaring: A and B

22. Rim sanoq tizimida berilgan quyidagi tengliklarni faqatgina bitta cho‘pchani o‘rnini almashtirish orqali to‘g‘rilab qo‘ying:

$$1) \text{VII} - \text{V} = \text{XI}$$

$$2) \text{IX} - \text{V} = \text{VI}$$

$$3) \text{VI} + \text{I} = \text{III}$$

$$4) \text{VIII} - \text{III} = \text{X}$$

23. Quyidagi berilgan mulohazalar A=”8 bit 1 baytga teng” va B=”1024 bayt 1 Kb dan katta” qanday qiymatga ega va ular ustidagi quyidagi amalni bajaring: A or B

24. Quyidagi ketma-ketlikdagi 21, 20, 12, 11, 10 sonlarini nima birlashtiradi?

25. Quyidagi berilgan mulohazalar A=”1 bayt 10 bitga teng” va B=”1024 bayt 1 Kb dan katta” qanday qiymatga ega va ular ustidagi quyidagi amalni bajaring: A or ( not B) .

26. Quyidagi berilgan mulohazalar A=”0 va 1 ikkilik sanoq tizimi alifbosi” va B=”1024 Kbayt 1 Mb ga teng” qanday qiymatga ega va ular ustidagi quyidagi amalni bajaring: A and ( not B) .

27. Quyidagi berilgan mulohazalar A=”Sakkizlik sanoq tizimi alifbosi 8 ta belgidan iborat” va B=”1024 Mbayt 1 Gb ga teng” qanday qiymatga ega va ular ustidagi quyidagi amalni bajaring: (not A) or (not B) .

28. Aka-ukalar Iskandar, Jahongir, Bahodirlar kelgusida soatsoz, iqtisodchi va o‘qituvchi kasblarini egallahmoqchilar. Kelgusida qaysi kasblarni egallahni istaysizlar degan savolga, aka-ukalardan biri quyidagicha javob qaytaribdi: «Iskandar soatsoz bo‘lishni istaydi, Jahongir soatsoz bo‘lishni istamaydi, Bahodir o‘qituvchi bo‘lishni istamaydi». Keyinchalik ma’lum bo‘lishicha, ushbu javobda faqatgina bitta mulohaza to‘g‘ri bo‘lib, qolgan ikkitasi noto‘g‘ri ekan. Aka-ukalar qaysi kasblarni egallahmoqchi ekanligini aniqlang.

29. Qaysi sanoq tizimida quyidagi  $11 + 22 + 12 = 100$  tenglik bajarilishini aniqlang.

30. Berilgan uchta tillo tangalardan bittasi qalbaki ekan. Qalbaki tanganing boshqa tangalarga nisbatan og‘ir yoki engilligi noma’lum ekan. Oddiy ikki pallali tarozi yordamida qalbaki tangani aniqlaydigan sxemani keltiring.

31. ASCII jadvalida keltirilgan belgilarning kodlari ustida quyidagi amallarni bajarib javobini bitta so‘z bilan yozing:

- a)  $(M \text{ xor } N) \text{ xor } N$       b)  $(I \text{ xor } O) \text{ xor } O$       c)  $(R \text{ xor } D) \text{ xor } D$   
d)  $(Z \text{ xor } I) \text{ xor } I$       e)  $(O \text{ xor } R) \text{ xor } R$

32. Qaysi sanoq tizimida quyidagi  $x^2 - 4x + 1 = -10_{(d)}$  tenglama natural sonlarda yechimga ega bo‘ladi?

33. ASCII jadvalida keltirilgan belgilarning kodlariga 1 ni qo‘shish orqali hosil bo‘lgan harflar javobini bitta so‘z bilan yozing:

- a) E + 1      b) N +1      c) N +1      d) N +1      e) N +1      f) N +1

34. Quyidagi berilgan A=13 va B=12 qiymatlar uchun (A and B) amalini bajaring.

35. ASCII jadvalida keltirilgan belgilarning kodlariga 1 ni qo‘shish va ayirish orqali hosil bo‘lgan harflar javobini bitta so‘z bilan yozing:

- a) Y + 1      b) B - 1      c) G +1      d) S - 1      e) N +1

36. ASCII jadvalida keltirilgan belgilarning kodlariga 1 ni qo‘shish va ayirish orqali hosil bo‘lgan harflar javobini bitta so‘z bilan yozing:

- a) B - 1      b) M - 1      c) H +1

37. ASCII jadvalida keltirilgan belgilarning kodlariga 1 ni qo‘shish va ayirish orqali hosil bo‘lgan harflar javobini bitta so‘z bilan yozing:

- a) S + 1      b) B - 1      c) U - 1      d) V - 1

38. ASCII jadvalida keltirilgan belgilarning kodlari ustida quyidagi amallarni bajarib javobini bitta so‘z bilan yozing:

- a)  $(R \text{ xor } N) \text{ xor } N$       b)  $(A \text{ xor } O) \text{ xor } O$       c)  $(S \text{ xor } D) \text{ xor } D$   
d)  $(U \text{ xor } I) \text{ xor } I$       e)  $(L \text{ xor } R) \text{ xor } R$

39. Asosi (d) bo‘lgan qaysi sanoq tizimlarida quyidagi  $x^2 - 6x + 4 = -10_{(d)}$  tenglama natural sonlarda yechimga ega bo‘ladi? (Javobi: 4 va 5)

40. Quyidagi mantiqiy ifodaning A v (A  $\wedge$  C) qiymatini toping. (Javobi: A)

41. Quyidagi berilgan mulohazalardan 3=”16-lik sanoq tizimi alifbosi 15 ta belgidan iborat”, 5=”Sakkizlik sanoq tizimida 88<sub>8</sub> mavjud emas” va 7=”1024 Gbayt 1 Tb ga teng” rostlarining yig‘indisini hisoblang.

42. Quyidagi 43<sub>(8)</sub> va 56<sub>(16)</sub> sonlar yig‘indisini hisoblang va natijani sakkizlik sanoq tizimiga keltiring.

43. Agar  $a = DB_{(16)}$  va  $b = 331_{(8)}$  bo‘lsa, unda  $a < c < b$  tengsizlikni qanoatlantiruvchi  $c$  sonini aniqlang va natijani ikkilik sanoq tizimiga keltiring.
44. Quyidagi  $110_{(x)} = 12$  tenglama yechimini toping.
45. Quyidagi  $10_{(2)} + 10_{(8)} + 10_{(16)}$  sonlar yig‘indisini hisoblang va natijani ikkilik sanoq tizimiga keltiring.
46. Quyidagi  $100_{(x)} = 49$  tenglama yechimini toping va natijani ikkilik sanoq tizimiga keltiring.
47. Quyidagi  $1004_{(x)} = 129$  tenglama yechimini toping va natijani ikkilik sanoq tizimiga keltiring.
48. Quyidagi  $14_{(x)} + 42_{(x)} = 100_{(x)}$  tenglama yechimini toping va natijani ikkilik sanoq tizimiga keltiring.
49. Mantiqiy A, B, C, D qiymatlar uchun quyidagi tenglik  $(A \vee B) \wedge (C \vee D) = 1$  nechta yechimga ega?
50. ASCII jadvalida keltirilgan katta O harf belgisining qo‘simecha kodini aniqlang va javobini 16-lik son bilan yozing.

## 2.2. Butun sonlarning bo‘linish belgisi

Har qanday  $a$  butun son  $b$  butun songa ( $b \neq 0$ ) bo‘linadi agar shunday  $q$  butun son mayjud bo‘lib, bunda  $a = bq$  tenglik o‘rinli bo‘lsa va  $b$  soni  $a$  sonning bo‘luvchisi deyiladi. Bunda  $q$  bo‘linma,  $b$  bo‘luvchi,  $a$  bo‘linuvchi deb ataladi. Algebrada  $a$  sonni  $b$  songa bo‘linishi  $b/a$  shaklda belgilanadi, agar  $a$  son  $b$  songa bo‘linmasa, unda  $b \nmid a$  deb belgilanadi.

Bo‘linish xossalari:

- bo‘linish refleksiv, ya’ni  $a|a$ ;
- bo‘linish tranzitiv, ya’ni agar  $b|a$  va  $c|b$  bo‘lsa, u holda  $c|a$ ;
- $c|a$  dan ixtiyoriy butun  $b$  son uchun  $c|ab$  o‘rinli;
- $c|a$  va  $c|b$  dan ixtiyoriy butun  $x$  va  $y$  sonlar uchun  $c|ax+by$  o‘rinli;
- $b|a$  va  $a|b$  bo‘lsa,  $a = \pm b$ ;
- $b|a$ ,  $a > 0$ ,  $b > 0$  dan  $b \leq a$  kelib chiqadi.

**Qoldiqli bo‘lish haqidagi teorema:**  $a$  – butun son,  $b$  – butun musbat son bo‘lsin.  $a$  son hamma vaqt  $b$  songa bo‘linmaydi, lekin hamma vaqt  $a$  son  $b$  songa qoldiqli bo‘linadi, ya’ni shunday yagona butun  $q$  va  $r$  sonlar topiladiki, bular uchun

$$a = bq + r, \quad 0 \leq r < b$$

tenglik o‘rinli bo‘ladi, bu yerda  $q$  - to‘liqmas bo‘linma,  $r$  - soni  $a$  ni  $b$  ga bo‘lgandagi qoldiq deyiladi.

**1-misol.**  $a$  sonni 13 ga bo‘lganda to‘liqmas bo‘linma 17 ga teng bo‘lsa,  $a$  ning eng katta qiymatini toping.

*Yechilishi.* Masala shartiga ko‘ra,  $a = 13 \cdot 17 + r$ ,  $0 \leq r < 13$ . Demak,  $a$  ning qiymati eng katta bo‘lishi uchun  $r = 12$  bo‘lishi kerak, ya’ni  $13 \cdot 17 + 12 = 233$ .

**2-misol.** Bo‘linuvchi 371, to‘liqmas bo‘linma 14 ga teng bo‘lsa, bo‘luvchi va unga mos qoldiqlarni toping.

*Yechilishi.* Masala shartiga ko‘ra,  $371 = b \cdot 14 + r$ ,  $0 \leq r < b$ , bundan  $14b < 371$ ,  $b \leq 26$ . Boshqa tomondan  $15b > 371$ , bundan  $b > 24$ . Demak,  $b=25; 26$  va  $r=21; 7$  bo‘ladi.

**3-misol.**  $a$  sonni  $b$  songa bo‘lganda bo‘linma  $q$  va nolmas qoldiq  $r$  ga teng.  $a$  ni qanday natural  $n$  songa ko‘paytirganda bo‘linma  $n$  marta ortadi?

*Yechilishi.*  $an = bqn + rn$  dan  $rn < b$  va  $n < \frac{b}{r}$ .

**4-misol.** Uchta ketma-ket natural sonlardan bittasi 3 ga bo‘linishini isbotlang.

*Yechilishi.* Natural sonni  $3k$ ,  $3k + 1$ ,  $3k + 2$  sonlarning bittasi shaklida ifodalash mumkin. Agar  $n = 3k$  bo‘lsa, u holda  $3/n$ ; agar  $n = 3k + 1$  bo‘lsa, u holda  $3/n + 2$ ; agar  $n = 3k + 2$  bo‘lsa, u holda  $3/n+1$ .

**5-misol.** Agar besh xonali son 41 ga bo‘linsa, shu son tashkil qilgan raqamlarni aylanma almashtirish yordamida hosil bo‘lgan har qanday sonni 41 ga bo‘linishini isbotlang.

*Yechilishi.* Besh xonali son  $N=10^4a+10^3b+10^2s+10d+e$  bo‘lsin va u 41 ga bo‘linsin. Raqamlarni aylanma almashtirishdan (chapga bir raqamga) quyidagi sonni hosil qilamiz:

$N_1=10^4b+10^3c+10^2d+10e+a=10(10^4a+10^3b+10^2c+10d+e)-10^5a+a=10N-99999a$ .

41| N va 41|99999 dan 41| N<sub>1</sub> kelib chiqadi.

**6-misol.**  $2^{2^n} + 1 (n = 2, 3, \dots)$  ko‘rinishdagi barcha sonlar 7 raqam bilan tugashini isbotlang.

*Yechilishi.*  $2^{2^2} + 1 = 17$ . Agar  $2^{2^n} + 1 = 10q + 7$ , bo‘lsa, u holda

$$2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (10q + 6)^2 + 1 = (10Q + 6) + 1 = 10Q + 7.$$

### Topshiriqlar

1. 15 sonning har qanday natural darajaga ko‘tarib 7 ga bo‘linsa qanday qoldiq qolishini isbotlang.
2. Agar bo‘linuvchi va bo‘linma berilgan bo‘lsa, bo‘luvchi va qoldiqni toping: 25 va 3.
3. Agar bo‘linuvchi va bo‘linma berilgan bo‘lsa, bo‘luvchi va qoldiqni toping: – 30 va – 4.
4. Toq natural sonning kvadratini 8 ga bo‘lganda qoldiqni aniqlang.
5. Ketma-ket ikki natural son kvadratlari yig‘indisini 4 ga bo‘lganda qoldiqni aniqlang.
6. Ixtiyoriy butun  $n$  son uchun  $n^3 - n$  qanday songa bo‘linishini toping.
7. Agar besh xonali son 41 ga bo‘linsa, shu son tashkil qilgan raqamlarni aylanma almashtirish yordamida hosil bo‘lgan har qanday sonni 41 qanday songa bo‘linishini aniqlang.
8. Ixtiyoriy butun  $n$  son uchun  $n^7 - n$  qanday songa bo‘linishini toping.
9. Raqamlar yig‘indisi bir xil bo‘lgan ixtiyoriy ikki son ayirmasi qanday songa bo‘linishini isbotlang.
10.  $11^{10} - 1$  sonining oxirqi ikki raqamini toping.
11. Ketma-ket kelgan to‘rtta raqam birin-ketin yozilgan bo‘lib, birinchi ikkita raqam o‘rni almashtirilgandan so‘ng to‘la kvadrat bo‘lgan to‘rt xonali son hosil qilingan. Shu sonni toping.

12. Ixtiyoriy butun  $n$  son uchun  $n^5 - n$  qanday songa bo‘linishini toping.
13. Olti raqamli son 5 bilan tugaydi, agar bu sonni chap tomonga birinchi o‘ringa o‘tkazsak, u holda berilgan sondan 4 marta katta son hosil bo‘ladi. Shu sonni toping.
14. To‘la kvadrat bo‘lgan to‘rt xonali sonning minglar va o‘nlar xonasidagi raqamlar bir xil, yuzlar xonasidagi raqam birlik raqamdan 1 ga katta. Shu sonni toping.

### 2.3. Tub sonlar

Natural son **tub son** deyiladi, agar u faqatgina ikkita turli natural bo‘luvchiga (bir va o‘ziga) ega bo‘lsa va **murakkab son** deyiladi, agar uning bo‘luvchilar soni ikkitadan ko‘p bo‘lsa.

Bir soni na tub, na murakkab songa tegishli emas. Tub sonlar (va ularning natural darajalari) o‘zaro tubdir. Murakkab sonning birdan farqli natural bo‘luvchisi  $\sqrt{a}$  dan katta emas. Bu shartdan foydalanib  $a$  sonning tub bo‘luvchilarini faqat  $\sqrt{a}$  dan katta bo‘lmagan tub sonlar orasidan izlash kerakligi kelib chiqadi.

Istalgan  $a$  sondan katta bo‘lmagan tub sonlarni jadvalini tuzish uchun **Eratosfen g‘alviri** deb ataluvchi usul mavjud. Bu usul bo‘yicha sonlar qatorida birinchi topilgan  $p_1$  tub songa karrali bo‘lgan sonlarni o‘chirish, so‘ng ikkinchi  $p_2$  tub sonni topib, unga karrali sonlarni o‘chirish va hokazo. Bu jarayonni  $\sqrt{a}$  dan katta bo‘lmagan tub songacha davom ettirib, 1 dan  $a$  gacha sonlar qatorida o‘chirilmay qolgan sonlar 1 dan katta bo‘lgan tub sonlarni beradi.

**1-misol.** Eratosfen g‘alviri orqali 15 gacha bo‘lgan tub sonlarni aniqlang.

*Yechilishi.* 1 dan 15 gacha sonlarni yozib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

Jarayonni tub bo‘lgan 2 dan boshlaymiz, chunki 1 tub sonlarga kirmaydi. Birinchi tub bo‘lgan son 2, uni qoldirib unga karrali bo‘lgan sonlarni ostiga chizib o‘chirib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

E'tibor bering, bu yerda birinchi o'chirilmay qolgan son bu 3 va u tub son, chunki oldingi tub sonlarga bo'linmaydi. Demak 3 ni qoldiramiz va unga karrali bo'lган sonlarni ostiga chizib o'chirib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

Yuqoridagi ketma-ketlikda birinchi o'chirilmay qolgan son bu 5 va u tub son, chunki oldingi tub sonlarga bo'linmaydi. Demak 5 ni qoldiramiz va unga karrali bo'lган sonlar ostiga chizib o'chirib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

Ketma-ketlikda birinchi o'chirilmay qolgan son bu 7 va u tub son, chunki oldingi tub sonlarga bo'linmaydi. Demak 7 ni qoldiramiz va unga karrali bo'lган sonlar ostiga chizib o'chirib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

Ketma-ketlikda birinchi o'chirilmay qolgan son bu 11 va u tub son, chunki oldingi tub sonlarga bo'linmaydi. Demak 11 ni qoldiramiz va unga karrali bo'lган sonlar ostiga chizib o'chirib chiqamiz:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 .

Natijaviy jarayondan so'ng birinchi o'chirilmay qolgan son bu 13 va u tub son, chunki oldingi tub sonlarga bo'linmaydi. Demak 13 ni qoldiramiz va boshqa son qolmadi, demak tub sonlar bular: 2, 3, 5, 7, 11, 13.

### Topshiriqlar

1. 127 tub yoki murakkab son ekanligini aniqlang.
2. 481 tub yoki murakkab son ekanligini aniqlang.
3. 919 tub yoki murakkab son ekanligini aniqlang.
4. 323 tub yoki murakkab son ekanligini aniqlang.
5. 2320 va 2350 sonlari orasida joylashgan barcha tub sonlarni toping.
6. 200 va 220 sonlari orasida joylashgan barcha tub sonlarni toping.
7. 2540 va 2570 sonlari orasida joylashgan barcha tub sonlarni toping.
8. 1200 va 1250 sonlari orasida joylashgan barcha tub sonlarni toping.

9. 1 va 40 sonlari orasida joylashgan barcha tub sonlarni Eratosfen g‘alviri yordamida toping.

10. Quyidagi 13<sup>11</sup> sonining nechta bo‘luvchishi bor?

#### 2.4. Sonlarni ko‘paytuvchilarga yoyish

Ixtiyoriy murakkab natural  $a$  sonni faqat bir usulda  $p_1, p_2, \dots, p_n$  tub sonlar ko‘paytuvchilariga ajratish mumkin:

$$a = p_1 p_2 \dots p_n .$$

Ba’zi ko‘paytuvchilar takrorlanib kelishi mumkin, shuning uchun ularni karralilarini mos ravishda  $\alpha_1, \alpha_2, \dots, \alpha_n$  lar bilan belgilab,  $a$  sonning **kanonik yoyilmasini** hosil qilamiz, ya’ni:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} .$$

Masalan, 3600 sonini tub sonlar ko‘paytmasi shaklida quyidagicha yozish mumkin:  $3600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$ . Kanonik yoyilmasi esa:  $3600 = 2^4 \cdot 3^2 \cdot 5^2$  bo‘ladi. Xuddi shunday 588000 sonining kanonik yoyilmasi quyidagicha bo‘ladi:  $588000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$ .

Bundan  $a$  sonning har qanday bo‘luvchisi

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

ko‘rinishga ega bo‘lishi kelib chiqadi, bu yerda  $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_n \leq \alpha_n$ .

$a$  sonning bo‘luvchilarining umumiy soni esa  $\tau(a)$  deb belgilanadi va quyidagicha aniqlanadi:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1).$$

Bo‘luvchilar sonini aniqlashga qaratilgan maxsus jadvallar ham mavjud, masalan

$a$	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(a)$	1	2	2	3	2	4	2	4	3	4	2	6

#### Topshiriqlar

1. Toq 6643 sonni ko‘paytuvchilarga ajrating.
2. Toq 1769 sonni ko‘paytuvchilarga ajrating.
3. Toq 3551sonni ko‘paytuvchilarga ajrating.
4. Toq 6497 sonni ko‘paytuvchilarga ajrating.
5. Toq 1309 sonni ko‘paytuvchilarga ajrating.
6. Toq 819 sonni ko‘paytuvchilarga ajrating.
7. Toq 1221 sonni ko‘paytuvchilarga ajrating.
8. Toq 1323 sonni ko‘paytuvchilarga ajrating.
9. Juft 5292 sonni ko‘paytuvchilarga ajrating.
10. Toq 2431 sonni ko‘paytuvchilarga ajrating.
11. Toq 507 sonni ko‘paytuvchilarga ajrating.
12. Juft 2940 sonni ko‘paytuvchilarga ajrating.
13. Toq 7469 sonni ko‘paytuvchilarga ajrating.
14. Juft 2700 sonni ko‘paytuvchilarga ajrating.
15. Quyidagi sonlarning umumiy bo‘luvchilaridan eng kattasini aniqlang:  
 $2910600=2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$ ,  $178500=2^2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 17$  va  $27720=2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ .
16. Quyidagi sonlarning umumiy bo‘luvchilaridan eng kattasini aniqlang:  
 $242550=2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11$ ,  $23100=2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$  va  $21420=2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17$ .
17. 100 dan katta bo‘lmagan sonlar ichidan eng ko‘p bo‘luvchilarga ega sonlarni aniqlang.
18. 14 ta bo‘luvchiga ega eng kichik natural sonni aniqlang.

## 2.5. Eng katta umumiy bo‘luvchi

Bir nechta  $a, b, \dots, l$  sonlarni bo‘luvchi butun son shu sonlarning **umumiy bo‘luvchisi** deyiladi.

Shu bo‘luvchilarning eng kattasi **eng katta umumiy bo‘luvchi** (EKUB) deyiladi va  $d = (a, b, \dots, l)$  yoki  $d = EKUB(a, b, \dots, l)$  kabi belgilanadi.

Agar  $(a, b, \dots, l) = 1$  bo‘lsa,  $a, b, \dots, l$  sonlar o‘zaro **tub sonlar** deyiladi. Agar  $a, b, \dots, l$  sonlarning har biri qolganlari bilan o‘zaro tub bo‘lsa, bu sonlar **juft-juft tub sonlar** deyiladi.

Agar  $d = (a, b)$  bo'lsa, u holda  $(a/d, b/d) = 1$  bo'ladi.

Har qanday  $a, b$  butun sonlari uchun shunday  $x_0$  va  $y_0$  butun sonlar mavjudki,  $(a, b) = a \cdot x_0 + b \cdot y_0$  tenglik bajariladi.

Har qanday  $a, b, c$  butun sonlari uchun  $(a, b) = 1$  va  $ab$  son  $c$  ga bo'linsa, u holda  $b$  soni ham  $c$  ga bo'linadi.

Yevklid algoritmini qo'llab sonlarni EKUB qiymatini topish mumkin, bu usul quyidagicha: agar  $a$  va  $b$  – natural sonlar va  $a > b$  bo'lsa, u holda

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2,$$

.....

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n q_{n+1}, \quad r_{n+1} = 0.$$

Noldan farqli oxirgi  $r_n$  qoldiq masala shartidagi  $a$  va  $b$  sonlarining EKUB sonini beradi.

**1-misol.** (525, 231) qiymatini Yevklid algoritmini qo'llab aniqlang.

*Yechilishi.*

1-qadam:

525	231	$525 = 231 \cdot 2 + 63$
462	2	
	63	

2-qadam:

231	63	$231 = 63 \cdot 3 + 42$
189	2	
	42	

3-qadam:

63	42	$63 = 42 \cdot 1 + 21$
42	1	
	21	

4-qadam:

42	21	$42 = 21 \cdot 2$
42	2	
	0	

Demak,  $(525, 231) = 21$  ga teng.

Har qanday  $a, b, \dots, l$  sonlarga bo‘linadigan son berilgan sonlarni **umumiylaralisi** deyiladi. Umumiylaralarning eng kichigi **eng kichik umumiylaralisi** (**EKUK**) deyiladi va  $m = [a, b, \dots, l]$  bilan belgilanadi.

$a$  va  $b$  sonlarning umumiylaralisi

$$M = \frac{ab}{d} t, \quad t \in \mathbf{Z}, \quad d = (a, b)$$

tenglik yordamida topiladi. Agar  $t = 1$  bo‘lsa, bu tenglikdan  $a$  va  $b$  sonlarning EKUK qiymati kelib chiqadi, ya’ni

$$m = \frac{ab}{d}, \quad \text{yoki} \quad [a, b] = \frac{ab}{(a, b)}.$$

Juft-juft o‘zaro tub sonlarning EKUK qiymati shu sonlar ko‘paytmasiga teng.

Agar  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  bo‘lsa  $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , 6y epda  $p_1, p_2, \dots, p_k$  – turli tub sonlar,  $\alpha_i, \beta_j$  – butun musbat sonlar bo‘lsin. U holda

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)},$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}.$$

Quyidagi rekurrent formulalar yordamida bir nechta sonlarni EKUK va EKUB qiymatlarini topish mumkin:

$$(a_1, a_2, \dots, a_{n-1}, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n),$$

$$[a_1, a_2, \dots, a_{n-1}, a_n] = [[a_1, a_2, \dots, a_{n-1}], a_n]$$

Demak bu formulalardan bir nechta sonlarni EKUB va EKUK qiymatlarini topish ikkita sonni EKUB va EKUK qiymatlarini topish masalasiga keltiriladi.

Agar  $a, b, c$  – butun musbat sonlar bo‘lsa va  $a = cq + r$ ,  $b = cq_1 + r_1$  bo‘lib,  $q, q_1, r, r_1$  – butun nomanfiy sonlar bo‘lsa, u holda quyidagi tenglik o‘rinlidir:

$$(a, b, c) = (c, r, r_1).$$

**2-misol.** (1734, 822) va [1734, 822] ni toping.

*Yechilishi.* Bu sonlar uchun Yevklid algoritmini qo‘llaymiz:

$$1734 = 822 \cdot 2 + 90;$$

$$822 = 90 \cdot 9 + 12;$$

$$90 = 12 \cdot 7 + 6;$$

$$12 = 6 \cdot 2.$$

Demak,  $(1734, 822) = 6$ .

$$[1734, 822] = \frac{1734 \cdot 822}{6} = 237558.$$

**3-misol.**  $3 = (51, 21)$  ni  $51x+21y$  shaklda ifodalang.

*Yechilishi.*  $51 = 21 \cdot 2 + 9$ ,  $21 = 9 \cdot 2 + 3$ .

Bundan  $3 = 21 - 2 \cdot 9 = 21 - 2(51 - 21 \cdot 2) = 21 \cdot 5 - 51 \cdot 2$ .

**4-misol.**  $\begin{cases} x + y = 150 \\ (x, y) = 30 \end{cases}$  sistemani natural yechimlarini toping.

*Yechilishi.*  $(x, y) = 30$  quyidagi sistemaga teng kuchli.

$$\begin{cases} x = 30u \\ y = 30v \\ (u, v) = 1. \end{cases}$$

Bundan berilgan sistemaning birinchi tenglamasi  $u + v = 5$  ko‘rinishga keladi va  $u = 1, 2, 3, 4$  qiymatlar qabul qiladi. Demak,  $x = 30, 60, 90, 120$  ga teng bo‘lishi mumkin.  $y = 150 - x$  dan  $y = 120, 90, 60, 30$ .

**5-misol.** Agar  $(a, b) = 24$ ,  $[a, b] = 2496$  bo‘lsa,  $a$  va  $b$  larni toping.

*Yechilishi.*  $(a, b) = 24$  dan  $a = 24x$ ,  $b = 24y$  va  $(x, y) = 1$  kelib chiqadi.  $x < y$  bo‘lsin.  $[a, b] = \frac{ab}{(a, b)}$  dan

$$2496 = \frac{24x \cdot 24y}{24} \text{ yoki } xy = 104 = 2^2 \cdot 13.$$

$(x, y) = 1$  dan  $xy = 1 \cdot 104$  yoki  $xy = 8 \cdot 13$  bo‘lishi mumkin. Bundan  $x = 1$  va  $y = 104$  bo‘lganda  $a = 24 \cdot 1 = 24$ ,  $b = 24 \cdot 104 = 2496$ ;  $x = 8$  va  $y = 13$  bo‘lganda  $a = 24 \cdot 8 = 192$ ,  $b = 24 \cdot 13 = 312$ .

### Topshiriqlar

1. Yevklid algoritmi yordamida 546 va 231 sonlarning EKUB qiymatini toping.

2. Yevklid algoritmi yordamida 1001 va 6253 sonlarning EKUB qiymatini toping.
3. Yevklid algoritmi yordamida 2737, 9163 va 9639 sonlarning EKUB qiymatini toping.
4. Yevklid algoritmi yordamida 420, 126 va 525 sonlarning EKUB qiymatini toping.
5. Yevklid algoritmi yordamida 529, 1541 va 1817 sonlarning EKUB qiymatini toping.
6. Sonlarni tub ko‘paytuvchilarga ajratib 360 va 504 sonlarning EKUB qiymatini toping.
7. Sonlarni tub ko‘paytuvchilarga ajratib 387 va 528 sonlarning EKUB qiymatini toping.
8. Sonlarni tub ko‘paytuvchilarga ajratib 135 va -180 sonlarning EKUB qiymatini toping.

9. Quyidagi  $[a,b] = \frac{ab}{(a,b)}$  formuladan foydalanib, 252 va 468 sonlarining EKUK qiymatini toping.

10. Quyidagi  $[a,b] = \frac{ab}{(a,b)}$  formuladan foydalanib, quyidagi 279 va 372 sonlarning EKUK qiymatini toping.

11. Quyidagi  $[a,b] = \frac{ab}{(a,b)}$  formuladan foydalanib, 299 va 234 sonlarining EKUK qiymatini toping.

12.  $a = 899$ ,  $b = 493$  berilgan.  $d = (a,b)$  ni toping va shunday  $x$  va  $y$  larni aniqlangki,  $d = ax + by$  ko‘rinishda ifodalash mumkin bo‘lsin.

13.  $a = 90$ ,  $b = 35$  berilgan.  $d = (a,b)$  ni toping va shunday  $x$  va  $y$  larni aniqlangki,  $d = ax + by$  ko‘rinishda ifodalash mumkin bo‘lsin.

14.  $a = 1445$ ,  $b = 629$  berilgan.  $d = (a,b)$  ni toping va shunday  $x$  va  $y$  larni aniqlangki,  $d = ax + by$  ko‘rinishda ifodalash mumkin bo‘lsin.

15.  $a = 903$ ,  $b = 731$  berilgan.  $d = (a,b)$  ni toping va shunday  $x$  va  $y$  larni aniqlangki,  $d = ax + by$  ko‘rinishda ifodalash mumkin bo‘lsin.

16.  $a = 1786$ ,  $b = 705$  berilgan.  $d = (a, b)$  ni toping va shunday  $x$  va  $y$  larni aniqlangki,  $d = ax + by$  ko‘rinishda ifodalash mumkin bo‘lsin.

17. Quyidagi tenglamalar sistemasining natural yechimlarini toping:

$$\begin{cases} (x, y) = 45 \\ \frac{x}{y} = \frac{11}{7} \end{cases}$$

18. Quyidagi tenglamalar sistemasining natural yechimlarini toping:

$$\begin{cases} \frac{x}{y} = \frac{5}{9} \\ (x, y) = 28 \end{cases}$$

## 2.6. Taqqoslama arifmetikasi

$m$  – natural son,  $a$  va  $b$  – butun sonlar berilgan bo‘lsin. Agar  $a - b$  ayirma  $m$  ga bo‘linsa,  $a$  son  $b$  bilan  $m$  modul bo‘yicha **taqqoslanuvchi** deyiladi va quyidagi ko‘rinishda  $a \equiv b \pmod{m}$  yoziladi.

Bunda quyidagi xossalar o‘rinli:

1.  $a \equiv a \pmod{m}$  (refleksivlik xossasi), chunki ( $a - a$ ) soni  $m$  ga bo‘linadi.
2.  $a \equiv b \pmod{m}$  bo‘lsa, u holda  $b \equiv a \pmod{m}$  (simmetriklik xossasi), chunki ( $a - b$ ) soni  $m$  ga bo‘linsa, unda  $b - a = -(a - b)$  ham  $m$  ga bo‘linadi.
3. Agar  $a \equiv b \pmod{m}$  va  $b \equiv c \pmod{m}$  bo‘lsa, u holda  $a \equiv c \pmod{m}$ , chunki ( $a - b$ ) soni  $m$  ga bo‘linsa va  $b - c$  soni  $m$  ga bo‘linsa, u holda quyidagi tenglikdan  $a - c = (a - b) + (b - c)$  bevosita  $a - c$  soni ham  $m$  ga bo‘linadi.

Bu uchta xossaning o‘rinligi  $a \equiv b \pmod{m}$  binar munosabat bevosita ekvivalentlik munosabati ekanligini ko‘rsatadi. Butun sonlar to‘plamida  $Z$  bu ekvivalentlik munosabati hosil qilgan sinflarni  $m$  modul bo‘yicha **chegirmalar sinflari** deyiladi,  $a \equiv b \pmod{m}$  munosabat esa **taqqoslama** deyiladi.

Bundan,  $a \equiv b \pmod{m}$  munosabati  $a$  va  $b$  sonlar  $m$  ga bo‘linganda bir xil qoldiqga ega bo‘lishiga teng kuchli bo‘lgani uchun,  $m$  modul bo‘yicha har bir chegirmalar sinfi  $m$  ga bo‘linganda bir xil qoldiq beradigan barcha butun sonlardan iborat bo‘ladi. Butun son  $m$  ga bo‘linganda faqat  $0, 1, \dots, m-1$  sonlarga qoldiq sifatida hosil bo‘ladi, ya’ni  $m$  modul bo‘yicha faqatgina  $m$  ta chegirmalar sinfi bor.

Agar  $a \equiv b \pmod{m}$  va  $c \equiv d \pmod{m}$  bo'lsa, u holda quyidagilar o'rinnlidir:

$$a + c \equiv b + d \pmod{m},$$

$$a \cdot c \equiv b \cdot d \pmod{m}.$$

Ammo,  $a \equiv b \pmod{m}$  taqqoslamaning ikki tomonini qisqartirish har doim ham to'g'ri bo'lmaydi, masalan, taqqoslama  $22 \equiv -2 \pmod{8}$  o'rinnli bo'lsada,  $11 \equiv -1 \pmod{8}$  bajarilmaydi.

Faqatgina quyidagi vaziyatda qisqartirishni amalga oshirish mumkin: agar  $ac \equiv bc \pmod{m}$  bo'lsa, sonlar  $m$  va  $c$  o'zaro tub bo'lgandagina  $a \equiv b \pmod{m}$  bajariladi. Masalan,  $4 \equiv 48 \pmod{11}$  uchun  $(11,4)=1$  bo'lganligi sababli 4 ga qisqartiramiz va natija  $1 \equiv 12 \pmod{11}$  o'rinnli.

Agar  $a \equiv b \pmod{m}$  tenglik o'rinnli bo'lsa, u holda tenglikning ikki tomonini istalgan darajaga ko'tarish mumkin, ya'ni  $n$  natural son uchun  $a^n \equiv b^n \pmod{m}$  o'rinnlidir. Ushbu xossaladan foydalanib, katta darajali sonlarning bo'linmadagi qoldiqlarini aniqlash mumkin. Masalan,  $3^{89} \pmod{7}$  qiymatini quyidagicha aniqlash mumkin bo'ladi. Quyidagi tenglik  $9=3^2 \equiv 2 \pmod{7}$  o'rinnli bo'lganligi sababli, uni ikkinchi daraja ko'taramiz, ya'ni  $3^4 \equiv 4 \pmod{7}$  bo'ladi. Xuddi shunday qolgan variantlarni ham bajaramiz, ya'ni

$$3^8 \equiv 16 \pmod{7} = 2 \pmod{7},$$

$$3^{16} \equiv 4 \pmod{7},$$

$$3^{32} \equiv 16 \pmod{7} = 2 \pmod{7},$$

$$3^{64} \equiv 4 \pmod{7},$$

Quyidagi tenglikdan foydalanamiz,  $89 = 64 + 16 + 8 + 1 = 2^6 + 2^4 + 2^3 + 1$ , demak  $3^{89} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3 \equiv 4 \cdot 4 \cdot 2 \cdot 3 \equiv 5 \pmod{7}$ . Demak, qoldiq 5 ga teng bo'ladi.

Agar  $a \equiv b \pmod{m}$  bo'lsa, u holda  $(a, m) = (b, m)$  bo'ladi.

Bu yerda Fermaning kichik teoremasi deb nom olgan quyidagi natijani keltirib o'tamiz: Agar  $a$  – butun son va  $p$  – tub son bo'lsa, u holda  $a^p - a$  son  $p$  ga bo'linadi.

Agar  $a$  va  $b$  – butun son va  $p$  – tub son bo'lsa, u holda

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Bu yerdan Fermaning kichik teoremasini isbotlash mumkin. Agar  $a=1$  va  $b=1$  deb qabul qilsak, unda

$$2^p = (1 + 1)^p \equiv 1^p + 1^p \equiv 2 \pmod{p}.$$

Endi  $a=2$  va  $b=1$  deb qabul qilsak, unda

$$3^p = (2 + 1)^p \equiv 2^p + 1^p \equiv 2 + 1 \equiv 3 \pmod{p}.$$

Shu usul bilan davom ettirilsa, unda  $a^p \equiv a \pmod{p}$ . Umumiy holda, agar  $a$  va  $p$  sonlari o‘zaro tub bo‘lsa, u holda  $a^{p-1} \equiv 1 \pmod{p}$  bajariladi. Aksincha, ushbu tenglik bajarilsa, undan  $p$  soni tub bo‘lishi shart emas.

**1-misol.** Quyidagi  $13^{176} - 1$  ayirma 89 soniga bo‘linishini ko‘rsating.

*Yechilishi.* Quyidagi  $a^2 - b^2 = (a-b)(a+b)$  formuladan foydalanamiz:

$$13^{176} - 1 = (13^{88} - 1)(13^{88} + 1).$$

89 soni tub bo‘lganligidan va  $(13, 89) = 1$  bo‘lganligini e’tiborga olib, Ferma teoremasidan:

$13^{88} \equiv 1 \pmod{89}$ , bundan  $13^{88} - 1$  bevosita 89 ga bo‘linadi. Demak,  $13^{176} - 1$  ham 89 ga bo‘linadi.

Keltirilan xossalardan foydalanib har qanday sonni tub emasligini aniqlash mumkin bo‘ladi. Demak,  $N$  soni berilgan bo‘lsa, u holda  $a^{N-1} \equiv 1 \pmod{N}$  tenglik bajarilmasa, unda  $N$  murakkab son bo‘ladi. Misol sifatida  $N = 91$  va  $a = 2$  bo‘lsin. Bunda quyidagi bajariladi:

$$a^{N-1} = 2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2.$$

Bundan tashqari

$$2^8 = 256 \equiv -17 \pmod{91},$$

$$2^{16} = (2^8)^2 \equiv (-17)^2 = 289 \equiv 16 \pmod{91},$$

$$2^{32} = (2^{16})^2 \equiv (16)^2 = 256 \equiv -17 \pmod{91},$$

$$2^{64} = (2^{32})^2 \equiv (-17)^2 = 289 \equiv 16 \pmod{91}.$$

Demak,

$2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 16 \cdot 16 \cdot (-17) \cdot 4 \equiv 64 \neq 1 \pmod{91}$ . Bundan,  $N$  murakkab son ekanligi kelib chiqadi, haqiqatdan,  $91 = 7 \cdot 13$ .

Shu bilan birga, kriptografiya sohasida mavjud tenglamalarni yechishda quyidagi natija foydalidir, ya’ni  $a$  va  $b$  – butun sonlar bo‘lsin va  $m$  esa natural son bo‘lsin. Unda  $ax \equiv b \pmod{m}$  taqqoslama yechimga ega bo‘lishi uchun  $b$  ning  $d = (a, m)$  ga bo‘linishi zarur va yetarlidir. Bu shart bajarilganda taqqoslamaning umumiy yechimi  $x = x_0 + m_1 t$  formula bilan beriladi ( $t$  – butun son), bu yerda  $x_0$  – taqqoslamaning biror xususiy yechimi va  $m_1 = m/d$ .

Keltirilgan tushunchalar bilan quyidagi misollarda tanishib olamiz. Masalan, quyidagi taqqoslamalarni tekshirib ko‘ramiz.

**2-misol.**  $23 \equiv 8 \pmod{5}$ , haqiqatdan, taqqoslama ta’rifi bo‘yicha  $23 - 8 = 15 = 5 \cdot 3$ . Natija 5 ga bo‘linadi, demak tenglik o‘rinli.

**3-misol.**  $-11 \equiv 5 \pmod{8}$ , haqiqatdan,  $-11 - 5 = -16 = 8 \cdot (-2)$ . Natija 8 ga bo‘linadi, demak tenglik o‘rinli.

Har qanday  $a$  soni  $m$  ga bo‘linsa, unda  $a \equiv 0 \pmod{m}$  deb yozish mumkin. Agar  $a \equiv b \pmod{0}$  bo‘lsa, unda  $a=b$ .

Agar  $a$  va  $b$  – butun sonlarining  $m$  sanoq tizimida oxirgi raqamlari teng bo‘lsa, unda  $a \equiv b \pmod{m}$  tenglik bajariladi. Masalan,  $37 \equiv 87 \pmod{10}$ .

Taqqoslamaning ikki tomonini va modulni umumiy bo‘luvchiga qisqartirish mumkin, ya’ni  $a \equiv b \pmod{m}$  tenglik bajarilsa va  $a = a_1 d$ ,  $b = b_1 d$ ,  $m = m_1 d$  bo‘lsa, unda  $a_1 \equiv b_1 \pmod{m_1}$  tenglik bajariladi.

Agar  $a \equiv b \pmod{m}$  tenglik bajarilsa va  $m = m_1 d$  bo‘lsa, unda  $a \equiv b \pmod{m_1}$  tenglik ham bajariladi.

Agar  $a \equiv b \pmod{m}$  tenglik bajarilsa, unda  $(a, m) = (b, m)$  tenglik ham bajariladi.

Ko‘p uchraydigan masalalardan biri bu tenglamalarni yechish hisoblanadi. Masalan, quyidagi tenglama yechimini aniqlash talab etilsin:  $5x \equiv 7 \pmod{8}$ . Bevosita 8 sonini qo‘sish, masalan o‘ng qismiga, natijasida tenglik buzilmaydi, ya’ni  $5x \equiv 7 + 8 \pmod{8}$ . Bundan  $5x \equiv 15 \pmod{8}$ . Endi tenglikni 5 ga qisqartirsak  $x \equiv 3 \pmod{8}$  yechim hosil bo‘ladi.

Endi taqqoslamalardan iborat tenglamalar sistemasini yechishni ko‘rib chiqamiz. Demak,

**4-misol.** Taqqoslamalar sistemasini yeching:

$$\begin{cases} 2x \equiv 31 \pmod{35} \\ 4x \equiv 7 \pmod{25} \\ 5x \equiv 18 \pmod{21} \end{cases}$$

*Yechilishi.* Har bir taqqoslamani alohida yechib quyidagi natijaga kelish mumkin:

$$\begin{cases} x \equiv -2 \pmod{35} \\ x \equiv 8 \pmod{25} \\ x \equiv 12 \pmod{21} \end{cases}$$

Birinchi taqqoslamadan  $x = -2 + 35t$  ( $t$  – istalgan butun son) bo‘ladi. Ushbu natijani ikkinchi taqqoslamaga qo‘yib  $t$  ning qiymatlarini aniqlaymiz, ya’ni  $-2 + 35t \equiv 8 \pmod{25}$ , bundan  $35t \equiv 10 \pmod{25}$ , bundan esa  $t \equiv 1 \pmod{5}$ , ya’ni  $t = 1 + 5n$ , ( $n$  – istalgan butun son). Demak, birinchi va ikkinchi tenglamalar uchun quyidagi bajariladi:  $x = -2 + 35(1 + 5n) = 33 + 175n$ .

Uchinchi tenglamadan  $33 + 175n \equiv 12 \pmod{21}$ , yoki  $175n \equiv -21 \pmod{21}$ , bundan  $7n \equiv 0 \pmod{21}$  yoki  $n \equiv 0 \pmod{3}$ . Buning yechimi esa  $n \equiv 3k$  ( $k$  – istalgan butun son) bo‘ladi. Shunday qilib,

$$x = 33 + 175n = 33 + 175(3k) = 33 + 525k.$$

Umumiy ko‘rinishda quyidagi yechimga ega bo‘ldik:  $x \equiv 33 \pmod{525}$ .

Har qanday ko‘phad  $P(x)$  uchun

$$P(x) = a_n x^n + \dots + a_1 x + a_0$$

$a_i$  – koeffitsiyentlar butun son bo‘lib, butun  $a$  va  $b$  sonlar uchun  $a \equiv b \pmod{m}$  tenglik bajarilsa, unda  $P(a) \equiv P(b) \pmod{m}$  o‘rinlidir.

Ushbu xossa yordamida har qanday sonni uchgaga bo‘linish alomatini aniqlash mumkin. Haqiqatdan, natural  $N$  sonini quyidagi  $N = P(10) = a_n 10^n + \dots + a_1 10 + a_0$  shaklda tasvirlash mumkin. Quyidagi taqqoslama  $10 \equiv 1 \pmod{3}$  aniq bo‘lganligi sababli bevosita  $P(10) \equiv P(1) \pmod{3}$  o‘rinli bo‘ladi. Demak,  $N = P(10) = a_n 10^n + \dots + a_1 10 + a_0 \equiv a_n + \dots + a_1 + a_0 \pmod{3}$  bo‘ladi. Bundan,  $N$  soni 3 ga bo‘linishi uchun uning raqamlari yig‘indisi 3 ga bo‘linishi kifoya.

## Topshiriqlar

- Quyidagi uchun qoldiqni aniqlang:  $-37 \pmod{7}$ .
- Quyidagi uchun qoldiqni aniqlang:  $-111 \pmod{11}$ .
- Quyidagi uchun qoldiqni aniqlang:  $-365 \pmod{30}$ .
- Quyidagi tenglama yechimini aniqlang:  $256x \equiv 179 \pmod{337}$ .
- Quyidagi tenglama yechimini aniqlang:  $1296x \equiv 1105 \pmod{2413}$ .
- Quyidagi tenglamalar sistemasini yechimini aniqlang:

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 11 \pmod{20} \\ x \equiv 1 \pmod{15} \end{cases}$$

- Quyidagi tenglamalar sistemasini yechimini aniqlang:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 9 \pmod{11} \\ x \equiv 3 \pmod{13} \end{cases}$$

- Quyidagi tenglamalar sistemasini yechimini aniqlang:

$$\begin{cases} 3x + 4y - 29 \equiv 0 \pmod{143} \\ 2x - 9y + 84 \equiv 0 \pmod{143} \end{cases}$$

- Quyidagi funksiya uchun  $f(x) = 7x^4 + 19x + 25$ , taqqoslama  $f(x) \equiv 0 \pmod{27}$  yechimini aniqlang. Masalani  $f(x) \equiv 0 \pmod{3}$  yechimini aniqlashdan boshlang.
- Quyidagi taqqoslama  $x^3 + 2x + 2 \equiv 0 \pmod{125}$  yechimini aniqlang.
- Quyidagi taqqoslama  $37x \equiv 16 \pmod{11}$  yechimini aniqlang.
- Quyidagi taqqoslama  $39x \equiv 5 \pmod{11}$  yechimini aniqlang.
- Quyidagi taqqoslama  $11x \equiv 15 \pmod{24}$  yechimini aniqlang.
- Quyidagi taqqoslama  $39x \equiv 19 \pmod{53}$  yechimini aniqlang.
- Quyidagi taqqoslama  $12x \equiv 15 \pmod{35}$  yechimini aniqlang.
- Quyidagi taqqoslama  $21x \equiv 10 \pmod{25}$  yechimini aniqlang.
- Quyidagi taqqoslama  $15x \equiv 7 \pmod{16}$  yechimini aniqlang.
- Quyidagi taqqoslama  $8x \equiv 17 \pmod{23}$  yechimini aniqlang.

19. Quyidagi taqqoslama  $27x \equiv 11 \pmod{106}$  yechimini aniqlang.
20. Quyidagi taqqoslama  $64x \equiv 5 \pmod{13}$  yechimini aniqlang.
21. Quyidagi taqqoslama  $139x \equiv 7 \pmod{8}$  yechimini aniqlang.
22. Quyidagi taqqoslama  $14x \equiv 9 \pmod{37}$  yechimini aniqlang.
23. Quyidagi taqqoslama  $2x \equiv 13 \pmod{15}$  yechimini aniqlang.
24. Quyidagi taqqoslama  $19x \equiv 4 \pmod{25}$  yechimini aniqlang.
25. Quyidagi taqqoslama  $29x \equiv 35 \pmod{123}$  yechimini aniqlang.
26. Quyidagi taqqoslama  $27x \equiv 16 \pmod{58}$  yechimini aniqlang.
27. Quyidagi taqqoslama  $97x \equiv 53 \pmod{169}$  yechimini aniqlang.
28. Quyidagi taqqoslama  $5x \equiv 2 \pmod{8}$  yechimini aniqlang.
29. Quyidagi taqqoslama  $7x \equiv 2 \pmod{13}$  yechimini aniqlang.
30. Quyidagi taqqoslama  $17x \equiv 7 \pmod{30}$  yechimini aniqlang.
31. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 12 \pmod{17} \\ x \equiv 10 \pmod{11} \end{cases}$$

32. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 20 \pmod{23} \\ x \equiv 21 \pmod{25} \end{cases}$$

33. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 15 \pmod{17} \\ x \equiv 7 \pmod{20} \end{cases}$$

34. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 9 \pmod{16} \\ x \equiv 7 \pmod{25} \end{cases}$$

35. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 15 \pmod{23} \\ x \equiv 12 \pmod{29} \end{cases}$$

36. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} 3x \equiv 5 \pmod{4} \\ 5x \equiv 2 \pmod{7} \end{cases}$$

37. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} 3x \equiv 2 \pmod{13} \\ 5x \equiv 11 \pmod{16} \\ 5x \equiv 2 \pmod{9} \end{cases}$$

38. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} 3x \equiv 5 \pmod{13} \\ 2x \equiv 17 \pmod{21} \\ 5x \equiv 31 \pmod{32} \end{cases}$$

39. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 7 \pmod{25} \end{cases}$$

40. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{7} \\ x \equiv -2 \pmod{11} \end{cases}$$

41. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} 5x \equiv 2 \pmod{12} \\ 7x \equiv 2 \pmod{8} \\ 3x \equiv 1 \pmod{5} \end{cases}$$

42. Noma'lum butun son bevosita 7, 13, 17 sonlariga bo'linganda mos ravishda quyidagi qoldiqlarga 4, 9, 1 ega barcha butun sonlarni aniqlang.

43. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

44. Quyidagi taqqoslamalar sistemasining yechimini aniqlang.

$$\begin{cases} 3x \equiv 5 \pmod{7} \\ 2x \equiv 1 \pmod{5} \end{cases}$$

45. Quyidagi  $5^{100}$  sonining oxirgi ikki raqamini aniqlang.

46. Quyidagi  $7^{402}$  sonini 101 ga bo'lgandagi qoldiqni aniqlang.

47. Quyidagi  $243^{402}$  sonining oxirgi ikki raqamini aniqlang.

## 2.7. O‘rin almashtirishlar

Berilgan  $n$  ta  $1, 2, \dots, n$  sonlarning (yoki  $n$  ta har xil  $a_1, a_2, \dots, a_n$  belgilarning) ma’lum tartibdagi mumkin bo‘lgan ixtiyoriy joylashuviga shu sonlarning (yoki belgilarning) **o‘rin almashtirishi** deyiladi. Berilgan  $n$  ta belgilarni bevosita  $1, 2, \dots, n$ , sonlari bilan tartiblash mumkin bo‘lganligi sababli ixtiyoriy  $n$  ta belgilarning o‘rin almashtirishlarini o‘rganish  $1, 2, \dots, n$  larning o‘rin almashtirishlarini o‘rganishga keltiriladi. Berilgan  $n$  ta sonlarning barcha o‘rin almashtirishlari soni  $1 \cdot 2 \cdot 3 \cdots n = n!$  ga teng. Misol.  $a_1, a_2, a_3$  belgilarining barcha o‘rin almashtirishlari quyidagilardir:  $a_1 a_2 a_3, a_1 a_3 a_2, a_2 a_1 a_3, a_2 a_3 a_1, a_3 a_1 a_2, a_3 a_2 a_1$ . Demak, ularning umumiyligi soni  $3! = 6$  ta bo‘ladi.

Agar o‘rin almashtirishda ikki sondan kattasi kichigidan oldin kelsa bu sonlar **inversiyani** tashkil etadi, agar kichigi kattasidan oldin kelsa, **tartib** deyiladi. Inversiyalar sonini hisoblash usulini ko‘rib chiqamiz. O‘rin almashtirishdagi sonlarni yozilish tartibi bo‘yicha (chapdan o‘ngga) har bir son uchun undan o‘ng tomonda turgan kichik sonlar sanaladi va hosil bo‘lgan barcha sonlar qo‘shiladi. Masalan. (613542) o‘rin almashtirishda inversiyalar soni 9 ga teng, chunki (6) dan keyin 5 ta undan kichik sonlar kelyapdi, (1) dan kichik son yo‘q va h.k., demak  $5 + 0 + 1 + 2 + 1 = 9$ .

Inversiyalar sonining juft, toqligiga qarab o‘rin almashtirish **juft** yoki **toq** deyiladi.

O‘rin almashtirishdagi ikki sonni o‘rnini almashtirish **transpozitsiya** deyiladi. Va  $i$  va  $j$  sonlarning transpozitsiyasi ( $i, j$ ) bilan belgilanadi. Berilgan  $n$  ta sonning har qanday o‘rin almashtirishidan shu sonlarning istagan boshqa o‘rin almashtirishiga bir nechta transpozitsiyalarni bajarish bilan kelish mumkin bo‘lib, bunda  $n-1$  tadan ko‘p bo‘lmagan transpozitsiyalar bilan chegaralanishi mumkin. Misol. (312546) o‘rin almashtirishdan (631254) almashtirishga beshta: (3, 6), (3, 1), (1, 2), (2, 5), (5, 4) transpozitsiyalarni bajarish bilan kelish mumkin.

Berilgan  $1, 2, \dots, n$  sonlarning barcha  $n!$  o‘rin almashtirishlarning har bir keyingisi oldingisidan bitta transpozitsiyani bajarishdan hosil bo‘lgan tartibda (tushirib qoldirmaydigan va takrorlanmaydigan), birin-ketin joylashtirish mumkin. Har bir transpozitsiya bevosita o‘rin almashtirishning juft-toqligini o‘zgartiradi. Berilgan  $n \geq 2$  son uchun  $n$  ta sondan tuzilgan o‘rin almashtirishlardan juftlari soni bevosita toqlari soniga, ya’ni  $n!/2$  ga teng bo‘ladi.

Berilgan  $n$  ta  $1, 2, \dots, n$  sonlar to‘plamining o‘ziga o‘zaro bir qiymatli akslantirishiga (biyeksiyasiga) bu sonlarning **o‘rniga qo‘yish** yoki  **$n$ -tartibli o‘rniga qo‘yish** deyiladi. Shunday qilib, o‘rniga qo‘yishda 1 dan  $n$  gacha bo‘lgan har bir songa shu sonlardan qandaydir biri mos keltirilgan bo‘lib, ikkita har xil songa ikkita har xil son mos keladi. O‘rniga qo‘yish umumiyligi qavsga olingan ikkita satr ko‘rinishida, ya’ni yuqori satrda turgan har bir sonning tagida unga mos keluvchi sonni yozish bilan ifodalanadi. Masalan,  $\begin{pmatrix} 623451 \\ 436251 \end{pmatrix}$  o‘rniga qo‘yishda  $1 \rightarrow 1, 2 \rightarrow 3, 3 \rightarrow 6, 4 \rightarrow 2, 5 \rightarrow 5, 6 \rightarrow 4$  mos keltirilganligini bildiradi.

Sonlarning yuqori satrda joylashuviga qarab, bitta o‘rniga qo‘yishni bir nechta ko‘rinishda yozish mumkin. Masalan,

$$\begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \begin{pmatrix} 2134 \\ 4312 \end{pmatrix}, \begin{pmatrix} 3124 \\ 1342 \end{pmatrix}, \begin{pmatrix} 4123 \\ 2341 \end{pmatrix}$$

o‘rniga qo‘yishlarning barchasida 1 soni 3 ga, 2 soni 4 ga, 3 soni 1 ga, 4 soni 2 ga o‘tganligi sababli, ular aynan bitta o‘rniga qo‘yishni ifodalaydi. Berilgan  $n$  ta son yordamida tuzilgan har bir o‘rniga qo‘yishni  $n!$  har xil ko‘rinishlarda yozish mumkin. Bundan,  $n$  ta sondan tuzilgan har xil o‘rniga qo‘yishlar soni ham  $n!$  ga tengdir.

Agar o‘rniga qo‘yishning ikkala satridagi inversiyalar yig‘indisi juft bo‘lsa, o‘rniga qo‘yish **juft** deb, agar inversiyalar yig‘indisi toq bo‘lsa, **toq** deb aytildi. Demak, agar ikkala satrdagi inversiyalar bir xilda juft, yoki ikkalasi ham toq bo‘lsa, o‘rniga qo‘yish juft, agar har xil bo‘lsa o‘rniga qo‘yish toq bo‘ladi. O‘rniga qo‘yishning juft-toqligi uning ikkita satr yordamida ko‘rinishiga bog‘liq emas, ya’ni bitta o‘rniga qo‘yishning har xil ko‘rinishida inversiyalar juft-toqligi bir

xildir. Masalan,  $\begin{pmatrix} 3214 \\ 1324 \end{pmatrix} = \begin{pmatrix} 1234 \\ 2314 \end{pmatrix}$  o‘rniga qo‘yishning birinchi yozuvida to‘rtta, ikkinchisida ikkita inversiya bor, ya’ni juft.

Har qanday  $n$  elementdan tuzilgan juft o‘rniga qo‘yishlar soni toq o‘rniga qo‘yishlar soniga va demak,  $n!/2$  ga tengdir ( $n \geq 2$ ).

O‘rniga qo‘yishning juft-toqligini aniqlashning boshqa usuli ham bor. Bir nechta sonlar ketma-ketligida berilgan o‘rniga qo‘yishda birinchi son – ikkinchisiga, ikkinchisi – uchinchisiga va h.k oxirgisi – birinchisiga o‘tsa, bu sonlar **sikl** deb ataladi. Sikl undagi sonlarni umumiy qavslarga olib yozish bilan belgilanadi. Agarda son yana o‘ziga o‘tsa, u ham bitta siklni tashkil etadi. Umumiylar ega bo‘lmagan sikllar, **o‘zaro bog‘liq bo‘lmagan sikllar** deyiladi. Har qanday o‘rniga qo‘yishni o‘zaro bog‘liq bo‘lmagan sikllarga ajratish mumkin (yoki yoyish mumkin). Masalan,  $\begin{pmatrix} 123456 \\ 613542 \end{pmatrix} = (162)(45)(3)$ .

O‘rniga qo‘yishdagi elementlar soni  $n$  va uning yoyilmasidagi sikllar soni  $k$  ning ayirmasi bo‘lgan  $d$  soniga, ya’ni  $d = n - k$  ga, **o‘rniga qo‘yishning dekrementi** deyiladi. O‘rniga qo‘yishning juft-toqligi uning dekrementining juft-toqligi bilan bir xildir. Masalan:  $n = 6$ ,  $k = 3$ ,  $d = 3$  bo‘lib, o‘rniga qo‘yish toq.

$n$ -tartibli ikkita o‘rniga qo‘yishni ketma-ket bajarishdan hosil bo‘lgan o‘rniga qo‘yishga ularning **ko‘paytmasi** deyiladi. Masalan, agar  $a = \begin{pmatrix} 12345 \\ 31254 \end{pmatrix}$ ,

$$b = \begin{pmatrix} 12345 \\ 25314 \end{pmatrix}, \text{ bo‘lsa, u holda } ab = \begin{pmatrix} 12345 \\ 32541 \end{pmatrix} \text{ bo‘ladi.}$$

Agar siklni bevosita o‘rniga qo‘yish deb tushunsak, u holda o‘rniga qo‘yishni o‘zaro bog‘liq bo‘lmagan sikllarga yoyilmasiga uning shu sikllarning ko‘paytmasi ko‘rinishidagi ifodasi deb qarash mumkin. Agar  $1, 2, \dots, n$ , sonlarning o‘rniga qo‘yishda  $i_1$  son  $i_2$  ga,  $i_2 -- i_3$  ga, ...,  $i_{k-1} -- i_k$  ga ( $k \leq n$ ),  $i_k -- i_1$  ga o‘tib, golgan sonlar o‘ziga o‘tsa, bunday o‘rniga qo‘yishga **sikl** yoki **siklik o‘rniga qo‘yish** deyiladi va  $(i_1, i_2, \dots, i_k)$  ko‘rinishida belgilanadi.  $(i_1, i_2, \dots, i_k)$  va masalan,  $(i_2, i_3, \dots, i_k, i_1)$  sikllar o‘zaro tengdir.  $k$  soni esa **siklning uzunligi** deyiladi.

Uzunligi 1 ga teng sikl ko‘paytmada yozilmaydi. Masalan,  $\begin{pmatrix} 12345678 \\ 82157463 \end{pmatrix} = (183)(4576)$ . Uzunligi ikkiga teng sikl **transpozitsiy** deyiladi. Har qanday o‘rniga qo‘yishni transpozitsiyalar ko‘paytmasi shaklida ifodalash mumkin. Masalan,  $(i_1, i_2, \dots, i_k) = (i_1, i_2) (i_1, i_3) \dots (i_1, i_k)$ . Bu ifodalanish yagona emas, har qanday juft o‘rniga qo‘yishni juft sondagi transpozitsiyalar, toq o‘rniga qo‘yishni toq sondagi transpozitsiyalar ko‘paytmasi ko‘rinishida ifodalash mumkin.

**1-misol.** Agar FIRHS harfli o‘rin almashtirishni tartib deb qarab, unga nisbatan SHIFR o‘rin almashtirishining juft yoki toqligini aniqlang.

*Yechilishi.* Misolning shartiga binoan FIRHS harfli o‘rin almashtirish tartib ekan, demak uni quyidagicha belgilab olamiz:

F I R H S

1 2 3 4 5

Ushbu tartib bo‘yicha SHIFR quyidagicha o‘rin almashtirishni anglatadi: 5 4 2 1 3. Bundan S harfi 5 soni ekan, undan o‘ng tomondan kichik sonlar 4 inversiyani tashkil qiladi. Keyingi H harfi 4 soni ekan, undan o‘ng tomondan kichik sonlar 3 inversiyani, I harfi 2 soni ekan, undan o‘ng tomondan kichik sonlar 1 inversiyani, F harfi 1 soni ekan, undan o‘ng tomondan kichik sonlar 0 inversiyani hosil qiladi. Hammasi bo‘lib SHIFR o‘rin almashtirishida  $4+3+1+0=8$  ta inversiya bor. Demak, bu o‘rin almashtirish juft.

**2-misol.** Quyidagi  $(2n, 2n-2, \dots, 6, 4, 2, 2n-1, 2n-3, \dots, 5, 3, 1)$  o‘rin almashtirishida inversiyalar sonini toping. O‘rin almashtirishi juft bo‘ladigan  $n$  larning, va toq bo‘ladigan  $n$  larning umumiy ko‘rinishini ko‘rsating.

*Yechilishi.* Inversiyalar sonini hisoblaymiz:

$$(2n-1) + (2n-3) + \dots + 5 + 3 + 1 + (n-1) + (n-2) + \dots + 2 + 1 = \\ \frac{1+(2n-1)}{2} \cdot n + \frac{1+(n-1)}{2} \cdot (n-1) = n^2 + \frac{n(n-1)}{2} = \frac{1}{2}n(3n-1)$$

bundan  $n = 4k$  va  $n = 4k + 3$  bo‘lgandagina keltirilgan o‘rin almashtirish juft bo‘lishini ko‘ramiz.

**3-misol.** (9, 5, 1, 8, 3, 7, 4, 6, 2) o‘rin almashtirishdan (9, 8, 7, 6, 5, 4, 3, 2, 1) o‘rin almashtirishga o‘tish mumkin bo‘lgan transpozitsiyalarni ko‘rsating.

*Yechilishi.* Bu transpozitsiyalar quyidagilardan iborat ekanligini ko‘rish qiyin emas. (5, 8), (1, 7), (5, 6), (3, 5), (1, 4), (1, 3), (2, 1).

**4-misol.** Quyidagi o‘rin almashtirishni sikllar ko‘paytmasiga yoying va dekrement orqali juft-toqligini aniqlang

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ 2 & 1 & 4 & 3 & \dots & 2n & 2n-1 \end{pmatrix}.$$

*Yechilishi.* Har qanday berilgan o‘rniga qo‘yishni o‘zaro bog‘liq bo‘lmagan (1 2) (3 4) .... (2n-1, 2n) sikllarning ko‘paytmasi ko‘rinishida yoyish mumkin. Demak, uning dekrementi  $2n - n = n$  ga teng bo‘lib, o‘rniga qo‘yishning juft-toqligi  $n$  ning juft-toqligi bilan bir xildir.

**5-misol.** (3 2 1) (6 5 4) .... (3n, 3n-1, 3n-2) o‘rniga qo‘yishdagi sikllar yozuvidan ikki satrli yozuvga o‘ting.

*Yechilishi.* Birinchi sikldan 1 ning 3 ga, 3 ning 2 ga, 2 ning 1 ga o‘tishini ko‘ramiz. Ikkinci siklda 4 – 6 ga, 6 – 5 ga, 5 – 4 ga o‘tadi. Oxirgi siklda 3n -- 3n-1 ga, 3n-1 -- 3n-2 ga, 3n-2 esa 3n ga o‘tadi. Natijada, quyidagi o‘rniga qo‘yish hosil qilinadi:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 3 & 1 & 2 & 6 & 4 & 5 & \dots & 3n & 3n-2 & 3n-1 \end{pmatrix}.$$

**6-misol.** Hisoblang.

$$\begin{pmatrix} \alpha_1 \alpha_2 \dots \alpha_n \\ \beta_1 \beta_2 \dots \beta_n \end{pmatrix}^{-2} (\alpha_1 \alpha_2 \dots \alpha_n) \begin{pmatrix} \alpha_1 \alpha_2 \dots \alpha_n \\ \beta_1 \beta_2 \dots \beta_n \end{pmatrix}.$$

*Yechilishi.*

$$\begin{aligned} \left( \begin{array}{c} \beta_1 \beta_2 \dots \beta_n \\ \alpha_1 \alpha_2 \dots \alpha_n \end{array} \right) \left( \begin{array}{c} \alpha_1 \alpha_2 \dots \alpha_n \\ \alpha_2 \alpha_3 \dots \alpha_1 \end{array} \right) \left( \begin{array}{c} \alpha_1 \alpha_2 \dots \alpha_n \\ \beta_1 \beta_2 \dots \beta_n \end{array} \right) &= \left( \begin{array}{c} \beta_1 \beta_2 \dots \beta_n \\ \alpha_2 \alpha_3 \dots \alpha_1 \end{array} \right) \left( \begin{array}{c} \alpha_1 \alpha_2 \dots \alpha_n \\ \beta_1 \beta_2 \dots \beta_n \end{array} \right) = \\ \left( \begin{array}{c} \beta_1 \beta_2 \dots \beta_n \\ \beta_2 \beta_3 \dots \beta_1 \end{array} \right) &= (\beta_1 \beta_2 \dots \beta_n). \end{aligned}$$

**7-misol.** Agar

$$A = \begin{pmatrix} 12345 \\ 31254 \end{pmatrix}, B = \begin{pmatrix} 12345 \\ 42135 \end{pmatrix}, C = \begin{pmatrix} 12345 \\ 53124 \end{pmatrix}$$

bo‘lsa,  $A^{-1}XB=C$  tenglikdan  $X$  o‘rniga qo‘yishni toping.

*Yechilishi.*  $A^{-1}XB=C$  tenglikni chapdan  $A$  ga, o‘ngdan  $B^{-1}$  ga ko‘paytirsak,  $X=ACB^{-1}$  ni topgan bo‘lamiz.

$$B^{-1} = \begin{pmatrix} 12345 \\ 32415 \end{pmatrix} \text{ bo‘lganligi sababli,}$$

$$X = \begin{pmatrix} 12345 \\ 31254 \end{pmatrix} \begin{pmatrix} 12345 \\ 53124 \end{pmatrix} \begin{pmatrix} 12345 \\ 32415 \end{pmatrix} = \begin{pmatrix} 12345 \\ 35412 \end{pmatrix} \text{ ni hosil qilamiz.}$$

### Topshiriqlar

1. Berilgan o‘rin almashtirishlarning biridan ikkinchisiga o‘tish mumkin bo‘lgan transpozitsiyalarni ko‘rsating: (10, 1, 2, 8, 7, 4, 3, 6, 9, 5) o‘rin almashtirishdan (8, 9, 5, 1, 10, 7, 2, 3, 6, 4) o‘rin almashtirishga;
2.  $i$  va  $k$  larning (1, 2, 7, 4,  $i$ , 5, 6,  $k$ , 9) o‘rin almashtirish juft bo‘ladigan qiymatlarini toping.
3. Agar TOPKIR o‘rin almashtirish tartib deb garalsa, unda KRIPTO o‘rin almashtirishidagi inversiyalar sonini toping.
4. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (2, 4, 6, 8, 1, 3, 5, 7);
5. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (2, 4, 6, 8, 10, 1, 3, 5, 7, 9);
6. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang:  
(2, 4, 6, 8, 10, 12, 14, 1, 3, 5, 7, 9, 11, 13);

7. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (1, 3, 5, 7, 2, 4, 6, 8);
8. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (1, 3, 5, 7, 9, 2, 4, 6, 8, 10);
9. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (1, 3, 5, 2, 4, 6);
10. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (6, 1, 5 , 2, 4 , 3);
11. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (8, 1, 7, 2, 6, 3, 5, 4);
12. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (10, 1, 9, 2, 8, 3, 7, 4, 6, 5) ;
13. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (1, 4, 2, 5, 3, 6);
14. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang: (1, 4, 7, 2, 5, 8, 3, 6, 9);
15. Quyidagi o‘rin almashtirishdagi inversiyalar sonini toping. Shu bilan birga o‘rin almashtirishni juft yoki toq bo‘lishini aniqlang:  
(1, 4, 7, 10, 2, 5, 8, 11, 3, 6, 9, 12);
16. (1, 2,..., n) o‘rin almashtirishning k-chi o‘rnida turgan 1 soni nechta inversiyani hosil qiladi?
17. 1, 2, 3, ..., n o‘rin almashtirishning k-chi o‘rnida turgan n soni nechta inversiyani hosil qiladi?
18. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:
- $$\begin{pmatrix} 2 & 1 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}$$
19. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:

$$\begin{pmatrix} 4 & 2 & 1 & 3 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

20. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

21. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:

$$\begin{pmatrix} 2 & 1 & 3 & 2 & 4 \\ 2 & 3 & 4 & 2 & 1 \end{pmatrix}$$

22. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:

$$\begin{pmatrix} 1 & 3 & 4 & 2 & 3 \\ 4 & 3 & 1 & 2 & 3 \end{pmatrix}$$

23. Quyidagi binar munosabat o‘rniga qo‘yish bo‘lishi yoki bo‘lmasligini aniqlang:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 3 \\ 4 & 3 & 2 & 1 & 3 \end{pmatrix}$$

24. Quyidagi o‘rniga qo‘yishni o‘zaro bog‘liq bo‘lмаган sikllar ko‘paytmasi ko‘rinishida ifodalang va dekrement bo‘yicha uning juft-toqligini aniqlang:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 4 & 5 & 3 & 6 & 8 & 2 \end{pmatrix}$$

25. Quyidagi o‘rniga qo‘yishni o‘zaro bog‘liq bo‘lмаган sikllar ko‘paytmasi ko‘rinishida ifodalang va dekrement bo‘yicha uning juft-toqligini aniqlang:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 9 \end{pmatrix}$$

26. O‘rniga qo‘yishlarni ko‘paytiring:  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$

27. O‘rniga qo‘yishlarni ko‘paytiring:  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$

28. O‘rniga qo‘yishlarni ko‘paytiring:  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^2$

29. O‘rniga qo‘yishlarni ko‘paytiring:  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}^2$

30. Quyidagi o‘rniga qo‘yishda sikllar bo‘yicha yozuvlardan 2 ta satrlar bo‘yicha yozuvga o‘ting: ( 15 )( 234 );

31. Quyidagi o‘rniga qo‘yishda sikllar bo‘yicha yozuvlardan 2 ta satrlar bo‘yicha yozuvga o‘ting: (13) (25) (4);

32. Quyidagi o‘rniga qo‘yishda sikllar bo‘yicha yozuvlardan 2 ta satrlar bo‘yicha yozuvga o‘ting: ( 7531 ) ( 246 ) ( 8 ) ( 9 );

## 2.8. Matritsalar

Sonlardan tuzilgan va  $m$  ta satr va  $n$  ta ustunlardan iborat to‘g‘ri burchakli jadvalga **matritsa** deb aytildi:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Matritsaga misol sifatida quyidagi jadvalni keltirsa bo‘ladi:

$$\begin{pmatrix} -1 & 2 & 3 \\ 5 & 4 & -6 \end{pmatrix}.$$

Matritsa  $A$ ,  $B$ ,  $C, \dots$  harflar orqali belgilanadi.  $a_{ij}$  sonlar **matritsaning elementlari** deb aytildi. Matritsaning gorizontal qatoridagi sonlari uning **satrlari**, vertikal qatoridagi sonlari uning **ustunlari** deb aytildi. Matritsa  $m$  ta satrlarga va  $n$  ta ustunlarga ega bo‘lsa, uni  $m \times n$  **matritsa** deb aytildi. Agar  $m = n$  bo‘lsa, bunday matritsa  $n$ -tartibli kvadrat matritsa deb aytildi.

Agar  $A$  va  $B$  matritsalar berilgan bo'lsa va ularning satrlari va ustunlari soni mos ravishda teng bo'lsa, bunday matritsalar **nomdosh** matritsalar deb yuritiladi. Faqat nomdosh matritsalar teng bo'lishi mumkin.  $A$  ning har bir  $a_{ij}$  elementi va  $B$  ning unga mos  $b_{ij}$  elementiga teng bo'lsa, bu ikkita nomdosh matritsa teng, ya'ni  $A=B$  bo'ladi.

$B$  matritsa  $A$  matritsa bilan  $\alpha$  sonning ko'paytmasidan iborat deb aytiladi, agar ularning hamma elementlari uchun  $b_{ij} = \alpha a_{ij}$  tenglik bajarilsa ( $A$  va  $B$  matritsalarning o'lchovlari bir xil) va  $B = \alpha A$  deb belgilanadi.

Uchta  $A$ ,  $B$ ,  $C$  – matritsalar bir xil o'lchovli, ya'ni nomdosh bo'lsin.  $C$  matritsa  $A$  va  $B$  matritsalarning yig'indisi deb aytiladi va  $C=A+B$  deb belgilanadi, agar  $i$  va  $j$  indekslarning hamma qiymatlari uchun  $c_{ij} = a_{ij} + b_{ij}$  tenglik bajarilsa.

Faraz qilaylik,  $m \times n$  o'lchovli  $A = (a_{ij})$  va  $m \times p$  o'lchovli  $B = (b_{ij})$  matritsalar berilgan bo'lsin. Bu matritsalarning ko'paytmasi deb shunday  $C = AB = (c_{ik})$  matritsaga aytiladiki, uning elementlari quyidagi formula bilan beriladi:

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk} = \sum_{j=1}^n a_{ij}b_{jk}, \quad i=1,2,\dots,m; \quad k=1,2,\dots,p.$$

$B$  matritsa  $A$  matritsaga nisbatan **transponirlangan matritsa** deb aytiladi va  $B = A^T$  deb belgilanadi, agar  $B$  matritsaning ustunlari  $A$  matritsaning mos satrlari bo'lsa, ya'ni hamma  $i, j$  indekslar uchun  $b_{ij} = a_{ji}$ .  $A$  matritsadan  $A^T$  matritsaga o'tish amali  $A$  matritsani **transponirlash** deb aytiladi. Agar  $A$  matritsa  $m \times n$  o'lchovli bo'lsa,  $A^T$  matritsa  $n \times m$  o'lchovli bo'ladi.

$A$  matritsa **nol matritsa** deb aytiladi, agar uning hamma elementlari 0 ga teng bo'lsa va  $A=0$  deb belgalanadi.  $A$  matritsa  $i_0, j_0$  **indeksli birlik matritsa** deb aytiladi, agar  $a_{i_0 j_0} = 1$  bo'lib, qolgan elementlari nolga teng bo'lsa.

$a_{11}, a_{22}, \dots, a_{nn}$  elementlar  $n$  tartibli  $A = (a_{ij})$  kvadrat matritsaning bosh diagonalini tashkil qiladi va uning **diagonal elementlari** deb aytiladi. Matritsaning

diagonal elementlari yig‘indisi  $A$  matritsaning *izi* deb aytiladi va  $trA$  deb belgilanadi. Shunday qilib,  $trA = \sum_{i=1}^n a_{ii}$ .

Kvadrat matritsa diagonal matritsa deb aytiladi, agar uning diagonalida bo‘limgan elementlari 0 ga teng bo‘lsa, ya’ni  $a_{ij} = 0$ ,  $i \neq j$ .  $n$  tartibli diagonal matritsa  $diag(a_{11}, \dots, a_{nn})$  deb belgilanadi. Diagonal elementlari 1 ga teng bo‘lgan  $n$  tartibli diagonal matritsa **birlik matritsa** deb aytiladi va  $E$  yoki  $E_n$  deb belgilanadi. Birlik matritsaning elementlari  $\delta_{ij}$  deb belgilanadi:  $E = (\delta_{ij})$ ,

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \partial a,$$

Bir xil uzunlikdagi satrlarning **chiziqli kombinatsiyasi** deb, berilgan satrlarni chiziqli kombinatsiya koeffitsiyentlari deb ataluvchi sonlarga ko‘paytmalarining yig‘indisiga aytiladi.

Agar biror satr boshqalarining chiziqli kombinatsiyasidan iborat bo‘lsa, u holda berilgan satr bu satrlar orqali **chiziqli bog‘langan** deyiladi. Agar bir xil uzunlikdagi satrlarning hech biri qolganlari orqali chiziqli bog‘lanishda bo‘lmasa, bunday satrlar **chiziqli bog‘lanmagan** deyiladi.

Masalan,  $(-1, -7, 5, -3) = 2(1, -1, -2, -3) - 3(1, 2, -3, -1)$  tenglik birinchi satr qolgan ikki satrning chiziqli kombinatsiyasidan iborat ekanligini ko‘rsatadi.

**1-misol.** Matritsalarning chiziqli kombinatsiyasi topilsin:

$$2 \begin{pmatrix} 2 & 7 \\ -1 & 3 \end{pmatrix} - \begin{pmatrix} 5 & 4 \\ -2 & 1 \end{pmatrix} - 5 \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix} = \\ \begin{pmatrix} 2 \cdot 2 - 5 \cdot 1 & 2 \cdot 7 - 4 - 5 \cdot 0 \\ 2 \cdot (-1) - 2(-2) - 5 \cdot 0 & 2 \cdot 3 - 1 - 5 \cdot 8 \end{pmatrix} = \begin{pmatrix} -6 & 10 \\ 0 & -35 \end{pmatrix}$$

**2-misol.** Matritsalarning ko‘paytmasi topilsin:

$$A = \begin{pmatrix} 5 & 8 & -4 \\ 6 & 9 & -5 \\ 4 & 7 & -3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 2 & 5 \\ 4 & -1 & 3 \\ 9 & 6 & 5 \end{pmatrix}.$$

*Yechilishi.* Matritsalarni ko‘paytmasi formulasiga asosan quyidagi tenglik kelib chiqadi:

$$AB = \begin{pmatrix} 5 \cdot 3 + 8 \cdot 4 + (-4) \cdot 9 & 5 \cdot 2 + 8 \cdot (-1) + (-4) \cdot 6 & 5 \cdot 5 + 8 \cdot 3 + (-4) \cdot 5 \\ 6 \cdot 3 + 9 \cdot 4 + (-5) \cdot 9 & 6 \cdot 2 + 9 \cdot (-1) + (-5) \cdot 6 & 6 \cdot 5 + 9 \cdot 3 + (-5) \cdot 5 \\ 4 \cdot 3 + 7 \cdot 4 + (-3) \cdot 9 & 4 \cdot 2 + 7 \cdot (-1) + (-3) \cdot 6 & 4 \cdot 5 + 7 \cdot 3 + (-3) \cdot 5 \end{pmatrix} =$$

$$= \begin{pmatrix} 11 & -22 & 29 \\ 9 & -27 & 32 \\ 13 & -17 & 26 \end{pmatrix}.$$

Kvadrat matritsaning yuqori chap burchagini quyi o‘ng burchagi bilan tutashtiruvchi kesmada yotuvchi elementlar qatori matritsaning **bosh diagonali**, yuqori o‘ng burchagini quyi chap burchagi bilan tutashtiruvchi kesmadagi elementlar qatori **yordamchi diagonali** deyiladi.

Bir nechta bir xil uzunlikdagi satrlar yig‘indisi deganda, har bir elementi berilgan satrlardan mos elementlar yig‘indisidan iborat satrga aytildi. Satrni songa ko‘paytirish deganda uning har bir elementi shu songa ko‘paytirishdan hosil bo‘ladi.

Kvadrat matritsaning determinantini bevosita *determinantning hadlari* yig‘indisi bilan aniqlanadi. Bunda determinantning har bir hadi – matritsaning har bir satridan bittadan, har bir ustunidan bittadan olingan  $n$  ta elementlar ko‘paytmasiga teng bo‘lib, agar hosil qilingan o‘rniga qo‘yish juft bo‘lsa, bu ko‘paytma o‘z ishorasi bilan, agar o‘rniga qo‘yish toq bo‘lsa, teskari ishora bilan olinadi. Birinchi tartibli determinant o‘zining yagona elementiga teng. A matritsaning determinanti quyidagicha belgilanadi:  $\det A$  yoki  $|A|$ .

**1-misol.** Ikkinci tartibli determinant:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

**2-misol.** Uchinchi tartibli determinant:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

$A$  – matritsa  $n$ -chi tartibli kvadrat matritsa bo‘lsin.  $A$  matritsa uchun  $AB=BA=E$  tenglikni qanoatlantiruvchi  $B$  matritsa  $A$  ga **teskari matritsa** deyiladi va u  $B = A^{-1}$  ko‘rinishda belgilanadi.

$A$  matritsa **teskarilanuvchi** deb aytildi, agar  $\det A \neq 0$ , ya’ni  $A$  matritsa xosmas bo‘lsa.

Har qanday xosmas  $A$  matritsani faqat satrlar (yoki faqat ustunlar) elementar almashtirishlari yordamida birlik matritsaga keltirish mumkin. Elementar almashtirishlarni xuddi shunday ketma-ketlikda  $E$  birlik matritsaga tadbiq qilsak, teskari matritsa  $A^{-1}$  ni hosil qilamiz.  $A$  va  $E$  matritsalarni chiziq yordamida qo‘shni yozib ular ustida elementar almashtirishlarni bir vaqtida bijarish juda qulaydir.

2-mi s o l. Satrlarning elementar almashtirishlari yordamida teskari matritsa  $A^{-1}$  ni toping

$$A = \begin{pmatrix} 3 & -4 & 5 \\ 2 & -3 & 1 \\ 3 & -5 & -1 \end{pmatrix}.$$

*Yechilishi.* Quyidagilarni hosil qilamiz:

$$\begin{array}{c} \left( \begin{array}{ccc|ccc} 3 & -4 & 5 & 1 & 0 & 0 \\ 2 & -3 & 1 & 0 & 1 & 0 \\ 3 & -5 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_1-R_2} \left( \begin{array}{ccc|ccc} 1 & -1 & 4 & 1 & -1 & 0 \\ 2 & -3 & 1 & 0 & 1 & 0 \\ 3 & -5 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_2-2R_1} \\ \xrightarrow{R_2-2R_1} \left( \begin{array}{ccc|ccc} 1 & -1 & 4 & 1 & -1 & 0 \\ 0 & -1 & -7 & -2 & 3 & 0 \\ 3 & -5 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_3-3R_1} \left( \begin{array}{ccc|ccc} 1 & -1 & 4 & 1 & -1 & 0 \\ 0 & -1 & -7 & -2 & 3 & 0 \\ 0 & -2 & -13 & -3 & 3 & 1 \end{array} \right) \xrightarrow{R_3-2R_2} \\ \xrightarrow{R_3-2R_2} \left( \begin{array}{ccc|ccc} 1 & -1 & 4 & 1 & -1 & 0 \\ 0 & -1 & -7 & -2 & 3 & 0 \\ 0 & 0 & 1 & 1 & -3 & 1 \end{array} \right) \xrightarrow{R_1-4R_3} \left( \begin{array}{ccc|ccc} 1 & -1 & 0 & 3 & 11 & -4 \\ 0 & -1 & -7 & -2 & 3 & 0 \\ 0 & 0 & 1 & 1 & -3 & 1 \end{array} \right) \xrightarrow{R_2+7R_1} \\ \xrightarrow{R_2+7R_1} \left( \begin{array}{ccc|ccc} 1 & -1 & 0 & -3 & 11 & -4 \\ 0 & -1 & 0 & 5 & -18 & 7 \\ 0 & 0 & 1 & 1 & -3 & 1 \end{array} \right) \xrightarrow{R_1-R_2} \left( \begin{array}{ccc|ccc} 1 & 0 & 0 & -8 & 29 & -11 \\ 0 & -1 & 0 & 5 & -18 & 7 \\ 0 & 0 & 1 & 1 & -3 & 1 \end{array} \right) \xrightarrow{(-1)R_2} \\ \xrightarrow{(-1)R_2} \left( \begin{array}{ccc|ccc} 1 & 0 & 0 & -8 & 29 & -11 \\ 0 & 1 & 0 & -5 & 18 & -7 \\ 0 & 0 & 1 & 1 & -3 & 1 \end{array} \right). \end{array}$$

Bunda  $R_i$  matritsaning  $i$ -chi satri.

Shunday qilib, teskari matritsa quyidagi ko‘rinishga ega bo‘ladi:

$$A^{-1} = \begin{pmatrix} -8 & 29 & -11 \\ -5 & 18 & -7 \\ 1 & -3 & 1 \end{pmatrix}.$$

### Topshiriqlar

1. Matritsalarning chiziqli kombinatsiyasi topilsin:

$$3\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix} - 4\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix};$$

2. Matritsalarning ko‘paytmasi hisoblansin:

$$\begin{pmatrix} 2 & -3 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix};$$

3. Hisoblang

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}^3;$$

4. Matritsalarning ko‘paytmasi hisoblansin:

$$\begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix} \begin{pmatrix} 2 & -3 & 0 \end{pmatrix}$$

5. Determinantni hisoblang:  $\begin{vmatrix} -1 & 5 & 4 \\ 3 & -2 & 0 \\ -1 & 3 & 6 \end{vmatrix}$

6. Matritsalarning ko‘paytmasi hisoblansin:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 5 & 9 \end{pmatrix}$$

7. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

8. Matritsalarning ko‘paytmasi hisoblansin:

$$(1 \ 0) \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

9.  $A \times B = AB - BA$  ( $A$  va  $B$  matritsalarning kommutatori) matritsani hisoblang, agar:

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

10. Quyidagi tenglamalardan  $X$  matritsani toping:

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} X = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

11. Matritsalarning ko‘paytmasi hisoblansin:

$$(0 \ 1 \ 0 \ 0) \begin{pmatrix} 1 & 4 & 3 \\ 0 & 3 & 2 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

12. Matritsalarning ko‘paytmasi hisoblansin:

$$\left( \begin{array}{cccc} 3 & 3 & -4 & -3 \\ 0 & 6 & 1 & 1 \\ 5 & 4 & 2 & 1 \\ 2 & 3 & 3 & 2 \end{array} \right) \left( \begin{array}{c} 0 \\ 1 \\ 0 \\ 0 \end{array} \right)$$

13. Matritsalarning ko‘paytmasi hisoblansin:

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

14. Matritsalarning ko‘paytmasi hisoblansin:

$$(1 \ 1 \ 1) \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$$

15. Matritsalarining ko‘paytmasi hisoblansin:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

16. Matritsalarining ko‘paytmasi hisoblansin:

$$\begin{pmatrix} -1 & 1 & 1 \\ -5 & 21 & 17 \\ 6 & -26 & -21 \end{pmatrix}^2;$$

17. Hisoblang  $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^n$ ;

18. Hisoblang  $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}^n$

19. Hisoblang  $\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}^n$ ;

20. Hisoblang  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$ ;

21. Hisoblang  $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}^n$ ;

22.  $A \times B = AB - BA$  ( $A$  va  $B$  matritsalarining kommutatori) matritsani hisoblang, agar:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

23. Determinantlarni hisoblang:  $\begin{vmatrix} 3 & 5 \\ 5 & 8 \end{vmatrix}$

24. Matritsalarining chiziqli kombinatsiyasi topilsin:

$$2 \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} - 3 \begin{pmatrix} 0 \\ 5 \\ 6 \end{pmatrix};$$

25, Determinantlarni hisoblang:  $\begin{vmatrix} ab & ac \\ bd & cd \end{vmatrix}$

26, Determinantlarni hisoblang:  $\begin{vmatrix} \sin \alpha & \sin \beta \\ \cos \alpha & \cos \beta \end{vmatrix}$

27, Determinantlarni hisoblang:  $\begin{vmatrix} \log_b a & 1 \\ 1 & \log_a b \end{vmatrix}$

28. Determinantni hisoblang:  $\begin{vmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{vmatrix}$

29. Determinantni hisoblang:  $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$

30. Determinantni hisoblang:  $\begin{vmatrix} 0 & a & 0 \\ b & c & d \\ 0 & e & 0 \end{vmatrix}$

31. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

32. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

33. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix}$$

34. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \end{pmatrix}$$
35. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 0 \end{pmatrix}$$
36. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$
37. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$$
38. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 2 & 7 & 3 \\ 3 & 9 & 4 \\ 1 & 5 & 3 \end{pmatrix}$$
39. Elementar almashtirishlar yordamida berilgan matritsa uchun teskari matritsani toping:
- $$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix}$$
40. Quyidagi tenglamalardan  $X$  matritsani toping:
- $$X \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

### **3-bob. SIMMETRIK KALITLI SHIFRLASH TIZIMLARI**

Kriptografiyada o‘chmas iz qoldirgan usullar ushbu bobda to‘plangan bo‘lib, bevosita asrlar davomida jamlangan bilimlar talabalarga tushunarli shaklda yoritib berilgan. Paragraf oxirida keltirilgan topshiriqlar talabalar bilimlarini mustahkamlashga yordam beradi. Keltirilgan usullar hozirgi kunda ham o‘z dolzarbligini saqlab qo‘lib, zamonaviy usullardan qisman bo‘lsada o‘rin egallagan. Ushbu usullar birinchi bobda keltirilgan tasnif asosida ketma-ket keltirilgan. Keltirilgan usullar talabalarda qiziqish uyg‘otishi va kelgusida yanada mukammal usullar yaratilishlariga asos bo‘lib xizmat qiladi.

#### **3.1. O‘rniga qo‘yish usuli**

O‘rniga qo‘yish usullarining mohiyati bir alifboda yozilgan boshlang‘ich axborotning belgilarini ma’lum bir qoida bo‘yicha boshqa alifbodagi belgilar bilan almashtirishdadir. Bunda belgilar ketma-ketligi boshqa belgilar ketma-ketligi bilan almashtiriladi. Olingan shifrlangan matn o‘rniga qo‘yish shifri deb ataladi.

Shunday qilib, o‘rniga qo‘yish shifri – bu bevosita ochiq matnning bir belgisini boshqa belgilarga almashtirish yo‘li bilan shifrlash usuli hisoblanadi.

**To‘g‘ridan-to‘g‘ri o‘rniga qo‘yish usuli** eng oddiy hisoblanadi. Boshlang‘ich axborot yoziladigan boshlang‘ich  $A_o$  alifboning belgilari ketma-ketligi mos ravishda ixtiyoriy tartiblangan, shifrllovchi  $A_m$  alifboning belgilariga mos holda qo‘yiladi. Oddiy holatda ikkala alifbo ham bir belgilar to‘plamidan tashkil topishi mumkin. Masalan, ikkala alifbo ham rus yoki ingliz alifbo harflarini o‘z ichiga olishi mumkin.

Ikkala alifbolarning belgilari o‘rtasidagi muvofiqlikni berilishi ma’lum bir algoritm bo‘yicha uzunligi  $k$  ta belgilardan tashkil topgan boshlang‘ich  $T_o$  matnning belgilarini sonli teng kuchlilarini o‘zgartirish yordamida amalga oshiriladi.

### O‘rniga qo‘yish jadvali

A <sub>o</sub>	A	B	C	D	E	F	G	H	I	J	K	L	M
i	1	2	3	4	5	6	7	8	9	10	11	12	13
A <sub>m</sub>	U	V	X	B	G	Y	K	R	W	A	F	M	Q

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	27
H	L	E	_	I	J	Z	T	C	S	N	P	O	D

O‘rniga qo‘yish jadvalini ishlatish shifrlash jarayonini sezilarli soddalashtiradi. Shifrlashda boshlang‘ich matn belgisi jadvalning A<sub>o</sub> qatoridagi belgilar bilan taqqoslanadi. Agar taqqoslangan belgi i-ustunda mos kelsa, unda boshlang‘ich matn belgisi jadvalning o‘sha i-ustunida joylashgan, A<sub>m</sub> qatoridagi belgi bilan almashtiriladi.

Deshifrlash jarayoni ham shunga o‘xhash amalga oshiriladi, lekin jadvalga kirish A<sub>m</sub> qator bo‘yicha amalga oshiriladi.

To‘g‘ridan-to‘g‘ri o‘rniga qo‘yish usulining asosiy kamchiligi – bu boshlang‘ich va yopiq matnlarining bir xil statistik tavsiflarini mavjudligidadir.

Boshlang‘ich matn qaysi tilda yozilganini va bu tilning alifbolari belgilarini ishlatishni<sup>IT</sup> chastotali tavsifini bilgan holda, kriptotahlil qiluvchi ushlab olingan ma’lumotlarni statistik qayta ishlash yo‘li bilan ikkala alifbolarning belgilari o‘rtasidagi muvofiqlikni o‘rnatishi mumkin.

O‘rniga qo‘yish usulini quyidagi misolda ko‘rib chiqamiz.

**Misol:** “TELEFON” so‘zini o‘rniga qo‘yish usuli yordamida shifrlang. Bu misolda quyidagilar berilgan: Shifrlanadigan so‘z T<sub>o</sub>=<TELEFON> va shifrllovchi jadval (bu yerda 2-jadval). Shifrlangan T<sub>m</sub> so‘zini aniqlang.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
U	V	X	B	G	Y	K	R	W	A	F	M	Q	H	L

P	Q	R	S	T	U	V	W	X	Y	Z	_
↓	↑	↓	↓	↑	↓	↑	↓	↑	↓	↓	↑
E	_	I	J	Z	T	C	S	N	P	O	D

3-jadval

T	E	L	E	F	O	N
↓	↑	↓	↑	↓	↓	↑
Z	G	M	G	Y	L	H

Demak shifrlangan xabar:  $T_m = \langle ZGMGYLH \rangle$ .

Shifrlangan xabarni deshifrlash ya'ni shifrdan ochishda shifrlash jarayoniga teskari amal bajariladi:

4-jadval

U	V	X	B	G	Y	K	R	W	A	F	M	Q	H	L
↓	↑	↓	↑	↓	↑	↓	↑	↓	↑	↓	↓	↑	↓	↑
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

E	_	I	J	Z	T	C	S	N	P	O	D
↓	↑	↓	↑	↑	↓	↑	↓	↑	↓	↑	↑
P	Q	R	S	T	U	V	W	X	Y	Z	_

5-jadval

Z	G	M	G	Y	L	H
↓	↑	↓	↑	↓	↓	↑
T	E	L	E	F	O	N

Demak maxfiy xabar:  $T_o = \langle TELEFON \rangle$ .

### Topshiriq

Quyida berilgan ( $T_o$ ) so'zlardan shifrlangan xabarni ( $T_m$ ) aniqlang va teskari jarayon orqali deshifrlang.

Variantlar

№	Shifrlanadigan so'z ( $T_o$ )	№	Shifrlanadigan so'z ( $T_m$ )
1	DASTURIY_QAROQCHILIK	26	TELEVIZOR_KANALI
2	BIBLIOGRAFIK_TAVSIF	27	YULDUZLAR_JILOSI
3	TEZYORDAM_MASHINASI	28	KASALXONA_BINOSI

4	DASTURIY_VOSITALAR	29	KUTUBXONA_KITABI
5	TAQINCHOQLAR_NARXI	30	KOSMONAVTLAR_UYI
6	YILPIGICHLAR_RANGI	31	QIZIQ_MATEMATIKA
7	UNIVERSITET_BINOSI	32	YANGI_MUZLATGICH
8	DASTURIY_JAMLANMA	33	BAZIS_VARIANTLAR
9	AXBOROT_ESKIRISHI	34	KARNAY_SURNAYCHI
10	AXBOROT_BUTUNLIGI	35	TILLA_TISHCHALAR
11	DASTURIY_MAHSULOT	36	BILIMLAR_OMBORI
12	AXBOROT_AGENTLIGI	37	AXBOROT_BIZNESI
13	DASTURIY_ILOVALAR	38	AXBOROT_BALANSI
14	MILITSIYA_IDORASI	39	DIREKTOR_XONASI
15	QULUPNAY_SHARBATI	40	ASKARLAR_HAYOTI
16	RAQAMLAR_AYIRMASI	41	BUYRUQLAR_SATRI
17	SHAFTOLI_SHARBATI	42	YANGI_DAFTARLAR
18	FOTOAPPARAT_QISMI	43	TISH_DOKTORLARI
19	YANGI_TEXNOLOGIYA	44	AXBOROT_BOZORI
20	BOSHQARUV_XONASI	45	VAQT_MASHINASI
21	BANKLARARO_TIZIM	46	BOSH_SAHFACHI
22	BANNER_REKLAMASI	47	BULL_ALGEBRASI
23	DASTURNI_SOZLASH	48	BANYAN_TARMOQ
24	TELEFON_TRUBKASI	49	BETA_TESTLASH
25	QOVURILGAN_BALIQ	50	BOSH_MUHARRIR

### 3.2. Monoalifboli o‘rniga qo‘yish usuli

Monoalifboli o‘rniga qo‘yish usullari sifatida quyidagi usullarni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch so‘zli Sezar usuli va boshqalar.

Monoalifboli shifrlash usuli – bu ma’lum algoritmga muvofiq shifrlash jadvalini yaratishga asoslangan shifrlash usullari sinfi bo‘lib, unda ochiq matnning har bir harfi uchun maxfiy algoritm asosida hosil bo‘lgan shifrmatnning mos harfi mavjud bo‘ladi. Bu usulda shifrlash jadvalga muvofiq harflarni almashtirishdan iborat. Shifrni ochish uchun bir xil jadvalga ega bo‘lish yoki uni tuzish algoritmini

bilish kifoya. Monoalifboli o‘rniga qo‘yish algoritmi quyidagi qadamlar ketma-ketligidan iborat:

**1-qadam.**  $T_o$  ochiq xabarning har bir belgisi mos ravishda  $[1xR]$  o‘lchamli tanlangan  $A_o$  alifbodagi har bir belgining tartib raqamiga mos keluvchi  $L_o$  songa almashtiriladi.

**2-qadam.**  $L_o$  sonlar ketma-ketligining har bir sonini

$$L_m = (k_1 * L_o + k_2) * (\text{mod } R)$$

formula orqali hisoblanuvchi  $L_m$  songa almashtiriladi, bu yerda  $k_1$ -o‘nlik koeffitsienti;  $k_2$ -siljитish koeffitsienti. Tanlangan  $k_1$ ,  $k_2$  koeffitsentlar  $L_o$ ,  $L_m$  sonlarning bir ma’noli mosligini ta’minlashi lozim.

**Eslatma:**  $L_m=0$  olinganida esa  $L_m=R$  ( $R$  – alifbodagi belgilar soni) almashinuvi bajarilishi kerak.

**3-qadam.**  $L_m$  ketma-ketlikning har bir sonini  $[1xR]$  o‘lchamli shifrlash alifbosining mos  $A_m$  alifbo belgisi bilan almashtirish yo‘li bilan  $T_m$  shifrmatn hosil qilinadi.

**4-qadam.** Olingan shifrmatn o‘zgarmas  $b$  uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to‘liq bo‘lmasa blok orqasiga maxsus belgi – to‘ldiruvchilar joylashtiriladi (masalan, \*).

**Misol.** Shifrlash uchun dastlabki ma’lumotlar quyidagilar:

$T_o = <\text{KIBER\_XAVFSIZLIK}>$ ;

$$R=27; \quad k_1=4; \quad k_2=17; \quad b=4.$$

1-jadval

<b>A<sub>o</sub></b>	A	B	C	D	E	F	G	H	I	J	K	L	M
<b>L<sub>o</sub></b>	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>L<sub>m</sub></b>	21	25	2	6	10	14	18	22	26	3	7	11	15
<b>A<sub>m</sub></b>	U	Y	B	F	J	N	R	V	Z	C	G	K	O

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	27
19	23	0	4	8	12	16	20	24	1	5	9	13	17
S	W	_	D	H	L	P	T	X	A	E	I	M	Q

Algoritmning qadamma-qadam bajarilishida quyidagi natijalar olindi:

2-jadval

A <sub>o</sub>	K	I	B	E	R	_	X	A	V	F	S	I	Z	L	I	K
L <sub>o</sub>	11	9	2	5	18	27	24	1	22	6	19	9	26	12	9	11
L <sub>m</sub>	7	26	25	10	8	17	5	21	24	14	12	26	13	11	26	7
A <sub>m</sub>	G	Z	Y	J	H	Q	E	U	X	N	L	Z	M	K	Z	G

1-qadam. L<sub>o</sub>=<11, 9, 2, 5, 18, 27, 24, 1, 22, 6, 19, 9, 26, 12, 9, 11>

2-qadam. L<sub>m</sub>=<7, 26, 25, 10, 8, 17, 5, 21, 24, 14, 12, 26, 13, 11, 26, 7>

3-qadam. T<sub>m</sub>=<GZYJHQEU XNLZ MKZG>

4-qadam. T<sub>m</sub>=<GZYJ HQEU XNLZ MKZG>

Shifr ma'lumotni deshifrlashda (shifrdan ochishda) bloklar birlashtirilib K belgili shifrmatn T<sub>m</sub> hosil qilinadi. Deshifrovka qilish uchun quyidagi butun sonli tenglamani yechish lozim:

$$k_1 L_o + k_2 = n R + L_m,$$

bu yerda k<sub>1</sub>, k<sub>2</sub>, L<sub>m</sub> va R butun sonlar ma'lum bo'lganda L<sub>o</sub> kattaligi n soni saralash orqali hisoblanadi (n=0, 1, 2, ...).

1-qadam. T<sub>m</sub>=<GZYJ HQEU XNLZ MKZG>

2-qadam. T<sub>m</sub>=<GZYJHQEU XNLZ MKZG>

3-qadam. L<sub>m</sub>=<7, 26, 25, 10, 8, 17, 5, 21, 24, 14, 12, 26, 13, 11, 26, 7>

4-qadam. R=27;            k<sub>1</sub>=4;            k<sub>2</sub>=17;            L<sub>m</sub>=7.

$$4 * L_o + 17 = n * 27 + 7;$$

$$L_o = \frac{27 * n - 10}{4};$$

1 ≤ L<sub>o</sub> ≤ R – shartni qanoatlantiruvchi, butun qiymatli L<sub>o</sub> ni qidiramiz:

n=0 da L<sub>o</sub> = -2,5 – bu yuqoridagi shartni qanoatlantirmaydi;

n=1 da L<sub>o</sub> = 4,25 – bu yuqoridagi shartni qanoatlantirmaydi;

n=2 da L<sub>o</sub> = 11 – bu yuqoridagi shartga mos keladi.

Demak, n=2, L<sub>o</sub>=11 ekan. Ushbu jarayonni shifrmatnning barcha belgilariga tadbiq qilish uning deshifrlanishiga olib keladi.

Bu usulning kamchiligi sifatida dastlabki va berilgan matnlar statistik xarakteristikalarining bir xilligidir. Dastlabki matn qaysi tilda yozilganligini bilgan kriptoanalitik ushlab qolingga axborotlarni statistik qayta ishlab, ikkala alifbodagi belgilar o‘rtasidagi muvofiqlikni aniqlashi mumkin bo‘ladi.

### **Topshiriq**

Quyidagi ( $T_o$ ) so‘zlarni berilgan qiymatlar yordamida shifrlang ( $T_m$ ) va teskari jarayon orqali deshifrlang. Bu yerda  $R=27$ ;  $k_1=3$ ;  $k_2=15$ ;  $b=5$ .

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_o</math>)</b>	<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_o</math>)</b>
1	DASTURIY_QAROQCHILIK	26	TELEVIZOR_KANALI
2	BIBLIOGRAFIK_TAVSIF	27	YULDUZLAR_JILOSI
3	TEZYORDAM_MASHINASI	28	KASALXONA_BINOSI
4	DASTURIY_VOSITALAR	29	KUTUBXONA_KITOBI
5	TAQINCHOQLAR_NARXI	30	KOSMONAVTLAR_UYI
6	YILPIGICHLAR_RANGI	31	QIZIQ_MATEMATIKA
7	BINOSI_UNIVERSITET	32	YANGI_MUZLATGICH
8	DASTURIY_JAMLANMA	33	BAZIS_VARIANTLAR
9	AXBOROT_ESKIRISHI	34	KARNAY_SURNAYCHI
10	AXBOROT_BUTUNLIGI	35	TILLA_TISHCHALAR
11	DASTURIY_MAHSULOT	36	BILIMLAR_OMBORI
12	AXBOROT_AGENTLIGI	37	AXBOROT_BIZNESI
13	DASTURIY_ILOVALAR	38	AXBOROT_BALANSI
14	MILITSIYA_IDORASI	39	DIREKTOR_XONASI
15	QULUPNAY_SHARBATI	40	ASKARLAR_HAYOTI
16	RAQAMLAR_AYIRMASI	41	BUYRUQLAR_SATRI
17	SHAFTOLI_SHARBATI	42	YANGI_DAFTARLAR
18	FOTOAPPARAT_QISMI	43	TISH_DOKTORLARI
19	YANGI_TEXNOLOGIYA	44	AXBOROT_BOZORI
20	BOSHQARUV_XONASI	45	VAQT_MASHINASI
21	BANKLARARO_TIZIM	46	BOSH_SAHFACHA
22	BANNER_REKLAMASI	47	BULL_ALGEBRASI
23	DASTURNI_SOZLASH	48	BANYAN_TARMOQ
24	TELEFON_TRUBKASI	49	BETA_TESTLASH
25	QOVURILGAN_BALIQ	50	BOSH_MUHARRIR

### 3.2.1. Sezar usuli

Qadimgi Rim imperatori Yuliy Sezar axborotni maxfiyligini saqlash uchun o‘zining matnni shifrlash usulini o‘ylab topgan.

**Sezar shifri** – bu shifrlash usuli ko‘p adabiyotlarda **siljitim usuli** ham deb nomlangan, eng oson va eng keng tarqalgan shifrlash usuli hisoblanadi. Sezar shifri ham almashtirish usullariga asoslangan bo‘lib, unda oddiy matndagi har bir belgi alifboda chapga yoki uning o‘ng tomonidagi o‘zgarmas sonlarda joylashgan belgilar bilan almashtiriladi. Masalan, o‘ng tomonga siljishi bo‘lgan shifrda A o‘rniga M, B ga N va boshqalar almashishadi.

Qadimda Yuliy Sezar o‘z shifridan Sitseron (miloddan avvalgi 106-43 yillar) bilan axborot almashishda foydalangani ma’lum. Turli davrlarda bu tizimning turli shakllaridan foydalanib kelingan. Dastlabki matnning qanday berilishi ahamiyatga ega emas. Sezar usulida shifrlash dastlabki matnga tegishli alifbo harfi o‘rniga shifr-lash kaliti *k* qadamga surilgan o‘rinda joylashgan alifbo harfini qo‘yish asosida amal-ga oshiriladi (1-jadval). Bu yerda bo‘sh katak ham alifboga kiritilgan. Bunda surish alifbo harflari soni 27 ga teng bo‘lgan modul bo‘yicha bajariladi. Alifbo harflari boshidan oxiri tomon va oxiridan qayta bosh tomon davriy ravishda surib boriladi.

**Misol.** Shifrlanadigan xabar  $T_o = <\text{SHER}>$ ,  $k=3$ ,  $T_m=?$  bo‘lgan hol uchun quyidagi ko‘rinishga ega bo‘lamiz:

1-jadval.

Sezar usulida shifrlash

<b>№</b>	0	1	2	3	<b>4</b>	5	6	<b>7</b>	8	9	10	11	12
<b>T<sub>o</sub></b>	A	B	C	D	<b>E</b>	F	G	<b>H</b>	I	J	K	L	M
<b>T<sub>m</sub></b>	D	E	F	G	<b>H</b>	I	J	<b>K</b>	L	M	N	O	P

13	14	15	16	<b>17</b>	<b>18</b>	19	20	21	22	23	24	25	26
N	O	P	Q	<b>R</b>	<b>S</b>	T	U	V	W	X	Y	Z	_
Q	R	S	T	<b>U</b>	<b>V</b>	W	X	Y	Z	_	A	B	C

Xabardagi harflar 1-jadvalda qalin shiftda ko‘rsatilgan, bu holda dastlabki matn  $T_o = <\text{SHER}>$  ni shifrlash natijasi  $T_m = <\text{VKHU}>$  bo‘ladi.

Endi teskarilash jarayonini ko‘rib chiqamiz. Bu yerda  $T_m = \text{VKHU}$  bo‘ladi va  $k=3$  bo‘lganda,  $T_o$  ni aniqlash talab etiladi. Quyidagi 2-jadvalda harflar qalin shriftda ko‘rsailgan:

2-jadval.

<b>№</b>	0	1	2	3	<b>4</b>	5	6	<b>7</b>	8	9	10	11	12
<b>T<sub>m</sub></b>	D	E	F	G	<b>H</b>	I	J	<b>K</b>	L	M	N	O	P
<b>T<sub>o</sub></b>	A	B	C	D	<b>E</b>	F	G	<b>H</b>	I	J	K	L	M

13	14	15	16	<b>17</b>	<b>18</b>	19	20	21	22	23	24	25	26
Q	R	S	T	<b>U</b>	<b>V</b>	W	X	Y	Z	_	A	B	C
N	O	P	Q	<b>R</b>	<b>S</b>	T	U	V	W	X	Y	Z	_

Demak, dastlabki ochiq xabar:  $T_o = \text{SHER}$ .

Sezar tizimi va unga o‘xhash tizimlarni, ya’ni harflarni alifbodagi tartib raqami bilan almashtirishni, sonlar ustida modul bo‘yicha oddiy qo‘shish amali (+) yordamida tushuntirish mumkin. Sezar tizimiga muvofiq, shifrmatn hosil qilishda dastlabki matnning har bir  $x$  harfi shifrmatnda quyidagi formula asosida:

$$y \equiv (x + k) \pmod{n}$$

$y$  harfiga aylanadi. Dastlabki matn harfi ( $n$  – bu alifbo quvvati)

$$x \equiv (y + n - k) \pmod{n}$$

ko‘rinishda tiklanadi.

Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir. Kriptotahlilda harflarning takrorlanish chastotasi yordamida bu usulda shifrlangan matn tezgina deshifrlanishi mumkin.

### Topshiriq

Quyida berilgan ( $T_o$ ) so‘zlardan berilgan kalit ( $k$ ) yordamida shifrlangan xabarni ( $T_m$ ) aniqlang va teskari jarayon orqali deshifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_o</math>)</b>	<b>(k)</b>	<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_o</math>)</b>	<b>(k)</b>
1	DASTURIY_QAROQCHILIK	26	26	TELEVIZOR_KANALI	1
2	BIBLIOGRAFIK_TAVSIF	25	27	YULDUZLAR_JILOSI	26
3	TEZYORDAM_MASHINASI	24	28	KASALXONA_BINOSI	25
4	DASTURIY_VOSITALAR	23	29	KUTUBXONA_KITOBI	24
5	TAQINCHOQLAR_NARXI	22	30	KOSMONAVTLAR_UYI	23
6	YILPIGICHLAR_RANGI	21	31	QIZIQ_MATEMATIKA	22

7	UNIVERSITET_BINOSI	20	32	YANGI_MUZLATGICH	21
8	DASTURIY_JAMLANMA	19	33	BAZIS_VARIANTLAR	20
9	AXBOROT_ESKIRISHI	18	34	KARNAY_SURNAYCHI	19
10	AXBOROT_BUTUNLIGI	17	35	TILLA_TISHCHALAR	18
11	DASTURIY_MAHSULOT	16	36	BILIMLAR_OMBORI	17
12	AXBOROT_AGENTLIGI	15	37	AXBOROT_BIZNESI	16
13	DASTURIY_ILOVALAR	14	38	AXBOROT_BALANSI	15
14	MILITSIYA_IDORASI	13	39	DIREKTOR_XONASI	14
15	QULUPNAY_SHARBATI	12	40	ASKARLAR_HAYOTI	13
16	RAQAMLAR_AYIRMASI	11	41	BUYRUQLAR_SATRI	12
17	SHAFTOLI_SHARBATI	10	42	YANGI_DAFTARLAR	11
18	FOTOAPPARAT_QISMI	9	43	TISH_DOKTORLARI	10
19	YANGI_TEXNOLOGIYA	8	44	AXBOROT_BOZORI	9
20	BOSHQARUV_XONASI	7	45	VAQT_MASHINASI	8
21	BANKLARARO_TIZIM	6	46	BOSH_SAHFACHI	7
22	BANNER_REKLAMASI	5	47	BULL_ALGEBRASI	6
23	DASTURNI_SOZLASH	4	48	BANYAN_TARMOQ	5
24	TELEFON_TRUBKASI	3	49	BETA_TESTLASH	4
25	QOVURILGAN_BALIQ	2	50	BOSH_MUHARRIR	3

### 3.2.2. Affin tizimidagi Sezar usuli

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi:  $at+b \pmod{m}$ , bu yerda  $a$ ,  $b$  - butun sonlar,  $0 \leq a$ ,  $b < m$ ,  $\text{EKUB}(a,m)=1$ . Quyida  $m=26$ ,  $a=3$  va  $b=5$  bo‘lganda hosil bo‘lgan jadval keltirilgan va shunga mos ravishda harflar almashtiriladi:

T	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
alifbo	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$3t+5$	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2
Harf	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

Natijada yuqorida keltirilgan **SAMARQAND** matni quyidagicha shifrlanadi:  
**HFPFEBFSO.**

### Topshiriq

Quyidagi jadvalda berilgan so‘zlarni Affin tizimidagi Sezar usulida quyidagi  $at+b \pmod{26}$  formula bo‘yicha shifrlang va deshifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>at+b</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>at+b</b>
1	QAROQCHILIK	7t+5	26	TELEVIZOR	23t+5
2	BIBLIOGRAFIK	3t+7	27	YULDUZLAR	7t+1
3	TEZYORDAM	3t+9	28	KASALXONA	3t+3
4	VOSITALAR	5t+1	29	KUTUBXONA	3t+2
5	TAQINCHOQLAR	3t+2	30	KOSMONAVTLAR	5t+7
6	YILPIGICHLAR	9t+5	31	MATEMATIKA	3t+9
7	UNIVERSITET	7t+8	32	MUZLATGICH	9t+15
8	DASTURIY	11t+3	33	VARIANTLAR	7t+18
9	AXBOROT	11t+5	34	KARNAY	11t+13
10	BUTUNLIK	7t+1	35	TILLA	11t+17
11	MAHSULOT	9t+5	36	BILIMLAR	7t+21
12	AGENTLIK	7t+1	37	AXBOROT	9t+51
13	ILOVALAR	5t+2	38	BALANS	7t+17
14	IDORA	3t+4	39	DIREKTOR	5t+23
15	QULUPNAY	3t+15	40	ASKARLAR	3t+43
16	RAQAMLAR	3t+8	41	BUYRUQLAR	3t+25
17	SHAFTOLI	5t+9	42	DAFTARLAR	3t+18
18	FOTOAPPARAT	7t+12	43	DOKTORLARI	5t+19
19	TEXNOLOGIYA	9t+3	44	AXBOROTNOMA	7t+13
20	BOSHQARUV	11t+7	45	MASHINASI	9t+33
21	BANKLAR	11t+9	46	SAHIFACHI	11t+17
22	REKLAMASI	15t+1	47	ALGEBRASI	11t+19
23	SOZLASH	17t+2	48	TARMOQ	15t+31
24	TELEFON	19t+3	49	TESTLASH	17t+25
25	QOVURILGAN	21t+4	50	MUHARRIR	19t+13

### 3.2.3. Tayanch so‘zli Sezar usuli

Tayanch so‘zli Sezar usulida siljitish bilan birlgilikda tayanch so‘z qo‘llaniladi. Tayanch so‘zni qo‘llashdan maqsad hosil qilinadigan alifboda harflar ketma-ketligini o‘zgartirishdir.

**Misol.** Bu yerda  $k=5$  va **DIPLOMAT** tayanch so‘zini olamiz va bu so‘z  $k$ -o‘rindan yoziladi:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
				D	I	P	L	O	M	A	T														

Ushbu tayanch so‘z alifbodagi ko‘rsatilgan joyda joylashtiriladi, undagi harflar inobatga olinmasdan,

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	B	C		E	F	G	H	J	K		N		Q	R	S		U	V	W	X	Y	Z			
				D	I	P	L	O	M	A	T														

qolgan harflar alifbodagi tartib bo‘yicha tayanch so‘zdan keyin ketma-ket yoziladi va natijada quyidagi hosil qilinadi:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B	C	E	F	G	H	J	K	N	Q	R	S	U

Misol sifatida **SAMARQAND** so‘zini ko‘rib chamiz. Mazkur usul yordamida birirn-ketin harflar almashtiriladi, masalan, 18-katakda joylashgan **S** harfi **H** harfiga almashtiriladi va hokazo, natijada **HVTVGFBY** shifrlangan so‘z shakllanadi.

### Topshiriq

Quyidagi jadvalda berilgan so‘zlarni tayanch so‘zli Sezar usulida shifrlang va deshifrlang.

Variantlar

Nº	Shifrlanadigan so‘z	Kalit (k)	Tayanch so‘z
1	QAROQCHILIK	11	HIMOYA
2	BIBLIOGRAFIK	12	MUSIQA
3	TEZYORDAM	9	TEZKOR
4	VOSITALAR	9	MOUSE
5	TAQINCHOQLAR	11	STOP
6	YILPIGICHLAR	11	SHOX
7	UNIVERSITET	11	STUL
8	DASTURIY	8	ILOVA
9	AXBOROT	7	HAKER
10	BUTUNLIK	8	JISM
11	MAHSULOT	8	PALTO
12	AGENTLIK	8	POINT
13	ILOVALAR	8	DASTUR
14	IDORA	5	HUMO
15	QULUPNAY	8	XURMO
16	RAQAMLAR	8	BASIC

17	SHAFTOLI	7	LIMON
18	FOTOAPPARAT	11	MEDIYA
19	TEXNOLOGIYA	11	POWER
20	BOSHQARUV	8	PITON
21	BANKLAR	7	DARYO
22	REKLAMASI	9	ESHIK
23	SOZLASH	6	GILAM
24	TELEFON	7	PALTO
25	QOVURILGAN	10	LISP
26	TELEVIZOR	9	SABR
27	YULDUZLAR	9	KITOBI
28	KASALXONA	9	TEMIR
29	KUTUBXONA	9	PALOV
30	KOSMONAVTLAR	12	ESHIK
31	MATEMATIKA	10	DEVOR
32	MUZLATGICH	9	YURAK
33	VARIANTLAR	10	RASM
34	KARNAY	6	STOL
35	TILLA	5	MARS
36	BILIMLAR	8	TONG
37	AXBOROT	7	QASR
38	BALANS	6	LIFT
39	DIREKTOR	8	BOSH
40	ASKARLAR	8	PIYODA
41	BUYRUQLAR	9	KEMA
42	DAFTARLAR	9	YOZMA
43	DOKTORLARI	10	UZVIY
44	AXBOROTNOMA	11	RASMIY
45	MASHINASI	8	ENIGMA
46	SAHIFACHI	8	NASHR
47	ALGEBRASI	9	MANTIQ
48	TARMOQ	6	FILE
49	TESTLASH	7	AUDIT
50	MUHARRIR	8	FORMA

### 3.2.4. Polibiy kvadrati

Polibiy kvadrati (ingl. Polybius square). Bu sodda o‘rniga qo‘yish usuli sanalib, eramizdan oldingi III asrda Yunoniston olimi Polibiy tomonidan yaratilgan. Shifrlash usullarida ilk bor jadval tushunchasi qo‘llanilgan usul – bu Polibiy usuli hisoblanadi.

Ushbu usul quyidagi bosqichlardan iborat:

1-bosqich. Shifrlash jadvalini yaratish. Tanlangan belgilardan tashkil topgan alifbo iloji boricha tomonlari teng bo‘lgan jadvalda ifodalanadi. Jadval tomonlari qanchalik bir-biriga yaqin bo‘lsa, bardoshligi shunchalik yuqori bo‘ladi. Lotin alifbosi uchun 5x5 jadval shakllantiriladi. Umumiyl holda tanlangan jadvalda harflarni istalgan tartibda joylashtirish mumkin. Quyida lotin alifbosi uchun taklif etilgan jadval keltirilgan.

1-jadval

5x5 o‘lchamli jadvalda taqsimlangan lotin alifbosi

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

2-bosqich. Shifrlash. Ishlab chiqilgan alifbo asosida shifrlash jarayonini turli usullar asosida amalga oshirish mumkin. Quyida ularning 3 ta usuli keltirilgan.

**1- shifrlash usuli.** Bu usulda shifrlash uchun ochiq matn yuqoridagi 1-jadvaldan foydalilanadi. Ochiq matn harflari jadvaldan topilib, undan pastdagi belgi unga mos shifrmattn belgini ifodalaydi. Agar bu harf ustundagi oxirgi qatorda bo‘lsa, unda tanlangan ustunning birinchi katagidagi harf tanlanadi. Quyida “TOSHKENT” ochiq matnini shifrlash natijasi keltirilgan.

Ochiq matn belgisi	T	O	S	H	K	E	N	T
Shifrmattn belgisi	Y	T	X	N	P	K	S	Y

Olingan natijaviy shifrmattn “YTXNPKSY” ga teng bo‘ladi.

**2- shifrlash usuli.** Bu usulda ma’lumotni shifrlashda uning jadvaldagi joylashgan o‘rnidan foydalilanadi.

Ochiq matn belgisi	T	O	S	H	K	E	N	T
Gorizontal o‘rni	4	3	4	2	2	1	3	4
Vertikal o‘rni	4	4	3	3	5	5	3	4

Shundan so‘ng koordinatlar qator bo‘yicha juftlanib o‘qiladi va quyidigiga ega bo‘linadi: 43 42 21 34 44 33 55 34. Shundan so‘ng ushbu juftliklar gorizontal va vertikal koordinatalar shaklida ifodalanadi.

Gorizontal o‘rni	4	4	2	3	4	3	5	3
Vertikal o‘rni	3	2	1	4	4	3	5	4
Shifrmattn belgisi	S	R	F	O	T	N	Z	O

Olingan natijaviy shifrmattn “SRFOTNZO” ga teng bo‘ladi.

**3- shifrlash usuli.** Bu usul 2-usulda keltirilgan algoritmdan boshlanadi, ya’ni ma’lumotni shifrlashda uning jadvaldagi joylashgan o‘rnidan foydalaniladi.

Ochiq matn belgisi	T	O	S	H	K	E	N	T
Gorizontal o‘rni	4	3	4	2	2	1	3	4
Vertikal o‘rni	4	4	3	3	5	5	3	4

Shundan so‘ng koordinatlar qator bo‘yicha o‘qiladi va quyidigiga ega bo‘linadi: 43 42 21 34 44 33 55 34. Shundan so‘ng olingan ketma-ketlik chapga yoki o‘ngga siklik bir nechta belgiga siljtiladi. Masalan, Sezar usuli kabi  $k = 3$  ta ( $k = 3$ ) belgiga chapga siklik siljitariz va natijaviy 2213444335534434 ketma-ketlik juft-juft qilib yoziladi, 22 13 44 43 35 53 44 34 . Shundan so‘ng yuqoridagi juftliklar gorizontal va vertikal koordinatalar shaklida ifodalanadi.

Gorizontal o‘rni	2	1	4	4	3	5	4	3
Vertikal o‘rni	2	3	4	3	5	3	4	4
Shifrmattn belgisi	G	C	T	S	P	X	T	O

Olingan natijaviy shifrmattn “GCTSPXTO” ga teng bo‘ladi.

Yuqorida keltirilgan usullarda kalit so‘zini ham kiritish mumkin. Bunda kalit so‘zdagi harflar jadvaldan o‘chiriladi va qolgan harflar tartib bilan yoziladi.

Bunday yondashuv ilk bor Trisemus tomonidan 1508-yilda ko‘rsatilgan. Masalan, “SHIFR” kaliti uchun 1-jadval quyidagi ko‘rinishga ega bo‘ladi:

	1	2	3	4	5
1	S	H	I	F	R
2	A	B	C	D	E
3	G	K	L	M	N
4	O	P	Q	T	U
5	V	W	X	Y	Z

Ushbu jadvaldan foydalanib, yuqoridagi uchta shifrlash usullarining biridan foydalanib, matnlarni shifrlash mumkin bo‘ladi.

### 1-Topshiriq

Polibiy kvadratining 1-shifrlash usulidan foydalanib 1-jadvalga asoslanib quyidagi ma’lumotlarni shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	KOMPYUTER	21	DASTURLOVCHILAR
2	DARAXTSIMON	22	INTEGRATSIYA
3	TEXNOLOGIYALAR	23	ALGORITMLAR
4	AXBOROTLASHTIRISH	24	MATEMATIKA
5	KRIPTOGRAFIYA	25	INFORMATIKA
6	STEGANOGRAFIYA	26	ANTIVIRUS
7	KLAVIATURA	27	INTERVAL
8	SHIFRLANGAN	28	INTEGRAL
9	TARAQQIYOT	29	POWERPOINT
10	INNOVATSIYA	30	PHOTOSHOP
11	RIVOJLANISH	31	VINCHESTER
12	YUKSALISH	32	GEOMETRIYA
13	TELEVIZOR	33	PSEVDOTASODIFIY
14	MONITORING	34	TENGLAMALAR
15	MODULYATOR	35	OPTIMALLASHTIRISH
16	TRANSLYATOR	36	SODDALASHTIRISH
17	KOMPILYATOR	37	KOMBINATORIKA
18	INTERPRETATOR	38	XAVFSIZLIK
19	INTELLECT	39	QISQARTMA
20	GENERATOR	40	DAVOMAT

## 2-Topshiriq

Polibiy kvadratining 3-shifrlash usulidan foydalanib 1-jadvalga asoslanib ma'lumotlarni  $k$  kaliti asosida chapga siklik siljитish orqali quyidagi ma'lumotlarni shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so'z</b>	<b>k</b>	<b>№</b>	<b>Shifrlanadigan so'z</b>	<b>k</b>
41	kompyuter	3	51	dasturlovchilar	5
42	daraxtsimon	1	52	integratsiya	1
43	texnologiyalar	5	53	algoritmlar	3
44	axborotlashtirish	7	54	matematika	7
45	kriptografiya	1	55	informatika	1
46	steganografiya	3	56	antivirus	5
47	klaviatura	5	57	interval	3
48	shifrlangan	7	58	integral	7
49	taraqqiyot	9	59	powerpoint	9
50	innovatsiya	1	60	photoshop	1

### 3.2.5. Atbash usuli

Shifrlashning Atbash usuli harflarning o'rmini oddiy almashtirishga asoslangan. Ushbu shifr qadimda yahudiy alifbosidagi harflarni shifrlashda ishlatilgan, nomi ham shundan kelib chiqqan. Bu usulning Atbash deb atalishi yahudiy alifbosi harflarining almashtirilishi bilan izohlanadi. Atbash so'zi "alef", "tav", "bet", "shin" harflaridan iborat, ya'ni yahudiy alifbosining birinchi va oxirgi, ikkinchi va oxiridan ikkinchi harflaridan tuzilgan. Bu yerda shifrlashning qoidasi alifboning  $i$ -chi harfini  $n-i+1$  chi sondagi harf bilan almashtirish hisoblanadi (bu yerda:  $i$  – harfning alifbodagi joylashgan tartibi,  $n$  – esa alifbodagi harflar soni). Oddiy qilib tushuntiradigan bo'lsak, alifboning birinchi harfi oxirgi harfga almashtiriladi, ikkinchi harf esa oxiridan ikkinchisiga almashtiriladi va shu tartibda davom etadi. Quyidagi jadvalda ingliz va rus alifbolari uchun misollar keltirilgan:

**Atbash usulida ingliz va rus alifbolari shifrlanishi**

Ingliz harflari	Shifrlangan alifbo	Rus harflari	Shifrlangan alifbo
A	Z	А	Я
B	Y	Б	Ю
C	X	В	Э
D	W	Г	Ь
E	V	Д	Ы
F	U	Е	Ъ
G	T	Ё	Щ
H	S	Ж	Ш
I	R	З	Ч
J	Q	К	Ц
K	P	Л	Х
L	O	М	Ф
M	N	Н	У
N	M	О	Т
O	L	П	С
P	K	Р	Р
Q	J	С	П
R	I	Т	О
S	H	Ү	Н
T	G	Ф	М
U	F	Х	Л
V	E	Ц	К
W	D	Ч	З
X	C	Ш	Ж
Y	B	Щ	Ё
Z	A	Ь	Е
		Ы	Д
		Ь	Г
		Э	В
		Ю	Б
		Я	А

**1-misol.** Quyidagi misolda ma'lumotni Atbash usulida shifrlashni amalda ko'ramiz. "AXBOROT" xabarini yuqoridagi jadvaldan foydalanib shifrlaymiz:

A	X	B	O	R	O	T
↓	↓	↓	↓	↓	↓	↓
Z	C	Y	L	I	L	G

Demak, “AXBOROT” xabari Atbash usulida shifrlansa, “ZCYLILG” shifrmattan hosil bo‘ladi. Olingan shifrmatnni deshifrlash uchun ham alifbo jadvalidan foydalaniladi va natijada dastlabki matn “AXBOROT” hosil bo‘ladi.:

Z	C	Y	L	I	L	G
↓	↓	↓	↓	↓	↓	↓
A	X	B	O	R	O	T

### Topshiriq

Quyidagi jadvalda berilgan so‘zlarni Atbash usulida shifrlang va deshifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	TELEKOMMUNIKATSIYA	26	TEXNOKRATIYA
2	UNIVERSITETLARIMIZ	27	KRIPTOANALIZ
3	AVTOMATLASHTIRISH	28	INSTRUKTSIYA
4	MAQBULLASHTIRISH	29	INFORMATSIYA
5	ROBOTLASHTIRISH	30	KONFERENSIYA
6	TRANSFORMATSIYA	31	INSTRUMENTAL
7	JADALLASHTIRISH	32	KOMBINATSIYA
8	SHTANGENTSIRKUL	33	INTELLEKTUAL
9	KONFIGURATSIYA	34	KIBERNETIKA
10	STEGANOGRAFIYA	35	TEXNOLOGIYA
11	INFRASTRUKTURA	36	MUHANDISLIK
12	MODERNIZATSIYA	37	DIAGNOSTIKA
13	FUNKTSIONALLIK	38	XAVFSIZLIK
14	TRANSKRIPTSIYA	39	PROTSEDURA
15	PERPENDIKULYAR	40	TELEFONIYA
16	RIVOJLANTIRISH	41	KLAVIATURA
17	EKSPLUATATSIYA	42	MIKROSXEMA
18	SIVILIZATSIYA	43	PROTSESSOR
19	KONSTITUTSIYA	44	KONSTANTA
20	KOMPILYATSIYA	45	PLATFORMA
21	MASHINASOZLIK	46	REKURSIYA
22	KONSTRUKTSIYA	47	MENEJMENT
23	TARIFIKATSIYA	48	ANTIVIRUS
24	INTEGRATSIYA	49	MICROSKOP
25	KRIPTOLOGIYA	50	TEXNOGEN

### **3.2.6. Pleyfer usuli**

Pleyfer shifri yoki Pleyfer kvadrati – tarixda birinchi marta bigrammalarini almashtirish qo‘llanilgan simmetrik shifrlash usulidir. Bu usul 1854-yili ingliz fizigi Charlz Uitston tomonidan yaratilgan, lekin ushbu shifrlash tizimidan davlat xizmatida foydalanishni targ‘ib qilishda katta hissa qo‘sghan lord Layon Pleyfer nomi bilan atalgan. Pleyfer usulining boshqa shifrlardan farqi shundaki, bu usulda bitta belgi o‘rniga juft belgilar (bigrammalar) shifrlanadi. Shuning uchun oddiy almashtirish shifrlariga nisbatan mustahkam shifrlash usuli hisoblanadi.

Playfer shifrida kalit so‘z yoki iborani o‘z ichiga olgan 5x5 matritsadan foydalaniadi (ingliz alifbosi uchun, rus alifbosi uchun matritsa hajmini 4x8 ga oshirish kerak). Matritsani yasash va shifrdan foydalanish uchun kalit so‘zni hamda 4 ta oddiy qoidani yodda saqlash kifoya. Matritsani yasash uchun birinchi o‘rinda matritsaning bo‘sh kataklarini kalit so‘z harflari (bu yerda takrorlanadigan belgilar bo‘lmasligi talab etiladi) bilan to‘ldirish kerak. So‘ngra matritsaning qolgan kataklarini kalit so‘zda uchramaydigan alifbo harflari ketma-ketligi bilan to‘ldiriladi. Ba’zida usulida ingliz tilidagi so‘zlarni shifrlashda odatda Q harfi ishlatilmaydi. Ba’zi hollarda esa I va J harflari matritsaning bitta katagida yoziladi.

Kalit so‘z matritsaning birinchi satriga chapdan o‘ngga qarab yozilishi mumkin, yoki tepadagi chap burchakdan spiral tartibida matritsa markaziga qarab yozilishi mumkin. Alifbo yordamida to‘ldirilgan kalit so‘zi matritsaning tuzuvchisi va shifr kaliti hisoblanadi.

Xabarni shifrlash uchun uni bigrammalar (juft belgilar guruhi) ga bo‘lib chiqish kerak. Masalan, “AXBOROT XAVFSIZLIGI” xabarining bigrammalari “AX BO RO TX AV FS IZ LI GI” ko‘rinishga ega bo‘ladi va bu bigrammalarini jadvaldan izlash kerak. Bigrammaning ikkita belgisi matritsada to‘g‘ri to‘rtburchakni hosil qiladi. Aniqlangan to‘rtburchak burchaklari joylashish holatini aniqlab olamiz. Keyin, quyidagi 4 ta qoidadan foydalanib, chiquvchi matnning ikkala belgisini shifrlaymiz:

**1-qoida.** Agar bigrammaning ikki belgisi bir xil bo‘lsa birinchi belgidan so‘ng, yoki oxirida bitta belgi qolsa undan so‘ng “X” harfi qo‘shiladi va shifrlash davom ettiriladi. Masalan, “SAKKIZ” so‘zi quyidagicha bigrammalarga ajratiladi: “**SA** **KX** **KI** **ZX**”. Pleyfer shifrlashning ayrim variantlarida “X” o‘rniga “Q” harfi ishlatiladi.

**2-qoida.** Agar bigrammaning belgilari bitta satrda uchrasa, u holda belgilar o‘zidan bitta keyingi ustundagi belgiga almashtiriladi. Faraz qilaylik bizga “**AN**” bigrammasi quyidagi tartibda berilgan bo‘lsin:

*	*	*	*	*
*	<b>A</b> → <b>Y</b>	<b>N</b> → <b>Z</b>		
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

**AN → YZ**

Shifrlash

*	*	*	*	*
*	<b>A</b> ← <b>Y</b>	<b>N</b> ← <b>Z</b>		
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

**YZ → AN**

Deshifrlash

Agar shifrlanayotgan belgi satr oxirida bo‘lsa, unda shu satrning birinchi belgisiga almashtiriladi:

*	*	*	*	*
*	*	*	*	*
	<b>Y</b>	<b>A</b> → <b>Z</b>	<b>*</b>	<b>N</b>
*	*	*	*	*
*	*	*	*	*

**AN → ZY**

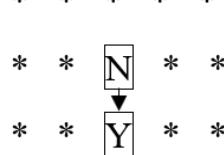
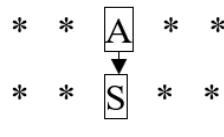
Shifrlash

*	*	*	*	*
*	*	*	*	*
	<b>Y</b>	<b>A</b> ← <b>Z</b>	<b>*</b>	<b>N</b>
*	*	*	*	*
*	*	*	*	*

**ZY → AN**

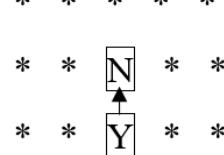
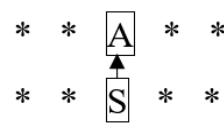
Deshifrlash

**3-qoida.** Agar bigramma belgilari bitta ustunda uchrasa, u holda belgilar o‘zidan bitta pastdagи belgiga almashtiriladi:



$\text{AN} \rightarrow \text{SY}$

Shifrlash

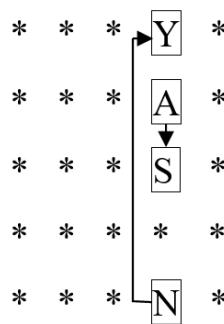


$\text{SY} \rightarrow \text{AN}$

Deshifrlash

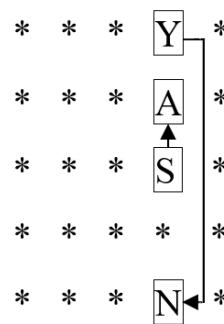
Agar belgi ustunning eng pastida joylashgan bo‘lsa, unda ustunning eng tepasidagi

birinchi belgiga almashtiriladi:



$\text{AN} \rightarrow \text{SY}$

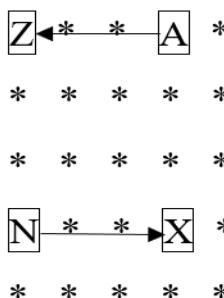
Shifrlash



$\text{SY} \rightarrow \text{AN}$

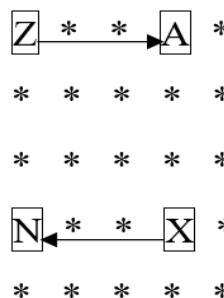
Deshifrlash

**4-qoida.** Agar bigramma belgilari har xil satr va ustunlarda joylashgan bo‘lsa, unda hosil bo‘lgan to‘rtburchakda o‘ziga qarama-qarshi burchakdagi belgilarga almashtiriladi. Birinchi belgi bevosita qatordagi belgiga almashtiriladi, xuddi shunday ikkinchi belgi:



$\text{AN} \rightarrow \text{ZX}$

Shifrlash



$\text{ZX} \rightarrow \text{AN}$

Deshifrlash

**1-misol:** “SAKKIZ” xabarini shifrlaymiz, kalit so‘zi sifatida “AXBOROT” so‘zini olamiz. Qoida bo‘yicha birinchi o‘rinda kalit so‘zi yoziladi va undan so‘ng alifboning qolgan harflari bilan matritsa to‘ldiriladi. Shifrlanadigan xabarni bigrammalarga bo‘lsak, “SA KK IZ” bo‘lishi kerak, lekin yuqoridagi qoidaga ko‘ra, ikkita K birga kelgan, ular mos ravishda X qo‘shilib “SA KX KI ZX” ko‘rinishda bo‘ladi.

A	X	B	O	R
T	C	D	E	F
G	H	I, J	K	L
M	N	P	Q	S
U	V	W	Y	Z

Yuqoridagi qoidadan foydalanib shifrlaymiz:

- SA → MR (4-qoida)
- KX → HO (1-qoida)
- KI → LK (2-qoida)
- ZX → VR (1-qoida)

Demak, “SAKKIZ” xabari “MRHOLKVR” shifrmatl ko‘rinishiga ega bo‘ladi.

**2-misol:** “AXROR” xabarini shifrlaymiz. Kalit so‘zi sifatida “AXBOROT” so‘zini olamiz. “AXROR” xabarini bigrammalarga bo‘lsak, “AX RO RX” ko‘rinishga keladi.

A	X	B	O	R
T	C	D	E	F
G	H	I, J	K	L
M	N	P	Q	S
U	V	W	Y	Z

Yuqoridagi qoidadan foydalanib bigrammalarini shifrlaymiz:

- AX → XB (2-qoida)

RO → AR                    (2-qoida)

RX → AB                    (2-qoida)

**3-misol:** “HIMOYA” xabarini shifrlaymiz. Kalit so‘zi sifatida “AXBOROT” so‘zini olamiz. “HIMOYA” xabarini bigrammalarga bo‘lsak, “HI MO YA” ko‘rinishga keladi.

A	X	B	O	R
T	C	D	E	F
G	H	I, J	K	L
M	N	P	Q	S
U	V	W	Y	Z

Yuqoridagi qoidadan foydalanib bigrammalarni shifrlaymiz:

HI → IK (yoki JK)                    (2-qoida)

MO → AQ                                (4-qoida)

YA → UO                                (4-qoida)

**4-misol:** “OLMA” xabarini shifrlaymiz. Kalit so‘zi sifatida “AXBOROT” so‘zini olamiz.

A	X	B	O	R
T	C	D	E	F
G	H	I, J	K	L
M	N	P	Q	S
U	V	W	Y	Z

“OLMA” xabarini bigrammalarga bo‘lsak, “OL MA” ko‘rinishga keladi.

Yuqoridagi qoidadan foydalanib bigrammalarni shifrlaymiz:

OL → RK                                (4-qoida)

MA → UT                                (3-qoida)

**5-misol:** “XAVFSIZLIK” xabarini shifrlaymiz, kalit so‘zi sifatida “AXBOROT” so‘zini olaylik.

A	X	B	O	R
T	C	D	E	F
G	H	I	K	L
M	N	P	Q	S
U	V	W	Y	Z

Demak, matritsani to‘ldirdik, endi xabarimizni bigrammalarga ajratamiz:

“XAVFSIZLIK” → “XA VF SI ZL IK”

Bigrammalarni shifrlaymiz:

$$XA \rightarrow BX \quad VF \rightarrow ZC \quad SI \rightarrow PL \quad ZL \rightarrow RS \quad IK \rightarrow KL$$

Shifrimiz quyidagi ko‘rinishga keldi: BX ZC PL RS KL.

Demak, “XAVFSIZLIK” xabari “AXBOROT” kalit so‘zidan foydalaniб Pleyfer usulida shifrlanganda, “BXZCPLRSKL” ko‘rinishdagi shifrga aylandi.

Endi teskari jarayonni bajaramiz, ya’ni “BXZCPLRSKL” shifrnini deshifrlaymiz. Shifrmatnni bigrammalarga ajratamiz: “BX ZC PL RS KL”. Bu bigrammalarni shifrlash matritsasidan qidiramiz:

A	X	B	O	R
T	C	D	E	F
G	H	I	K	L
M	N	P	Q	S
U	V	W	Y	Z

$$BX \rightarrow XA \quad ZC \rightarrow VF \quad PL \rightarrow SI \quad RS \rightarrow ZL \quad KL \rightarrow IK$$

Natijada quyidagi ochiq xabarga ega bo‘lamiz: “**XAVFSIZLIK**”.

### Topshiriq

Quyidagi jadvalda berilgan so‘zlarni Pleyfer usulida shifrlang va deshifrlang.

## Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>Kalit so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>Kalit so‘z</b>
1	COMPAS	TABLE	25	DOROGA	ARGON
2	CAMPUS	PRINT	26	YAKUZA	GURON
3	GULDON	KUSTO	27	KORDON	DAVOS
4	KAZBEK	FLASH	28	MEMORY	SINTO
5	GAVANA	FLAME	29	DRIVER	JUNGLI
6	KARNAY	TRADE	30	DIKTOR	MANGU
7	COMRAD	FRAME	31	SUNDAY	SKODA
8	TUNING	BRAVE	32	FRIDAY	WEIBO
9	FALCON	KABEL	33	DRAGON	KRIPT
10	BEGONA	SEZON	34	DAFTAR	DERSU
11	KORONA	MAKED	35	QOPLON	ILBON
12	SURNAY	PRINT	36	SAVLAT	JINGU
13	ANGOLA	VERDI	37	SANDIQ	VIOLA
14	PERUJA	MANGO	38	VATSON	TINKO
15	TREVOR	BINGO	39	DAVLAT	BEZOS
16	XENKOK	TRACK	40	NUMBER	GANDI
17	FIGARO	TASTE	41	NETBUK	TYSON
18	FLOPPY	DISCO	42	FOLLOW	KOREA
19	RANDOM	XUTOR	43	RAXMAT	GEYTS
20	DORUGA	DEBUG	44	KARVON	DOVUL
21	DASTUR	TRASH	45	VERDER	STRIM
22	SARDOR	MEIZU	46	SUBMIT	KARGO
23	PAYPAL	SALDO	47	SARDOR	PAROM
24	TEREZA	SURON	48	DAZMOL	SPORT

### 3.2.7. Omofon usuli

Omofon so‘zi yunoncha “*omos* – bir xil”, “*phon* - ovoz” degan ma’noni anglatadi, ya’ni bir xil eshitiladigan, shaklan har xil yoziladigan so‘zlarga nisbatan qo’llaniladi. Omofon almashtirish usulidan foydalanib shifrlash XV asrdan ma’lum. 1401 yilda ilk bor Simeon De Krema ko‘p qiymatli harflarni shifrlashda

omofon jadvalidan foydalangan. Keyinchalik italiyalik olim Leon Battista Alberti o‘zining 1466-yili nashr qilingan “Shifrlar haqida risola” kitobida Omofon almashtirish shifrini bir harfga bir nechta element to‘g‘ri kelishini tasvirlab bergen.

Omofon almashtirish shifri (ingizchasiga *Homophonic substitution cipher*) – almashtirish usullaridan biri bo‘lib, bunda ochiq matnning har bir belgisi bir nechta ehtimoliy belgilardan biriga almashtiriladi. Bitta harf uchun almashtiriladigan belgilar soni ushbu harf chastotasiga proportsionaldir. Bu usul shifrlangan matnda harfni uchrashining haqiqiy chastotasini yashirish imkonini beradi.

Keltirilgan usulning muhim jihat shundaki, bunda almashtiriladigan shifr belgilari takrorlanmaydi. Omofonik shifrlashda alifboning har bir harfi bir necha belgiga almashtirilishi tufayli ko‘p alifboli shifrlash usuli degan chalkash fikrga borilishi mumkin, aslida esa omofon almashtirish shifri monoalifboli (bir alifboli) shifrlash usulidir. Omofon shifrlashning monoalifboli deb hisoblanishining asosiy sababi shundaki, unda shifr alifbosi shifrlash jarayonida o‘zgarmaydi.

Misol uchun,  $i$  – ochiq matnda ishlatiladigan alifbo belgisi bo‘lsin. Har bir  $i$  uchun belgilar to‘plami  $M_i$  ni tuzamiz, bu holda ochiq matnning  $i$  va  $j$  belgilari uchun tuzilgan  $M_i$  va  $M_j$  to‘plamlar o‘zaro kesishmasligi lozim. Odatda  $M_i$  to‘plam elementlari sonlardan tuzilgan bo‘ladi. Omofon usulidagi shifrlashda to‘plamning elementlari sifatida sonlar olinishi u bilan ishlashni ancha osonlashtiradi.

Omofonik shifrlashda har bir belgi uchun almashtirish soni ushbu belgining ochiq matnda paydo bo‘lish ehtimoli bilan mutanosib ravishda olinadi. Shifrlashda ochiq matn belgisini almashtirish tasodifiy (tasodifiy sonlar generatori) yoki ma’lum bir usulda (masalan, tartibi bilan) tanlanadi. Ochiq matnda ko‘p uchraydigan harfni eslab qolish maqsadida ingliz va rus alifbolari uchun mos ravishda “tetrishonda” va “сеновалитр” harflari kombinatsiyasi ishlatiladi, ya’ni ingliz alifbosidagi 1 millionta harfli kitob ichida qaysi harflar eng ko‘p uchrashini analiz qilib ko‘rilganida “tetrishonda” harflari aniqlangan. Mos ravishda rus alifbosida eng ko‘p “сеновалитр” harflari uchrashi ma’lum bo‘lgan.

### Rus alifbosidagi harflarining ehtimoli

<b>Harf</b>	<b>Ehtimolligi</b>	<b>Harf</b>	<b>Ehtimolligi</b>	<b>Harf</b>	<b>Ehtimolligi</b>	<b>Harf</b>	<b>Ehtimolligi</b>
А	0,069	И	0,064	Р	0,042	ІІ	0,006
Б	0,013	Ҷ	0,010	С	0,046	ҶҶ	0,004
В	0,038	К	0,029	Т	0,054	Ҷъ	0,001
Г	0,014	Л	0,039	Ү	0,023	ҶІ	0,015
Д	0,024	М	0,027	Ф	0,003	Ҷ	0,013
Е, Ё	0,071	Н	0,057	Х	0,008	Ҷ	0,002
Ж	0,007	О	0,094	Ц	0,005	Ю	0,005
З	0,016	П	0,026	Ч	0,012	Я	0,017

Yuqoridagi jadvalda umumiy hajmi 1 million belgidan ortiq bo‘lgan badiiy va ilmiy-texnik matnlarning chastotali tahlili natijalari keltirilgan. Tahvilga ko‘ra "bo‘shliq (Space)" ehtimoli 0,146 ga teng.

Eng noyob harf bilan uchrashish ehtimoli taxminan mingdan birga teng bo‘lganligi sababli, oddiy matnni Omofonik almashtirish usuli bilan shifrlash shifr jadvaliga muvofiq amalga oshirilishi mumkin, bu yerda har bir shifr almashtirishi bir necha raqamdan iborat va ularning umumiy soni 1000 ga teng bo‘ladi. Bunga namuna sifatida quyidagi jadvalni keltiramiz:

### Rus alifbosidagi harflarning almashishlar soni

<b>Harf</b>	<b>Almashish-lar soni</b>						
А	69	И	64	Р	42	ІІ	6
Б	13	Ҷ	10	С	46	ҶҶ	4
В	38	К	29	Т	54	Ҷъ	1
Г	14	Л	39	Ү	23	ҶІ	15
Д	24	М	27	Ф	3	Ҷ	13
Е, Ё	71	Н	57	Х	8	Ҷ	2
Ж	7	О	94	Ц	5	Ю	5
З	16	П	26	Ч	12	Я	17

Quyidagi jadvalda ingliz alifbosidagi harflar uchun tasodifiy shifr almashtirish sonlari keltirilgan:

3-jadval

### **Ingliz alifbosidagi harflarning almashishlar namunasi**

<b>№</b>	<b>Harflar</b>	<b>Kalit sonlar</b>											
1	A	07	31	50	63	66	77	84					
2	B	11	64										
3	C	17	33	49									
4	D	10	27	51	76								
5	E	25	26	28	32	48	67	69	72	75	79	82	85
6	F	08	09										
7	G	44	83										
8	H	19	20	21	54	70	87						
9	I	02	03	29	53	68	73						
10	J	18											
11	K	41											
12	L	42	81	86	95								
13	M	40	52										
14	N	00	43	80	88	89							
15	O	16	30	61	65	91	94	96					
16	P	01	62										
17	Q	15											
18	R	04	24	39	58	71	99						
19	S	06	34	56	57	59	90						
20	T	05	23	35	37	38	60	74	78	92			
21	U	13	14	36									
22	V	22											
23	W	45	46										
24	X	12											
25	Y	55	93										
26	Z	47											

Ushbu jadvaldan foydalanib “KIBERXAVFSIZLIK” xabarini shifrlab ko‘ramiz.  
 “K”-41, “I”-68, “B”-64, “E”-82, “R”-71, “X”-12, “A”-63, “V”-22, “F”-08, “S”-57,  
 “I”-53, “Z”-47, “L”-81, “I”-03, “K”-41

Natijada quyidagi shifrmatnga ega bo‘lamiz: **“41 68 64 82 71 12 63 22 08 57 53 47  
 81 03 41”.**

Deshifrlash jarayoni 3-jadval asosida teskari tartibda bajariladi:

41-“K”, 68-“I”, 64-“B”, 82-“E”, 71-“R”, 12-“X”, 63-“A”, 22-“V”, 08-“F”, 57-“S”,  
53-“I”, 47-“Z”, 81-“L”, 03-“I”, 41-“K”

Natijada quyidagi ochiq xabarga ega bo‘lamiz: “**KIBERXAVFSIZLIK**”.

### Topshiriq

3-jadvaldan foydalanib, quyidagi berilgan so‘zlarni Omofon usulida shifrlang va deshifrlang.

#### Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	TELEKOMMUNIKATSIYA	26	TEXNOKRATIYA
2	UNIVERSITETLARIMIZ	27	KRIPTOANALIZ
3	AVTOMATLASHTIRISH	28	INSTRUKTSIYA
4	MAQBULLASHTIRISH	29	INFORMATSIYA
5	ROBOTLASHTIRISH	30	KONFERENSIYA
6	TRANSFORMATSIYA	31	INSTRUMENTAL
7	JADALLASHTIRISH	32	KOMBINATSIYA
8	SHTANGENTSIRKUL	33	INTELLEKTUAL
9	KONFIGURATSIYA	34	KIBERNETIKA
10	STEGANOGRAFIYA	35	TEXNOLOGIYA
11	INFRASTRUKTURA	36	MUHANDISLIK
12	MODERNIZATSIYA	37	DIAGNOSTIKA
13	FUNKTSIONALLIK	38	XAVFSIZLIK
14	TRANSKRIPTSIYA	39	PROTSEDURA
15	PERPENDIKULYAR	40	TELEFONIYA
16	RIVOJLANTIRISH	41	KLAVIATURA
17	EKSPLUATATSIYA	42	MIKROSXEMA
18	SIVILIZATSIYA	43	PROTSESSOR
19	KONSTITUTSIYA	44	KONSTANTA
20	KOMPILYATSIYA	45	PLATFORMA
21	MASHINASOZLIK	46	REKURSIYA
22	KONSTRUKTSIYA	47	MENEJMENT
23	TARIFIKATSIYA	48	ANTIVIRUS
24	INTEGRATSIYA	49	MICROSKOP
25	KRIPTOLOGIYA	50	TEXNOGEN

### 3.2.8. Vernam usuli

**Vernam shifri** (inglizcha Vernam Cipher) – simmetrik shifrlash tizimi, 1917-yilda Amerika telefon va telegraf (AT&T) kompaniyasi injineri Gilbert Vernam tomonidan ixtiro qilingan.

Vernam shifrlash tizimi oddiy kriptotizimlardan biri, yuqori kriptobardoshli bo‘lgan. Ushbu shifrlash tizimi Amerika telefon va telegraf (AT&T) operatori Gilbert Vernam sharafiga nomlandi va 1919-yilda telegraf xabarlarini avtomatik ravishda shifrlash tizimiga patent berildi.

Vernam shifrlash tizimi modul qiymati  $m=2$  bo‘lgan Vijiner shifrlash tizimining bir qismi hisoblanib, 1926-yilda bu usulning aniq ko‘rinishi ishlab chiqilgan. Gilbert Vernam kiruvchi matn sifatida ikkilik sanoq sistemasidan foydalanadi. Shifrlashda ingliz alifbosidagi ( $A, B, \dots, Z$ ) matnning har bir harfi 5 bitli ( $b_0, b_1, \dots, b_5$ ) Bodo kodlari bilan kodlanadi (1-jadval).

1-jadval  
**Bodo kodlari**

A	0	00000		Q	16	10000
B	1	00001		R	17	10001
C	2	00010		S	18	10010
D	3	00011		T	19	10011
E	4	00100		U	20	10100
F	5	00101		V	21	10101
G	6	00110		W	22	10110
H	7	00111		X	23	10111
I	8	01000		Y	24	11000
J	9	01001		Z	25	11001
K	10	01010		#	26	11010
L	11	01011		!	27	11011
M	12	01100		_	28	11100
N	13	01101		@	29	11101
O	14	01110		?	30	11110
P	15	01111		*	31	11111

Quyidagi rasmda uzatilayotgan axborotni Vernam usuli orqali shifrlash ko‘rsatilgan (2-rasm).



2-rasm. Vernam usuli orqali shifrlash

Kiruvchi matnni shifrlashda  $x$  kiruvchi matn ikkilik ko‘rinishiga o‘tkaziladi va ikkilik modul (XOR jadvali) ostida ikkilik ketma-ketlikdagi  $k$  kalit bilan shifrlash amalga oshiriladi:  $y = x \oplus k$ , bu yerda  $k$  – xabarni shifrlashdagi kalit so‘z bo‘lib, uning belgilari soni shifrlanuvchi xabarning belgilari sonidan kam bo‘lishi yoki oshib ketmasligi kerak.

Shifrni ochishda yozuvdagagi har bir ikkilik modul ostidagi belgilar  $k$  kalit ketma-ketligi bilan XOR jadvali (2-jadval) asosida qo‘shiladi:  $y \oplus k = x$ .

2-jadval

**XOR amali**

$m$	$n$	$m \oplus n$
0	0	0
0	1	1
1	0	1
1	1	0

Misol: “SALOM” so‘zini “YOZ” kalit so‘zi yordamida shifrlang.

Bu masalada quyidagilar berilgan:  $T_o = <\text{SALOM}>$ ,  $k = <\text{YOZ}>$ ,  $T_m = ?$

Berilganlardan kelib chiqib quyidagi jadvalni to‘ldirib olamiz. Shifrlanadigan xabarni har bir belgisiga kalit so‘zning belgilari ketma-ketligini mos holda joylashtiramiz. Agar shifrlanadigan xabarning belgilari soni kalit so‘zning belgilari sonidan ko‘p bo‘lsa, jadval to‘lgunicha kalit so‘zni takrorlaymiz:

3-jadval

$T_o$	S	A	L	O	M
$k$	Y	O	Z	Y	O

$$\begin{array}{l}
 1) \quad \begin{array}{r} \oplus \\ S=10010 \\ Y=11000 \\ \hline K=01010 \end{array} \quad 2) \quad \begin{array}{r} \oplus \\ A=00000 \\ O=01110 \\ \hline O=01110 \end{array} \quad 3) \quad \begin{array}{r} \oplus \\ L=01011 \\ Z=11001 \\ \hline S=10010 \end{array} \\
 4) \quad \begin{array}{r} \oplus \\ O=01110 \\ Y=11000 \\ \hline W=10110 \end{array} \quad 5) \quad \begin{array}{r} \oplus \\ M=01100 \\ O=01110 \\ \hline C=00010 \end{array}
 \end{array}$$

Demak shifrlangan xabar:  $T_m = \text{KOSWC}$ .

Shifrlangan xabarni deshifrlash ya’ni shifrnii ochishda shifrlash jarayoniga teskari amal bajariladi:

4-jadval

$T_m$	K	O	S	W	C
k	Y	O	Z	Y	O

$$\begin{array}{l}
 1) \quad \begin{array}{r} \oplus \\ K=01010 \\ Y=11000 \\ \hline S=10010 \end{array} \quad 2) \quad \begin{array}{r} \oplus \\ O=01110 \\ O=01110 \\ \hline A=00000 \end{array} \quad 3) \quad \begin{array}{r} \oplus \\ S=10010 \\ Z=11001 \\ \hline L=01011 \end{array} \\
 4) \quad \begin{array}{r} \oplus \\ W=10110 \\ Y=11000 \\ \hline O=01110 \end{array} \quad 5) \quad \begin{array}{r} \oplus \\ C=00010 \\ O=01110 \\ \hline M=01100 \end{array}
 \end{array}$$

Demak ochiq xabar:  $T_o = \langle \text{SALOM} \rangle$ .

Vernam shifrlash tizimining kamchiligi uzatuvchi orqali qabul qiluvchiga kalit ketma-ketligini qanday uzatish hisoblanadi. Chunki buzg‘unchi kalitni olsa, u yuborgan shifrlangan matnni bemalol olib o‘qiy oladi. Shuning uchun ham Vernamning shifrlash tizmi yetarli emasligi sababli buni hal qilish uchun shifrlashni gammalashtirish usuliga o‘tilgan.

### Topshiriq

Quyida berilgan ( $T_o$ ) so‘zlardan berilgan kalit so‘zlar yordamida shifrlangan xabarni ( $T_m$ ) aniqlang va teskari jarayon orqali deshifrlang.

Variantlar

<b>Nº</b>	<b>Shifrlanadigan so‘z (t<sub>0</sub>)</b>	<b>kalit so‘z (k)</b>	<b>Nº</b>	<b>Shifrlanadigan so‘z (t<sub>0</sub>)</b>	<b>kalit so‘z (k)</b>
1	dasturiy_qaroqchilik	piyola	26	televizor_kanali	sarob
2	bibliografik_tavsif	musiqa	27	yulduzlar_jilosি	kitob
3	tezyordam_mashinasi	mushuk	28	kasalxona_binosi	temir
4	dasturiy_vositalar	ananas	29	kutubxona_kitobi	palov
5	taqinchoqlar_narxi	stakan	30	kosmonavtlar_uyi	ermak
6	yilpigichlar_rangi	shahar	31	qiziq_matematika	devor
7	universitet_binosi	beshik	32	yangi_muzlatgich	yurak
8	dasturiy_jamlanma	dollar	33	bazis_variantlar	rasm
9	axborot_eskirishi	hakker	34	karnay_surnaychi	stul
10	axborot_butunligi	kosmos	35	tilla_tishchalar	mars
11	dasturiy_mahsulot	qizlar	36	bilimlar_ombori	shox
12	axborot_agentligi	gitara	37	axborot_biznesi	qasr
13	dasturiy_ilovalar	jarlik	38	axborot_balansi	lift
14	militsiya_idorasi	sigir	39	direktor_xonasi	taxt
15	qulupnay_sharbati	xurmo	40	askarlar_hayoti	gips
16	raqamlar_ayirmasi	bozor	41	buyruqlar_satri	kema
17	shaftoli_sharbati	limon	42	yangi_daftarlar	olma
18	fotoapparat_qismi	nemis	43	tish_doktorlari	orol
19	yangi_txenologiya	otlar	44	axborot_bozori	miya
20	boshqaruv_xonasi	soqol	45	vaqt_mashinasi	soch
21	banklararo_tizim	daryo	46	bosh_sahifachi	qabr
22	banner_reklamasi	eshik	47	bull_algebrasi	pul
23	dasturni_sozlash	gilam	48	banyan_tarmoq	fil
24	telefon_trubkasi	palto	49	beta_testlash	non
25	qovurilgan_baliq	osmon	50	bosh_muharrir	til

### 3.3. Polialifboli o‘rniga qo‘yish usuli

Polialifboli shifrlash – bu oddiy monoalifboli o‘rniga qo‘yish usullarining to‘plamidan tashkil topgan bo‘lib, ochiq matnning keyingi belgisini shifrlashda ma’lum bir qoida asosida amalga oshiriladi. Ilk bor polialifboli shifrlash usuli Ibn ad-Durayima (1312–1359) va Al-Kalkashandi (1355-1418) ilmiy ishlarida qayd qilingan. Bunda polialifboli shifrlash usulining asosiy g‘oyasi monoalifboli shifrlash usullaridan siklik ravishda bir necha bor foydalanishdadir. Masalan, agar matn quyidagi ketma-ketlikda bo‘lsa  $x_1, x_2, x_3, \dots, x_n, \dots, x_{2n}, \dots$ , unda ushbu

matnni shifrlashda  $n$  ta monoalifboli shifrlash usullaridan foydalanamiz, ya’ni birinchi harfga faqatgina birinchi monoalifboli shifrlash usulini qo‘llaymiz, ikkinchi harfga faqatgina ikkinchi monoalifboli shifrlash usulini qo‘llaymiz va hokazo  $n$ -harfga faqatgina  $n$ -monoalifboli shifrlash usulini qo‘llaymiz. Keyingi  $n+1$ -harfga esa yana birinchi monoalifboli shifrlash usulini qo‘llaymiz. Shu yo‘l bilan matn to‘liq shifrlanadi.

Polialifboli shifrlash usuli monoalifboli shifrlash usullaridan farqliroq bevosita harflarning chastotasini bir tekisda paydo bo‘lishini ta’minlaydi.

### 3.3.1. Gronsfeld usuli

Grongsfeld usuli murakkab o‘rniga qo‘yish usuli bo‘lib, Sezar usulining murakkablashtirilgan varianti hisoblanadi. Bunda kiritilgan sonli kalit raqamlari har bir belgilar qatoriga nisbatan alohida qo‘llaniladi. Agarda kalit sonida raqamlar soni kamlik qilsa, unda kalit sonni takroran yozish kerak bo‘ladi. Sezar usulida alifbo to‘liq kalit son asosida siljitelgan bo‘lsa, bu yerda har bir raqam alifboni qanchaga siljitishtirishni belgilab beradi. Masalan, kalit son sifatida matematikada mavjud  $\pi$  sonining 3 ta birinchi raqamini qabul qilamiz, ya’ni  $k=3$ . Ushbu kalit bo‘yicha alifbo harflarini siljitishtirish tartibini quyidagi jadvalda keltiramiz:

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$k$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Shifrlash uchun “STEGANOGRAPHY” so‘zini qabul qilamiz. Shifrlash jarayonini jadval shaklida tasvirlaymiz:

Matn	S	T	E	G	A	N	O	G	R	A	F	I	Y	A
Kalit	3	1	4	3	1	4	3	1	4	3	1	4	3	1
Shifrmatn	V	U	I	J	B	R	R	H	V	D	G	M	B	B

Natijaviy VUIJBRRHVDGMBB shifrmatn ustida boshqa kalit bilan shifrlash jarayoni takrorlanilsa, unda ushbu usulning kriptobardoshligi oshadi. Umumiy holda Gronsfeld usuli Vijiner usulining xususiy varianti hisoblanadi.

### Topshiriq

Quyida berilgan so‘zlarni, bo‘sh kataklarni inobatga olmay, berilgan kalit yordamida shifrlang va deshifrlang.

#### Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>kalit (k)</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>kalit (k)</b>
1	dasturiy qaroqchilik	2345	17	qiziq matematika	1359
2	bibliografik tavsif	3456	18	bilimlar ombori	1234
3	kutubxona fayli	4567	19	axborot biznesi	2345
4	dasturiy vositalar	5678	20	axborot balansi	3457
5	dasturni sozlash	6789	21	buyruqlar satri	4568
6	telefon trubkasi	7891	22	yangi daftarlar	5679
7	universitet binosi	8912	23	axborot bozori	4579
8	dasturiy jamlanma	9123	24	vaqt mashinasi	5794
9	axborot eskirishi	2468	25	bosh sahifachi	5684
10	axborot butunligi	4682	26	bull algebrasi	6845
11	dasturiy mahsulot	6824	27	raqamlar ayirmasi	4578
12	axborot agentligi	8246	28	yangi texnologiya	5789
13	dasturiy ilovalar	3579	29	boshqaruv xonasi	7891
14	beta testlash	5791	30	banklararo tizim	8924
15	operatsion tizim	7913	31	sehrli kvadrat	9248
16	buyruq qatori	9135	32	gammalash usuli	2489

### 3.3.2. Vijiner jadvali

Fransuz kriptografi Bleyz de Vijiner qadimda eng mashhur bo‘lgan ko‘p alifboli (polialifboli) o‘rniga qo‘yish tizimiga asos solgan. Bu tizim uning sharafiga Vijiner tizimi (fr. Chiffre de Vigenère) deb atalgan. Polialifboli usuli o‘rniga qo‘yish usullari aytarlicha yuqori kriptobardoshlilikka ega. Bu usullar dastlabki matn harflarini almashtirish uchun bir necha alifbodan foydalanishga asoslangan. Ammo shifrlash usulining statistik kriptotahlil usullariga bardoshliligi kalit uzunligiga bog‘liq bo‘ladi.

	<b>a</b>	<b>b</b>	<b>c</b>	<b>d</b>	<b>e</b>	<b>f</b>	<b>g</b>	<b>h</b>	<b>i</b>	<b>j</b>	<b>k</b>	<b>l</b>	<b>m</b>	<b>n</b>	<b>o</b>	<b>p</b>	<b>q</b>	<b>r</b>	<b>s</b>	<b>t</b>	<b>u</b>	<b>v</b>	<b>w</b>	<b>x</b>	<b>y</b>	<b>z</b>
<b>a</b>	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
<b>b</b>	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
<b>c</b>	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	
<b>d</b>	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	
<b>e</b>	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	
<b>f</b>	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	
<b>g</b>	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	
<b>h</b>	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	
<b>i</b>	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	
<b>j</b>	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	
<b>k</b>	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	
<b>l</b>	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	
<b>m</b>	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	
<b>n</b>	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	
<b>o</b>	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	
<b>p</b>	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	
<b>q</b>	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
<b>r</b>	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	
<b>s</b>	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	
<b>t</b>	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	
<b>u</b>	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	
<b>v</b>	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	
<b>w</b>	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	
<b>x</b>	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	
<b>y</b>	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	
<b>z</b>	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	

1-rasm. Vijiner matritsasi

Polialifboli o‘rniga qo‘yish usullari ichida Vijiner jadvalini (matritsasi) ishlatuvchi algoritm eng keng tarqalgan. Vijiner jadvali  $R \times R$  o‘lchamli kvadrat matritsadan iborat bo‘lib, (bu yerda  $R$  – bu ishlatilayotgan alifbodagi belgilar soni) birinchi qatorida harflar alifbo tartibida joylashtiriladi. Ikkinchi qatordan boshlab harflar chapga bitta o‘ringa siljitelgan holda yoziladi. Siqib chiqarilgan harf o‘ng tarafdagи bo‘shagan o‘rinni to‘ldiradi (siklik siljitish). Agar ingliz alifbosi ishlatilsa, Vijiner matritsasi  $26 \times 26$  o‘lchamga ega bo‘ladi va ko‘rinishda bo‘ladi (1-rasm).

Shifrlash jarayoni takrorlanmaydigan  $m$  ta harfdan iborat kalit yordamida amalga oshiriladi. Vijnerning to‘liq matritsasidan  $[(m+1), R]$  o‘lchamli shifrlash matritsasi ajratiladi.

a	b	c	d	e	F	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

2-rasm. « KITOB » kaliti uchun shifrlash matritsasi

Bu matritsa bevosita Vijnerning to‘liq matritsasining birinchi ustunida kalit harflariga mos keluvchi qatorlarni qoldirish orqali shakllanadi. Masalan, kalit sifatida <KITOB> so‘zi tanlangan bo‘lsa, shifrlash matritsasi olti qatordan iborat bo‘ladi (2-rasm). Faqat kalit so‘zda mavjud harf qatori qoldiriladi.

Vijiner jadvali yordamida shifrlash algoritmini amalga oshirish uchun dastlabki matnning har bir harfi ostiga kalit so‘zning harflari ketma-ket joylashtiriladi. Bunda qatorni to‘ldirish uchun kalit so‘z keraklicha takrorlanadi.

1-jadval

### Shifrlash jarayoni

<b>T<sub>o</sub></b>	a	x	b	o	r	o	t	x	a	v	f	s	i	z	l	i	g	i
<b>K</b>	k	i	t	o	b	k	i	t	o	b	k	i	t	o	b	k	i	t

2-rasmda keltirilgan shifrlash matritsasi asosida quyidagi natija olinadi:

2-jadval

### Shifrlash natijasi

<b>T<sub>o</sub></b>	a	x	b	o	r	o	t	x	a	v	f	s	i	z	l	i	g	i
<b>K</b>	k	i	t	o	b	k	i	t	o	b	k	i	t	o	b	k	i	t
<b>T</b>	k	f	u	c	s	y	b	q	o	w	p	a	b	n	m	s	o	b

Ushbu natijani tushunib olish uchun “f” harfini shifrini keltiramiz. Bunda 1-jadvalga binoan “f” harfiga “k” harfi mos keladi (3-rasmda kattalashtirib keltirilgan). Demak, 2-rasmdagi shifrlash matritsasida “k”-qator bilan “f”-ustun kesishmasidagi harf tanlanadi (belgilangan kvadrat katakchadagi “p” harfi):

a	b	c	d	e	F	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
K	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

3-rasm. Shifrlash jarayoni

Natijada  $T = \langle KFUC\ SYBQ\ OWPA\ BNMS\ OB^{**} \rangle$  shifrmatrani aniqlanildi.

Deshifrlash jarayoni ham xuddi shunday ketma-ketlikda amalga oshiriladi.

3-jadval

### Deshifrlash jarayoni

<b>T</b>	k	f	u	c	s	y	b	q	o	w	p	a	b	n	m	s	o	b
<b>K</b>	k	i	t	o	b	k	i	t	o	b	k	i	t	o	b	k	i	t
<b>T<sub>o</sub></b>	a	x	b	o	r	o	t	x	a	v	f	s	i	z	l	i	g	i

Deshifrlangan matn bo‘laklarga ajratilmasdan yoziladi. Xizmatchi belgilar ham olib tashlanadi. Natijada quyidagi hosil qilinadi:  $T_o = \langle AXBOROT XAVFSIZLIGI \rangle$ .

### Topshiriq

Quyida berilgan so‘zlarda bo‘sh kataklarni inobatga olmay berilgan kalit yordamida shifrlang va desifrlang.

## Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>kalit</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>kalit</b>
1	dasturiy qaroqchilik	kub	17	qiziq matematika	odam
2	bibliografik tavsif	aql	18	bilimlar ombori	yangi
3	kutubxona fayli	virus	19	axborot biznesi	vaqt
4	dasturiy vositalar	anti	20	axborot balansi	odat
5	dasturni sozlash	harf	21	buyruqlar satri	islom
6	telefon trubkasi	disk	22	yangi daftarlar	hayot
7	universitet binosi	flesh	23	axborot bozori	mars
8	dasturiy jamlanma	bino	24	vaqt mashinasi	oqim
9	axborot eskirishi	fayl	25	bosh sahifachi	bosh
10	axborot butunligi	ilova	26	bull algebrasi	tugma
11	dasturiy mahsulot	qator	27	raqamlar ayirmasi	tok
12	axborot agentligi	kimyo	28	yangi texnologiya	olma
13	dasturiy ilovalar	avlod	29	boshqaruv xonasi	anor
14	beta testlash	dunyo	30	banklararo tizim	qovun
15	operatsion tizim	zamin	31	sehrli kvadrat	xurmo
16	buyruq qatori	zamon	32	gammalash usuli	qush

### 3.3.3. ADFGX usuli

ADFGX yoki ADFGVX usullarida ikki yondashuv qo‘llaniladi: o‘rniga qo‘yish va o‘rin almashtirish. ADFGX usulida  $5 \times 5$  o‘lchamli matritsa va ADFGVX usulida esa  $6 \times 6$  o‘lchamli matritsa qo‘llaniladi.

Bu yerda faqatgina ADFGX usuli ko‘rib chiqilgan. Birinchi navbatda  $5 \times 5$  o‘lchamli matritsanı lotin harflari bilan to‘ldiramiz va bunda harflar tartibsiz joylashtiriladi (Eslatib o‘tamiz, bu yerda i va j harflari bitta harf sifatida qabul qilinadi). Shu bilan birga birinchi qator va ustunda ADFGX harflari joylashtiriladi, masalan (1-rasm):

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	i	c	u	x
X	m	r	e	w	y

1-rasm. Shifrllovchi jadval

Keyingi jarayonlarda kalit so‘z talab etiladi, masalan “formula”. Ochiq matn sifatida “one two three” so‘zlarini kiritamiz va har bir harfga 2 ta harfni 1-rasmga mos ravishda almashtiramiz (2-rasm).

o	n	e	t	w	o	t	h	r	e	e
DF	FX	XF	AD	XG	DF	AD	DD	XD	XF	XF

2-rasm. Almashtirish jarayoni

Ushbu natijani kalit so‘z ostidan qator bo‘ylab tartib bilan joylashtiramiz va jadvalni to‘ldirishda oxirgi belgini takroran yozamiz:

f	o	r	m	u	l	a
D	F	F	X	X	F	A
D	X	G	D	F	A	D
D	D	X	D	X	F	X
F	X	F	X	F	X	F

3-rasm. Kalit so‘zni va shifrni joylashtirish

Jadvalni ustun bo‘yicha tartiblash uchun kalit so‘zining ostidan quyidagi raqamlashtirishni amalga oshiramiz (4-rasm):

f	o	r	m	u	l	a
2	5	6	4	7	3	1
D	F	F	X	X	F	A
D	X	G	D	F	A	D
D	D	X	D	X	F	X
F	X	F	X	F	X	F

4-rasm. Kalit so‘zini raqamlashtirish

Keltirilgan kalit harflarini o‘sish tartibi bo‘yicha tartiblaymiz (5-rasm):

a	f	l	m	o	r	u
1	2	3	4	5	6	7
A	D	F	X	F	F	X
D	D	A	D	X	G	F
X	D	F	D	D	X	X
F	F	X	X	X	F	F

5-rasm. Ustunlarni tartiblash

Tartiblangan jadvaldan (5-rasm) harflar ustun bo‘yicha yoziladi va quyidagi shifrmatn hosil bo‘ladi: ADXF DDDF FAFX XDDX FXDX FGXF XFXF.

Ushbu yondashuvning Polibiy usuliga o‘xhashlik jihatlari mavjud bo‘lib, faqat bunda shifrmatn bevosita ochiq matnga nisbatan ikki baravar katta hajmda bo‘ladi.

### Topshiriq

Berilgan ochiq matnni  $T_0$  bevosita 1-jadvalga asoslanib ADFGX usuli orqali shifrlang.

#### Variantlar

№	Shifrlanadigan so‘z ( $T_0$ )	Kalit	№	Shifrlanadigan so‘z ( $T_0$ )	Kalit
1	dasturiy vosita	kabinet	12	axborot biznesi	joylash
2	tavsif asoslari	dasturi	13	ilovalar narxi	formula
3	mashina markasi	yuklash	14	xavfsiz chora	kabinet
4	dasturiy guruh	yetarli	15	fotoapparat izi	dasturi
5	buyruqlar satri	xavfsiz	16	texnologiyalar	yuklash
6	mantiqiy ayirma	kabinet	17	banklar tizimi	yetarli
7	filial xonasi	dasturi	18	dastur menyusi	xavfsiz
8	dasturiy asos	yuklash	19	mobil telefon	joylash
9	eskirish sababi	yetarli	20	kommunikatsiya	formula
10	axborot hujumi	xavfsiz	21	qiziqarli mavzu	kabinet
11	dasturiy bozor	kabinet	22	raqamli jihoz	dasturi

### 3.4. O‘rin almashtirish usuli

Shifrlash jarayonida ochiq ma’lumot alifbo belgilarining o‘rnlari almashtirilsa, bunday shifrlash algoritmi o‘rin almashtirish shifrlash sinfiga kiradi. Bunda belgilar ma’lum sxema bo‘yicha almashtiriladi. Olingan shifrlangan matn o‘rin almashtirish shifri deb ataladi. Demak, o‘rin almashtirish – bu ochiq matnni nisbatan oddiy kriptografik almashtirishlardan biri bo‘lib, uni shifrlashda shu matn

bloki doirasida ma'lum qoida bo'yicha elementlar (yoki ularning guruhlari) bir-biri bilan joy almashadi. Bunda elementlarning o'zi o'zgarmasdan qoladi.

Ko'rinib turibdiki, o'rin almashtirish shifrlash algoritmlarida ochiq ma'lumotni tashkil etuvchi alifbo belgilarining ma'nosi shifr ma'lumotda ham o'zgarmasdan qoladi. Aksincha, o'rniga qo'yish shifrlash algoritmlarida shifrma'lumotni tashkil etuvchi alifbo belgilari ma'nosi ochiq ma'lumotni tashkil etuvchi alifbo belgilarining ma'nosi bilan bir hil bo'lmaydi. Shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarining kombinatsiyalaridan bиргаликда foydalanilsa, bunday shifrlash algoritmi aralash shifrlash turkumiga kiradi. Demak, shifrlash algoritmlari akslantirish turlariga qarab o'rniga qo'yish, o'rin almashtirish va aralash shifrlash usullariga bo'linadi.

O'rin almashtirish shifrlash algoritmlarining asosiy xususiyati ochiq ma'lumot va shifrma'lumot alifbosi belgilarining bir xilligidadir, ya'ni shifrma'lumotni tashkil etuvchi belgilarning ma'nosi mos keluvchi ochiq ma'lumotdag'i belgilarning ma'nosi bilan bir xil bo'ladi. Haqiqatan ham, o'rin almashtirish shifrlash jarayonida ochiq ma'lumot alifbosi belgilari o'rinlari almashtirilishi natijasida shifrma'lumot hosil qilinadi.

Bunday shifrlash algoritmlarida kalit uzunligi, umuman olganda, shifrlanishi kerak bo'lgan ma'lumot uzunligiga, ya'ni ochiq ma'lumot tashkil etuvchi alifbo belgilarining soniga teng. Bundan tashqari, ochiq ma'lumotni tashkil etuvchi alifbo belgilarining chastotali xususiyatlari to'laligicha shifrma'lumotga o'tadi. Bunday holatlar amaliy tatbiq imkoniyatlarini cheklaydi. Shunday bo'lsada ularning samarali tatbiqlarini ta'minlashga qaratilgan ko'pgina usullar mavjud.

Shunday qilib, ushbu o'rniga qo'yish va o'rin almashtirish usullarni taqqoslash nuqtayi nazar quyidagi misollarni ko'rib chiqamiz. Bu yerda "HIMOYA" so'zini shifrlaymiz.

O'rniga qo'yish usuli uchun, misol sifatida quyidagi jadvalni qo'llaymiz:

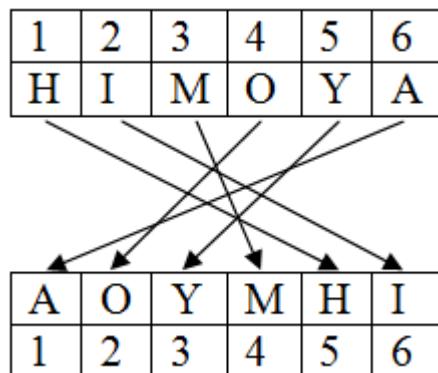
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Demak, "HIMOYA" so'zi uchun quyidagi "IJNPZB" natijaga erishamiz.

O‘rin almashtirish usulida esa, masalan, quyidagi almashuvlarni kiritamiz:

1 – 5 2 – 6 3 – 4 4 – 2 5 – 3 6 – 1

Natijani jadval shaklida keltiramiz



Demak, “HIMOYA” so‘zi uchun quyidagi “AOYMHI” natijaga erishamiz. Endi aralash usuliga misol keltiramiz. Bunda ikkala usuldan ketma-ket foydalanamiz:

### **o‘rin almashtirish + o‘rniga qo‘yish**

O‘rin almashtirish usuli orqali “HIMOYA” so‘zi uchun olingan natijaga “AOYMHI” yuqoridagi jadval asosida o‘rniga qo‘yish usulini qo‘llaymiz va quyidagi natijani olamiz: “BPZNIJ”. O‘rinlarini almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin: **shifrllovchi jadval** va **sehrli kvadrat**.

### **Topshiriq**

O‘rin almashtirish usulida quyidagi almashuvlarni bir necha bor qo‘llab 1 – 5 2 – 6 3 – 4 4 – 2 5 – 3 6 – 1, ko‘rsatilgan qadamdagি olingan natijani aniqlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>Qadam</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>Qadam</b>
1	BUXORO	3	11	SAHIFA	4
2	DASTUR	4	12	DENGIZ	4
3	SONLAR	2	13	BALANS	3
4	KODLAR	5	14	XAVFLI	3
5	TARMOQ	4	15	VOSITA	4
6	ALIFBO	3	16	DOKTOR	5
7	DAFTAR	2	17	AMALIY	5
8	BUYRUQ	3	18	KARNAY	4
9	DELFIN	4	19	TAHLIL	3
10	YULDUZ	5	20	YORDAM	5

### **3.4.1. Shifrllovchi jadval**

Shifrllovchi jadval usulida kalit sifatida quyidagilar qo‘llaniladi:

- jadval o‘lchovlari;
- so‘z yoki so‘zlar ketma-ketligi;
- jadval tarkibi xususiyatlari.

**Misol.** Quyidagi ochiq matn berilgan bo‘lsin:

#### **TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI**

Ochiq axborot ustun bo‘yicha ketma-ket jadvalga kiritiladi:

T	N	R	N	Y	U	S	S	A	I
O	T	O	O	A	N	I	A	N	A
S	A	T	L	L	I	T	M	D	L
H	X	T	O	A	V	E	A	F	I
K	B	E	G	R	E	T	R	I	*
E	O	X	I	I	R	I	Q	L	*

Natijada, 6x10 o‘lchovli jadval tashkil qilinadi. Endi shifrlangan matn qatorlar bo‘yicha aniqlanadi, ya’ni o‘zimiz uchun 4 tadan belgilarni ajratib yozamiz:

**TNRN YUSS AIOT OOAN IANA SATL LITM DLHX TOAV EAFI KBEG  
RETR I\*EO XIIR IQL\***

Bu yerda kalit sifatida jadval o‘lchovlari xizmat qiladi.

#### **Topshiriq**

Shifrllovchi jadval usulidan foydalanib ma’lumotlarni jadval o‘lchovlari kaliti (*k*) asosida shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>k</b>
1	KOMPYUTER TEXNOLOGIYALARI BIZNESDA	4x8
2	MA’LUMOTLARNING DARAXTSIMON MODELI	6x6
3	AXBOROT TEXNOLOGIYALAR VA TIZIMLARI	8x4
4	AXBOROTLASHTIRISH TO‘G‘RISIDAGI QONUN	7x5
5	KRIPTOGRAFIYANING MATEMATIK ASOSLARI	5x7

6	MA'LUMOTLARNI STEGANOGRAFIYADA YASHIRISH	6x7
7	KLAVIATURA TUGMALARINING TAVSIFI	5x6
8	SHIFRLANGAN MATNNI DESHIFRLASH	6x5
9	O'ZBEKISTON TARAQQIYOT OSTONASIDA	4x8
10	RAQAMLI TEXNOLOGIYALARDA INNOVATSIYA	7x5
11	TA'LIMNI RIVOJLANISHDA PEDTEXNOLOGIYALAR	5x8
12	O'ZBEKISTON YUKSALISH DAVRIDA	7x4
13	TELEVIZORLARNING MAVJUD TASNIFI	4x8
14	MONITORING JARAYONI MAZMUNI	3x9
15	SIGNALLARNI UZATISHDA MODULYATOR	5x6
16	TRANSLYATOR VA UNING TURLARI	5x5
17	KOMPILYATORNING ASOSIY MAZMUNI	7x4
18	INTERPRETATORLI DASTURLARGA MISOLLAR	5x7
19	SUN'iy INTELLEKTNING RIVOJLANISHI	4x8
20	PSEVDOTASODIFIY SONLAR GENERATORI	7x5

### 3.4.2. Tayanch so'zli shifrllovchi jadval

Shifrllovchi jadval usulini murakkablashtirish maqsadida tayanch so'zni kiritса bo'ladi. Yuqoridagi **TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI** misoli uchun quyidagi

#### TEZLASHMOQ

so'zini olamiz va oldingi paragrafda keltirilgan jadvalga joylashtiramiz:

T	E	Z	L	A	S	H	M	O	Q
9	2	10	4	1	8	3	5	6	7
T	N	R	N	Y	U	S	S	A	I
O	T	O	O	A	N	I	A	N	A
S	A	T	L	L	I	T	M	D	L
H	X	T	O	A	V	E	A	F	I
K	B	E	G	R	E	T	R	I	*
E	O	X	I	I	R	I	Q	L	*

Ikkinchi qatordagi raqamlar harflarning alifbo harflari ketma-ketligi bo'yicha tartiblashdan kelib chiqadi. Shu qatordagi raqamlar bo'yicha ustunlarni tartiblaymiz:

A	E	H	L	M	O	Q	S	T	Z
1	2	3	4	5	6	7	8	9	10
Y	N	S	N	S	A	I	U	T	R
A	T	I	O	A	N	A	N	O	O
L	A	T	L	M	D	L	I	S	T
A	X	E	O	A	F	I	V	H	T
R	B	T	G	R	I	*	E	K	E
I	O	I	I	Q	L	*	R	E	X

Shifrlangan matn quyidagi ko‘rinishda bo‘ladi:

YNSN SAIU TRAT IOAN ANOO LATL MDLI STAX EOAF IVHT RBTG RI\*E  
KEIO IIQL \*REX

### **Topshiriq**

Tayanch so‘zli shifrllovchi jadval usulidan foydalanib ma’lumotlarni jadval o‘lchovlari kaliti (*k*) asosida shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>Kalit (k)</b>	<b>Tayanch so‘z</b>
1	ochiq kalitdan foydalangan	4x7	texnika
2	identifikasiyalash va autentifikasiyalash usuli	7x7	magistr
3	kompyuter virusini tizimga kiritish	6x6	kotiba
4	yashirin tinglash qurilmasi haqida	5x7	tamoyil
5	kompyuter viruslari va ulardan himoyalanish	5x8	dasturiy
6	axborot xavfsizligida himoyalash usuli haqida	7x6	mantiq
7	pgp algoritmi haqida tushuncha	5x6	mantiq
8	simmetriyali kriptotizim asoslari	7x5	haker
9	gamilton marshruti asosida shifrlash usullari	6x7	tezlash
10	analitik usullariga asoslangan shifrlash algoritmi	6x8	mustaqil
11	kompyuter tarmoqlarida axborotni himoyalash	5x8	mahsulot
12	axborotni himoyalash funksiyalari	4x8	agentlik
13	parol yordamida shifrlash	4x6	piyoda
14	masofadan rasmga tushirish	5x5	idora
15	himoyalash vositalari haqida tushuncha	6x6	enigma
16	simmetrik shifrlash usullar	5x5	nashr
17	maxfiy xabarlarning mavjudligini yashirish	5x8	shaftoli
18	kompyuter steganografiyasi rivojlanish tendensiyasi	7x7	teskari
19	super kompyuterlar ishlatilganda bir asr kam	5x8	tezlamoq

20	yeterli darajada kriptobardoshlilik	5x7	sozlash
21	shifrlash va qaytarish jarayonining oddiyligi	6x7	tasodif
22	himoyalash vositalarini qasddan ishdan chiqarish	5x9	marketing
23	shifrlangan matnlarni yaratish	5x6	turizm
24	cloud computing texnologiyalari	5x6	moliya
25	elektron raqamli imzo	4x5	dinar
26	shifrlangan matn jadval elementlari	4x8	logarifm
27	affin tizimidagi sezar usulidan	4x7	tumaris
28	sezar usulida almashtiruvchi harf	5x6	tarmoq
29	algoritmlar integral sxemalarda amalgalash oshiriladi	6x8	integral
30	hozirgi kompyuter tarmoqlari haqida	4x8	xorazmiy
31	elektron pochtada kuzatiladi	4x7	avtobus
32	sezar usulining kamchiligi	4x6	mansub

### 3.4.3. Matritsa usuli

Matritsa usuli tayanch so‘zli shifrllovchi jadval usuliga o‘xshash bo‘lib, faqat bu yerda 2 ta kalit mavjud bo‘ladi. Bu yerda birlamchi bo‘sh  $M \times N$  o‘lchamli matritsa shakllantiriladi. Shu bilan birga 2 ta kalit so‘zlar  $K_M$  va  $K_N$  kiritiladi. Kalitlarning uzunligi matritsa tomonlariga teng bo‘ladi. Ochiq matn matritsaga chapdan o‘ngga qarab yoziladi. Matritsaning chekkalaridan mos ravishda kalitlar yoziladi. Matritsa qatorlari o‘rin almashtirish orqali kalit harflarini tartiblash bilan joylashtiriladi. Ushbu jarayonni ustun kaliti bilan ham bajaramiz. Natijada matritsadan harflar ustun bo‘yicha o‘qiladi va shifrlangan matn shakllanadi.

Misol sifatida  $M=5, N=4$  o‘lchamli matritsani va  $K_M = “kitob”$  va  $K_N = “shar”$  so‘zlarini quyidagicha joylashtiriladi:

	s	h	a	r
k				
i				
t				
o				
b				

1-rasm. Shifrllovchi jadval

Shifrllovchi jadvalga quyidagi “**kompyuter sohasida axborot xavfsizligi**” ochiq matnni qator bo‘ylab joylashtiramiz (1-qadam, 2-rasm). Agar jadval to‘lib

qolsa, unda yana bitta jadval ochiladi. Agar oxirgi jadval to‘lmay qolsa, unda, masalan, ‘o’ harflari bilan to‘ldiriladi:

<b>1-qadam</b>	<b>2-qadam</b>	<b>3-qadam</b>	<b>4-qadam</b>
	<b>s h a r</b>		<b>a h r s</b>
k o m p	k k o m p	b a a x b	b x a b a
y u t e	i y u t e	i y u t e	i t u e y
r s o h →	t r s o h →	k k o m p →	k m o p k
a s i d	o a s i d	o a s i d	o i s d a
a a x b	b a a x b	t r s o h	t o s h r
	<b>s h a r</b>		<b>a h r s</b>
o r o t	k o r o t	b o o o o	b o o o o
x a v f	i x a v f	i x a v f	i v a f x
s i z l →	t s i z l →	k o r o t →	k o r t o
i g i o	o i g i o	o i g i o	o i g o i
o o o o	b o o o o	t s i z l	t z i l s

## 2-rasm. Shifrlash jarayoni

2-qadamda jadval tomonlarida kalit so‘zlar joylashtiriladi. 3-qadamda qatorlar o‘rin almashtiriladi va bunda kalit so‘z alifbo tartibida bo‘lishi kerak. 4-qadamda ustunlar o‘rin almashtiriladi va bunda kalit so‘z alifbo tartibida bo‘lishi kerak. Natijada hosil bo‘lgan harflar ketma-ketligi ustun bo‘ylab terib chiqiladi va natijaviy shifrmatn quyidagi ko‘rinishda bo‘ladi:

**xtmioauossbepdhaykarovoizoargioftoloxois**

## Topshiriq

Yuqorida keltirilgan  $M=5$ ,  $N=4$  o‘lchamli matritsani va  $K_M$  = “kitob” va  $K_N$  = “shar” kalit so‘zlaridan foydalanib ma’lumotlarni shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	kompyuter viruslaridan himoyalanish
2	autentifikasiya jarayonlarining tahlili
3	identifikasiyadan o‘tishning maqsadi
4	yashirin qurilmalar tasnifi

5	internet va himoyalanish asri
6	xavfsiz axborot va ma'lumot
7	massivni saralash algoritmi haqida
8	axborotni shifrlashda kriptotizimlar
9	shifrlashning gamilton usuli haqida
10	shifrlashning analitik usullari
11	tarmoq himoyasini yaratish
12	axborotni himoyalashda shifrlash
13	ikkilik sanoq tizimi haqida
14	telefon orqali rasmga tushirish
15	serverni himoya qilish vositalari

#### 3.4.4. Sehrli kvadrat

Sehrli kvadrat deb katakchalariga 1 dan boshlab sonlar yozilib, undagi har bir ustun, satr va diagonal bo'yicha sonlar yig'indisi bitta songa teng bo'lgan kvadrat shaklidagi jadvalga aytildi.

Sehrli kvadratga sonlar tartibi bo'yicha belgilar kiritiladi va bu belgilar satrlar bo'yicha o'qilganda matn hosil bo'ladi.

**Misol.** 4x4 o'lchovli sehrli kvadratni olamiz. Bu yerda sonlarning har xil kombinatsiyasi orqali bevosita 880 ta sehrli kvadratni yaratish mumkin. Bu yerda faqatgina quyidagi variantni tanlaymiz:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Boshlang'ich matn sifatida quyidagi matnni olamiz: **DASTURIY VOSITASI** va jadvalga joylashtiramiz:

I	S	A	T
U	O	S	Y
V	R	I	I
T	S	A	D

Shifrlangan matn jadval elementlarini satrlar bo'yicha o'qish natijasida tashkil topadi: **IUVT SORS ASIA TYID**

### Topshiriq

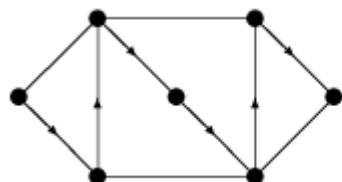
4x4 o'lchovli sehrli kvadratdan foydalanib ma'lumotlarni shifrlang.

#### Variantlar

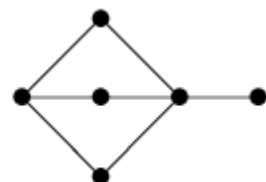
<b>№</b>	<b>Shifrlanadigan so'z</b>	<b>№</b>	<b>Shifrlanadigan so'z</b>
1	kompyuter virusi	16	maxfiy xabarlar
2	autentifikasiya	17	steganografiyasi
3	identifikasiya	18	superkompyuter
4	yashirin qurilma	19	criptobardoshlik
5	himoyalanish asri	20	shifrlash usuli
6	xavfsiz axborot	21	himoya vositalari
7	algoritm haqida	22	shifrlangan matn
8	kriptotizim asosi	23	cloud computing
9	gamilton usullari	24	raqamli imzo usuli
10	analitik usullar	25	jadval elementi
11	tarmoq himoyasi	26	ikkilik tub sonlar
12	axborot himoyasi	27	almashtirish soni
13	shifrlash paroli	28	integral sxemalar
14	rasmga tushirish	29	hozirgi kompyuter
15	himoyachi haqida	30	elektron pochta

#### 3.4.5.Gamilton usuli

Shifrlangan matnning bardoshligini oshirish yo'llaridan biri bu o'rinn almashtirish usulida gamilton siklini qo'llash hisoblanadi. Gamilton sikli tushunchasi graflar nazariyasiga mansub bo'lib, bunda grafning barcha uchlarini takrorlanmaydigan ketma-ket qamrab olgan siklga aytildi. Har qanday grafda Gamilton sikli mavjud bo'lishi haqida shu vaqtgacha hech qanday ma'lumot yo'q. Quyida Gamilton sikliga misol keltirilgan:

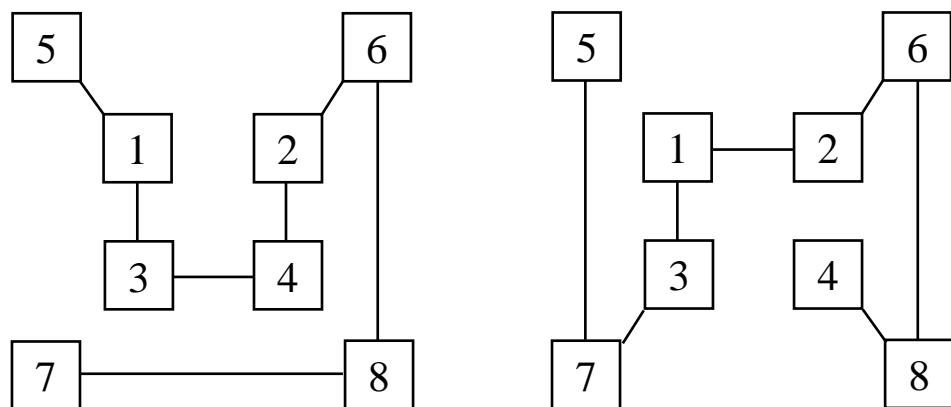


Gamilton sikli bor



Gamilton sikli yo'q

Gamilton siklini matnni shifrlashda qo'llashda grafning barcha uchlarini aylanib chiqish orqali amalga oshiriladi. Bunda shifrlash kaliti graf uchlari soni va marshrutlar bilan belgilanadi va har safar har xil marshrutlar qo'llaniladi. Masalan, quyida keltirilgan (1-rasm) 8 ta uchli graflarda mavjud Gamilton sikllari uchun mavjud marshrutlar 5-1-3-4-2-6-8-7 va 5-7-3-1-2-6-8-4 bevosita belgilarning o'rnini almashtirish uchun qo'llaniladi. Matndagi belgilar ushbu marshrutlarda keltirilgan tartibda keltiriladi.



1-rasm. Gamilton marshrutlari

Quyidagi misolda 1-rasmda keltirilgan marshrutlar asosida “SAMARQANDYULDUZI” matnni shifrlaymiz va buning uchun ma'lumotlarni jadvalga joylashtiramiz (1-jadval). Agarda oxirgi blok to'lmay qolsa, unda bo'sh kataklarni, masalan, “\*” belgisi bilan to'ldirish mumkin. Matn ikki blokga ajratiladi va har biri uchun alohida o'rin almashtirish qo'llaniladi.

1-jadval  
Gamilton marshrutlari asosida o'rin almashtirish tartibi.

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
S	A	M	A	R	Q	A	N	D	Y	U	L	D	U	Z	I
5	1	3	4	2	6	8	7	5	7	3	1	2	6	8	4
R	S	M	A	A	Q	N	A	D	Z	U	D	Y	U	I	L

Olingan natijani RSMAAQNADZUDYUIL ham bloklarga ajratish mumkin, masalan, RSMA AQNA DZUD YUIL. Olingan natijani deshifrlash uchun ham 1-jadvaldan foydalilanadi. Marshrutlar sonini ko'paytirish orqali esa ushbu usulning kriptobardoshligini oshirish mumkin bo'ladi.

## Topshiriq

Quyidagi Gamilton 5-1-3-4-2-6-8-7 va 5-7-3-1-2-6-8-4 marshrutlaridan foydalanib o‘rin almashtirish orqali ma’lumotlarni shifrlang va bunda bo‘sh kataklar inobatga olinmasin.

### Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	kompyuter virusi	16	maxfiy xabarlar
2	autentifikasiya	17	steganografiyasi
3	identifikasiya	18	superkompyuter
4	yashirin qurilma	19	criptobardoshlik
5	himoyalanish asri	20	shifrlash usuli
6	xavfsiz axborot	21	himoya vositalari
7	algoritm haqida	22	shifrlangan matn
8	kriptotizim asosi	23	cloud computing
9	gamilton usullari	24	raqamli imzo usuli
10	analitik usullar	25	jadval elementi
11	tarmoq himoyasi	26	ikkilik tub sonlar
12	axborot himoyasi	27	almashtirish soni
13	shifrlash paroli	28	integral sxemalar
14	rasmga tushirish	29	hozirgi kompyuter
15	himoyachi haqida	30	elektron pochta

### 3.5. Shifrlashning analitik usullari

Shifrlashning analitik usullari bevosita algebraning bir tomonlama funksiyalariga asoslanib ishlab chiqilgan. Har qanday funksiya  $y=f(x)$  bir tomonlama funksiya deb qabul qilinadi, agar  $x$  ochiq matndan shifrlanilgan y matnni cheklangan qadamlar jarayonida shakllantirish mumkin bo‘lsa va teskari jarayonni hisoblash uchun esa juda ko‘p vaqt talab etilsa.

Bir tomonlama funksiyalarga quyidagilarni misol qilib keltirsa bo‘ladi:

- matritsalarni ko‘paytirish;
- xaltaga buyumlarni joylashtirish masalasini yechish;
- polynom qiymatini modul bo‘yicha hisoblash;
- darajalarni hisoblash va b.

#### 3.5.1. Matritsalarni ko‘paytirish usuli

Shifrlashning analitik usullari bevosita algebraning matritsalar bilan bajariladigan amallari orqali ifodalanadi. Bu yerda ochiq matn  $n$  uzunlikdagi

bloklarga taqsimlanadi va har bir blok vektor  $b = (b_1, b_2, \dots, b_n)$  sifatida qabul qilinadi. Hosil qilingan vektorni kvadrat  $n \times n$  matritsaga  $A = \|a_{ij}\|$  ko‘paytirish orqali shifrmatn  $c = (c_1, c_2, \dots, c_n)$  tashkil etiladi:

$$c_i = \sum_j a_{ij} b_j.$$

Deshifrlash uchun esa teskari  $A^{-1}$  matritsani  $c = (c_1, c_2, \dots, c_n)$  vektorga ko‘paytirish talab etiladi.

**Misol.** Berilgan ochiq matnni  $T_0 = <\text{TAHLIL}>$  quyidagi matritsa orqali shifrlang:

$$A = \begin{pmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{pmatrix}$$

*Yechimi.* Shifrlanadigan matn bir xil  $n$  uzunlikdagi bloklarga bo‘linadi va  $n \times n$  o‘lchamli kvadrat matritsaga ko‘paytiriladi. Bu matritsa keltirilgan usulning kaliti hisoblanadi. Deshifrlashni bajarish uchun ushbu matritsa teskari matritsaga ega bo‘lishi kerak. Shifrlashni amalga oshirish uchun quyidagi qadamlarni birin-ketin bajaramiz:

0-qadam. Bunda harflar, masalan faqatgina lotin harflari uchun, quyidagi jadval asosida raqamlanadi:

1-jadval

#### **Harflarni sonlar bilan ifodalash**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1-qadam. Ochiq “TAHLIL” matnni 1-jadvalga asoslanib sonlar orqali belgilaymiz:  $T_0 = <20, 1, 8, 12, 9, 12>$ .

2-qadam. Endi  $A$  matritsani birin-ketin quyidagi vektorlarga ko‘paytiramiz:

$b_1 = (20, 1, 8)$  va  $b_2 = (12, 9, 12)$ :

$$c_1 = \begin{pmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 1 \\ 8 \end{pmatrix} = \begin{pmatrix} 88 \\ 83 \\ 169 \end{pmatrix},$$

$$c_2 = \begin{pmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 9 \\ 12 \end{pmatrix} = \begin{pmatrix} 144 \\ 123 \\ 213 \end{pmatrix}.$$

3-qadam. Bu yerdan shifrmattn quyidagi sonlardan iborat bo‘ladi:  $T_1 = \langle 88, 83, 169, 144, 123, 213 \rangle$ .

Olingan natijani tekshirish uchun deshifrlash jarayonini quyidagicha bajaramiz:

1-qadam.  $A$  matritsaning determinantini hisoblaymiz (bu yerda keng tarqalgan amaliy dasturlardan foydalanish mumkin, masalan, MS Excel):  $|A| = -115$ .

2-qadam.  $A$  matritsaning algebraik to‘ldiruvchilarini hisoblab, uning qo‘shib olingan matritsasini  $A^*$  aniqlaymiz. Qo‘shib olingan  $A^*$  matritsa  $A$  ning har bir  $a_{ij}$  elementi o‘rniga uning  $A_{ij}$  algebraik to‘ldiruvchisi qo‘yilgan bo‘ladi.

$$A^* = \begin{pmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{pmatrix}$$

Qo‘shib olingan  $A^*$  matritsa quyidagi xossaga ega (bu yerda  $D = |A|$ ):

$$AA^* = A^*A = \begin{pmatrix} D & & 0 \\ & \ddots & \\ 0 & & D \end{pmatrix}$$

Misol sifatida algebraik to‘ldiruvchini hisoblashdagi faqatgina bitta variantini keltiramiz, ya’ni  $A_{23}$ :

$$A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 4 \\ 6 & 9 \end{vmatrix} = -(1 \cdot 9 - 4 \cdot 6) = 15.$$

3-qadam. Aniqlangan  $A^*$  matritsaning transponirlangan  $A^T$  matritsasini hisoblaymiz:

$$A^T = \begin{pmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{pmatrix}$$

4-qadam. Teskari matritsani quyidagi formula bo‘yicha hisoblaymiz:

$$A^{-1} = A^T / |A|.$$

Ushbu formula bo‘yicha quyidagi natijani olamiz:

$$A^{-1} = \begin{pmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{pmatrix}$$

5-qadam. Bu yerda bevosita shifrmatndan ochiq  $b_1$  va  $b_2$  matnni tiklash jarayonini keltiramiz:

$$b_1 = A^{-1} \cdot c_1; \quad b_2 = A^{-1} \cdot c_2.$$

$$b_1 = \begin{pmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{pmatrix} \cdot \begin{pmatrix} 88 \\ 83 \\ 169 \end{pmatrix} = \begin{pmatrix} 20 \\ 1 \\ 8 \end{pmatrix}.$$

Faqat  $b_1$  ning birinchi elementining hisobini keltiramiz:

$$(-17 \cdot 88 - 52 \cdot 83 + 48 \cdot 169) / 115 = (-1496 - 4316 + 8112) / 115 = 2300 / 115 = 20;$$

$$b_2 = \begin{pmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{pmatrix} \cdot \begin{pmatrix} 144 \\ 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 12 \\ 9 \\ 12 \end{pmatrix}.$$

Faqat  $b_2$  ning uchinchi elementining hisobini keltiramiz:

$$(15 \cdot 144 - 15 \cdot 123 + 5 \cdot 213) / 115 = (2160 - 1845 + 1065) / 115 = 1380 / 115 = 12;$$

6-qadam. Olingan natija  $T_0 = \langle 20, 1, 8, 12, 9, 12 \rangle$  1-jadvalga binoan ochiq matnga “TAHLIL” so‘ziga mos keldi.

### Topshiriq

Berilgan ochiq matnni  $T_0$  bevosita 1-jadvalga asoslanib matritsalarni ko‘paytirish usuli orqali shifrlang va deshifrlang.

<b>№</b>	<b>Matritsa, <math>A</math></b>	<b>Ochiq matn, <math>T_0</math></b>	<b>№</b>	<b>Matritsa, <math>A</math></b>	<b>Ochiq matn, <math>T_0</math></b>
1	$\begin{pmatrix} 3 & 3 & 3 \\ 5 & 2 & 1 \\ 2 & 4 & 2 \end{pmatrix}$	AFSONA	2	$\begin{pmatrix} 3 & 2 & 1 \\ 2 & 2 & 2 \\ 5 & 1 & 2 \end{pmatrix}$	SHIFRLASH
3	$\begin{pmatrix} 3 & 3 & 3 \\ 3 & 2 & 1 \\ 5 & 2 & 2 \end{pmatrix}$	TELEVIZOR	4	$\begin{pmatrix} 3 & 1 & 1 \\ 2 & 2 & 3 \\ 3 & 2 & 3 \end{pmatrix}$	KOMPYUTER
5	$\begin{pmatrix} 5 & 1 & 1 \\ 4 & 5 & 2 \\ 1 & 6 & 5 \end{pmatrix}$	ANTIVIRUS	6	$\begin{pmatrix} 3 & 2 & 3 \\ 2 & 3 & 1 \\ 1 & 2 & 7 \end{pmatrix}$	DASTUR
7	$\begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 8 \\ 1 & 0 & 7 \end{pmatrix}$	AMALIY	8	$\begin{pmatrix} 3 & 1 & 1 \\ 2 & 1 & 3 \\ 4 & 1 & 1 \end{pmatrix}$	ZAMONAVIY
9	$\begin{pmatrix} 2 & 3 & 4 \\ 3 & 7 & 5 \\ 4 & 5 & 1 \end{pmatrix}$	TASODIFIY	10	$\begin{pmatrix} 1 & 2 & 4 \\ 5 & 1 & 2 \\ 3 & 1 & 1 \end{pmatrix}$	DOKTORANT
11	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{pmatrix}$	NAMUNA	12	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 6 & 4 \\ 3 & 4 & 5 \end{pmatrix}$	HIMOYA

### 3.5.2. Xaltaga buyumlarni joylashtirish masalasi

Xaltaga buyumlarni joylashtirish masalasi (ingl. Knapsack problem) – NP-to‘liq masalaga mansub bo‘lib, bunda qimmatbaho buyumlarni hajmi cheklangan xaltaga ko‘proq joylashtirish talab etiladi. Ushbu masala har xil variantlarda iqtisodiyotda, amaliy matematikada, kriptografiyada va logistikada uchrab turadi. Albatta, adabiyotlarda xalta so‘zining o‘rniga sumka, portfel, chamadon kabi so‘zlar ishlatalishi mumkin.

Umumiy holda masalani quyidagicha ta’riflash mumkin: Buyumlar narxi va og‘irligi bilan berilgan to‘plamdan shunday qismto‘plamni tanlash kerakki, bunda buyumlarning narxi maksimal bo‘lganda, ularning og‘irligi cheklangan bo‘ladi. Oddiyroq variantda quyidagi masalani keltirish mumkin: Tartib bilan berilgan 1, 6,

8, 15 va 24 og‘irlikdagi toshlar ichidan xaltaga jami 30 birlik og‘irlikdagi toshlarni joylashtirish talab etiladi. Shu bilan birga masalaning yechimi mavjud deb qabul qilinadi.

Ilk bor 1978-yilda Merkl va Xellman tomonidan xaltaga buyumlarni joylashtirish masalasiga asoslangan ochiq kalitli kriptotizim taklif etildi. Kriptografiyada murakkab masalalarga e’tibor berilishining asosiy sababi – bu umumiyl holda keltirilgan masalaning yechimi cheklangan zaruriy vaqt mobaynida aniqlash mumkin emasligida. Taklif etilgan kriptotizim faqatgina shifrlashda qo‘llanishga mo‘ljallangan bo‘lgan, keyinchalik Shamir ushbu algoritmni elektron raqamli imzo uchun moslashtirgan.

Shifrlashda ochiq buyumlar tizimidan tashkil topgan ochiq math o‘rniga ularning umumiyl vazni shifrmatn bo‘lib xizmat qiladi. Bu yerda quyidagi tushunchalar kiritiladi.

- 1) Xalta vektori  $A=(a_1, a_2, \dots, a_n)$  – bu tartiblangan buyumlar to‘plami bo‘lib, bu yerda  $a_i$  – bu  $i$ -buyumning vazni.
- 2) Xalta vektori bevosita ochiq kalit sifatida xizmat qiladi.
- 3) Ochiq matn uzunligi  $n$  bitdan iborat bo‘lgan bloklarga taqsimlanadi. Masalan,  $n=6$  bo‘lganda va ochiq matn (111100) bo‘lsa, bunda har bir bit xaltada buyumning borligini bildiradi, ya’ni birinchi to‘rtda buyum xaltada mavjud ekanligini bildiradi. Kelishuv bo‘yicha bit 1 ga teng bo ‘lsa, unda xaltada buyumning borligini, aksincha 0 bo‘lsa, yo‘qligini bildiradi.
- 4) Xaltada mavjud buyumlar vaznlari yig‘indisi hisoblanadi va shifrmatn sifatida uzatiladi.

Taklif etilgan algoritmni aniq misolda ko‘rib chiqamiz. Xalta vektori quyidagicha berilgan bo‘lsin:  $A = (3, 4, 6, 7, 10, 11)$  va  $n=6$ . Agar ochiq matn quyidagicha bo‘lsa: 1 1 1 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 1, unda uni  $n=6$  uzunlikdagi bloklarga taqsimlab olamiz va xaltani buyumlar bilan quyidagi jadvalda keltirilgan shaklda to‘ldiramiz:

Ochiq matn	1 1 1 1 1 0	0 0 1 1 0 0	0 0 0 0 0 0	0 0 0 0 0 1
Xalta buyumlari	3 4 6 7 10	6 7		11
Shifrmatn	$3+4+6+7+10=30$	$6 + 7 = 13$	0	11

Shifrmatni shakllantirishdagi ushbu usul additiv deb nomlanadi, agar ko‘paytiruv orqali shakllantirilsa, unda multiplikativ deb nomlanadi, ya’ni

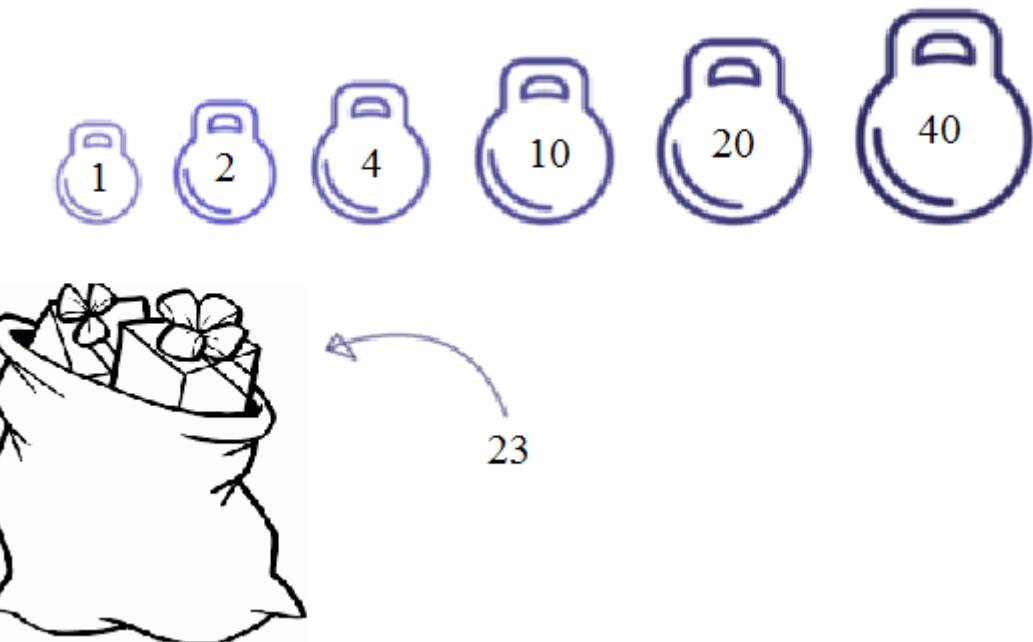
Ochiq matn	1 1 1 1 1 0	0 0 1 1 0 0	0 0 0 0 0 0	0 0 0 0 0 1
Xalta buyumlari	3 4 6 7 10	6 7		11
Shifrmatn	$3 \cdot 4 \cdot 6 \cdot 7 \cdot 10 = 5040$	$6 \cdot 7 = 42$	0	11

Bu yerda additiv usul bilan tanishib olamiz. Keltirilgan yondashuv ochiq va yopiq kalitlarni ishlab chiqishda qo‘llaniladi. Xususan, ochiq kalit sifatida “qiyin” masala yechimini aniqlash talab etiladi va uning yordamida ochiq matn shifrlanadi, ammo uning yordamida shifrmatnni deshifrlash mumkin bo‘lmaydi. Yopiq kalit sifatida “yengil” masala yechimi aniqlanadi va uning yordamida deshifrlash amalga oshiriladi.

Umumiy holda ochiq va yopiq kalitlarni shakllantirishda to‘g‘ridan- to‘g‘ri keltirilgan usulni qo‘llab bo‘lmaydi. Shu bois, ushbu masala ikkiga bo‘linadi: yengil muammo va qiyin muammo. Buning uchun tezkor o‘sish ketma-ketligi tushunchasi kiritiladi.

Tezkor o‘sish ketma-ketligi – bu agar ketma-ketlikning istalgan a’zosi bevosita undan oldin joylashgan sonlar yig‘indisidan katta bo‘lishi kerak. Masalan, quyidagi  $\{1, 3, 6, 13, 27, 52\}$  ketma-ketlik tezkor o‘sish tartibida bo‘lib, aksincha  $\{1, 3, 4, 9, 15, 25\}$  ketma-ketligi – bu tezkor o‘sish emas. Yengil muammoni quyidagi misol doirasida ko‘rib chiqamiz, ya’ni tezkor o‘sish tartibida berilgan toshlar uchun masala yechimini topish murakkab bo‘lmaydi.

Masalan, 1, 2, 4, 10, 20, 40 toshlardan xaltaga 23 og‘irlilik toshlarni jamlash kerak bo‘lsin (1-rasm).



1-rasm. Masalaning qo‘yilishi

Bunday masalaning yechimini aniqlash qiyin emas, buning uchun toshlarni tartib bilan ko‘rib chiqamiz (1-jadval) va 23 dan kichik bo‘lgan eng katta sonni olamiz, bizda bu 20. Endi  $23-20=3$  sonini olib, xuddi shunday jarayonni bajaramiz.

1-jadval

Toshlarni tanlash algoritmi.

Bosqich	Taqqoslash jarayoni	Tanlandi	Tanlash natijasi bitda	Taqqoslash qiymati
1	$40 > 23$	Y‘oq	0	
2	$20 < 23$	Ha	1	$3 = 23 - 20$
3	$10 > 3$	Y‘oq	0	
4	$4 > 3$	Y‘oq	0	
5	$2 < 3$	Ha	1	$1 = 3 - 2$
6	$1 = 1$	Ha	1	

Natijada 1, 2, 20 toshlari yechim bo‘ladi.

“Qiyin” muammoda berilgan toshlar tezkor o‘sish tartibida bo‘lmaydi, shu bois chekli vaqt mobaynida masalaning yechimini aniqlab bo‘lmaydi. Merkl va Xellman taklif qilgan yondashuvda ushbu ikki muammo bevosita biri ikkinchisidan kelib chiqadi. Buning uchun taqqoslama arifmetikasidan foydalaniłgan.

Taklif etilgan algoritmni aniq misolda ko‘rib chiqamiz. Masalan, tezkor o‘sish tartibida berilgan quyidagi sonlarni olamiz: {1, 2, 4, 10, 20, 40}. Modul  $m$  bo‘yicha hisoblashlarni amalga oshirish uchun, uning qiymati berilgan sonlar yig‘indisidan katta bo‘lishi kerak, masalan,  $m=110$  bo‘lsin. Berilgan toshlar maxsus koeffisiyent  $n$  ga ko‘paytiriladi va bu sonning modul bilan umumiyligi bo‘luvchisi bo‘lmasligi kerak, ya’ni  $(n,m)=1$  bo‘lishi shart, masalan  $n=31$  deb olamiz.

Bu yerda yopiq kalit sifatida {1, 2, 4, 10, 20, 40} qabul qilindi va u bilan quyidagi amallarni bajaramiz:

$$1 \cdot 31 \pmod{110} = 31,$$

$$2 \cdot 31 \pmod{110} = 62,$$

$$4 \cdot 31 \pmod{110} = 14,$$

$$10 \cdot 31 \pmod{110} = 90,$$

$$20 \cdot 31 \pmod{110} = 70,$$

$$40 \cdot 31 \pmod{110} = 30.$$

Bu yerdan yopiq kalit teng bo‘ladi: {31, 62, 14, 90, 70, 30}.

Shunday qilib, keltirilgan hisoblashlar natijasida ochiq kalit – {31, 62, 14, 90, 70, 30} va yopiq kalit – {1, 2, 4, 10, 20, 40} aniqlanildi. Endi shularga asoslanib ochiq matnni 100100111100101110 shifrlab jo‘natish jarayoni bilan tanishamiz.

Ochiq matnni 6 ta bitdan taqsimlab olamiz, chunki toshlar soni 6 ta, ya’ni

100100      111100      101110

Barcha amallarni jadval shaklida keltiramiz va ochiq kalit – {31, 62, 14, 90, 70, 30} ekanligini inobatga olamiz, natijada:

Ochiq matn	100100	111100	101110
Xalta buyumlari	31 90	31 62 14 90	31 14 90 70
Shifrmatn	31+90=121	31+62+14+90=197	31+14+90+70=205

Demak, shifrmatn **121, 197, 205** bo‘ladi.

Olingan natijaviy shifrmatnni deshifrlash jarayoni quyidagi qadamlardan iborat bo‘ladi:

1-qadam. Yopiq kalitdan –  $\{1, 2, 4, 10, 20.40\}$  bevosita ochiq kalitni shakllantirish jarayonida  $n=31$  va  $m=110$  deb qabul qilindi.

2-qadam.  $n^{-1}$  qiymaini hisoblash zarur bo‘ladi, ya’ni  $n \cdot n^{-1} = 1 \pmod{m}$  tenglikdan  $31 \cdot 31^{-1} = 1 \pmod{110}$  yoki  $31 \cdot x = 1 \pmod{110}$  tenglama hosil bo‘ladi. Bu yerdan  $31^{-1} = 71$  bo‘ladi.

3-qadam. Shifrmatnni  $71 \pmod{110}$  ga ko‘paytiramiz, ya’ni  
 $121 \cdot 71 \pmod{110} = 11$ ,  
 $197 \cdot 71 \pmod{110} = 17$ ,  
 $205 \cdot 71 \pmod{110} = 35$ .

4-qadam. Yopiq kalitdan foydalanib topilgan  $11, 17, 35$  vaznlarni  $\{1, 2, 4, 10, 20, 40\}$  toshlar bo‘yicha kombinatsiyalarini aniqlaymiz (quyidagi jadvalda yopiq kalitdan olinadigan toshlar kattalashtirib ko‘rsatilgan va ularning ostidan 1 yoki 0 bitlar ko‘rsatilgan):

Shifrmatn vazni	11	17	35
Xalta buyumlari	$1+10 (=11)$	$1+2+4+10 (=17)$	$1+4+10+20 (=35)$
Yopiq kalit	<b>1, 2, 4, 10, 20. 40</b>	<b>1, 2, 4, 10, 20. 40</b>	<b>1, 2, 4, 10, 20. 40</b>
Ochiq matn	1 0 0 1 0 0	1 1 1 1 0 0	1 0 1 1 1 0

Shunday qilib, deshifflash jarayonida olingan natija berilgan ochiq matnga “100100111100101110” teng bo‘ldi.

### Topshiriq

Tezkor o‘sish tartibida berilgan quyidagi ketma-ketlik  $\{1, 2, 4, 10, 20, 40\}$  va sonlar  $(m,n)=1$  uchun ochiq matnni shifrlang va deshifrlang.

Variantlar

Nº	Ochiq matn, $T_0$	$(m, n)$
1	100110110100110110	(113, 31)
2	110100011100101010	(113, 29)
3	100100011000111010	(109, 33)
4	101101111010110011	(111, 31)
5	101101111010110011	(111, 29)
6	100110101110100101	(107, 31)
7	110010101101001100	(107, 33)
8	101010101111100110	(109, 31)
9	110110111010110010	(107, 37)

10	110011011010101011	(113, 35)
11	101010010111011110	(109, 37)
12	110110011111010111	(101, 41)
13	110010101101001100	(113, 31)
14	101010101111001110	(113, 29)
15	110110111010110010	(109, 33)
16	110011011010101011	(111, 31)
17	101010010111011110	(111, 29)
18	110110011111010111	(107, 31)
19	100110110100110110	(107, 33)
20	110100011100101010	(109, 31)
21	100100011000111010	(107, 37)
22	101101111010110011	(113, 35)
23	101101111010110011	(109, 37)
24	100110101110100101	(101, 41)

### 3.6. Shifrlashning additiv usullari

Shifrlashning additiv usullarining mohiyati bevosita ochiq matnning raqamli kodlar ketma-ketligining maxsus belgilar kodlari bilan yig‘indisi orqali aniqlanadi. Maxsus belgilar ketma-ketligi esa gamma deb nomlanadi, shu bois additiv usullar ko‘pincha gammalashtirish deb yuritiladi va gamma bevosita kalit sifatida qabul qilinadi. Additiv usullarning kriptobardoshligi kalitning uzunligi va statistik parametrlari bilan aniqlanadi. Agarda kalit uzunligi ochiq matn uzunligidan kichik bo‘lsa, unda shifrmatnni statistik usullar orqali tahlil qilish mumkin bo‘ladi. Kalit uzunligi qancha katta bo‘lsa, unga nisbatan yushtiriladigan hujum shuncha samarasiz bo‘ladi. Agar kalit belgilari nodavriy va tasodifiy ketma-ketlik bo‘lsa, va kalit uzunligi ochiq matndan katta bo‘lsa, unda kalitni bilmasdan turib deshifrlash mumkin bo‘lmaydi.

Additiv usullarida ochiq matn va gamma belgilari alifbodagi tartib raqami bilan almashtiriladi va shifrlash quyidagi formula bo‘yicha amalga oshiriladi:

$$C_i = (T_i + G_i) \pmod{N}.$$

Bu yerda,  $N$  alifbodagi belgilar soni,  $C_i$  (- shifrmatn),  $T_i$  (- ochiq matn) va  $G_i$  (- gamma) - bu  $i$ -belgining tartib raqami.

Deshifrlash jarayoni esa quyidagi formula bo‘yicha bajariladi:

$$T_i = (C_i \cdot G_i + N) \pmod{N}.$$

Amaliyotda asosan aralash usullardan foydalaniladi, masalan, 1) o‘rniga qo‘yish + gammalashtirish; 2) o‘rin almashtirish + gammalashtirish; 3) gammalashtirish + gammalashtirish; 4) o‘rniga qo‘yish + o‘rin almashtirish.

### 3.6.1.Gammalashtirish usuli

**Gammalashtirish** (ingl. gamma xoring) – ochiq matnga gamma nomli ketma-ketligini qo‘sish amali bilan bajariladigan shifrlash usuli hisoblanadi. Ushbu usul simmetrik shifrlash usuli bo‘lib, gamma bevosita tasodifiy sonlardan tashkil topishi kerak. Gammalashtirish usuli jadvalli yoki modulli bo‘ladi. Jadvalli gammalashtirish usulida  $A = \{a_1, \dots, a_n\}$  alifbo to‘plamidan asoslangan istalgan tartibda tashkil topgan lotin kvadrati nomli  $L$  jadvali gamma natijasi bo‘lib xizmat qiladi. Ochiq matnning  $a_i$  harfi bevosita gammaning ( $G$ )  $a_j$  belgisi orqali shifrlangan matnning  $a_k$  harfiga almashtiriladi.

	$T_0$	$\rightarrow$	$a_i$	
$G$	1	2	3	4 5
$\downarrow$	1			$\downarrow$
	2			
$a_j$	3	$\rightarrow$	$a_k$	
	4			
	5			$L$

1-rasm. Gammalashtirish jadvali

1-rasmida keltirilgan variantda alifbo  $A = \{a_1, \dots, a_5\}$  to‘plami 5 ta belgidan iborat. Bu yerda ochiq matnning ( $T_0$ ) navbatdagi belgisi  $a_i$ , masalan,  $A$  to‘plamining 3-elementi bo‘lsa, unda  $G$  gammaning 3-elementi  $a_i$  bilan qandaydir (\*) amal bajariladi, ya’ni

$$a_k = a_i * a_j.$$

Amaliyotada asosan gammalashtirishning modulli usuli qo‘llaniladi. Umumiy holda  $(\text{mod } n)$  yoki kompyutering mantiqiy asosiga moslashtirilgan xususiy  $(\text{mod } 2)$  varianti (Vernam usuli) qo‘llaniladi.

Modulli hisoblash 1888-yilda taklif etilgan bo‘lib, unda ochiq matn va kalit harflari sonlar bilan almashtirilganda quyidagi formulalar o‘rinli bo‘ladi:

$$C_i = (T_i + G_i) \pmod{N}. \quad (1)$$

bu yerda  $T_i$  - ochiq matnning  $i$ -belgisi,  $C_i$  – shifrmatnning  $i$ -belgisi,  $N$  – alifbodagi belgilar soni,  $G_i$  – gammaning  $i$ -belgisi.

Deshifrlash jarayoni esa quyidagi formula bo‘yicha bajariladi:

$$T_i = (C_i - G_i + N) \pmod{N}. \quad (2)$$

Ushbu formulalar shifrlashning Vijiner usuliga olib keladi.

Yuqorida keltirilgan formulalarni aniq misolda lotin alifbosi ( $N=26$ ) uchun ko‘rib chiqamiz.

1-jadval

Lotin harflarini kodlash

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ochiq matn sifatida “kompyuter” so‘zini olamiz va unga uzunligi bo‘yicha mos keladigan “shifrlash” so‘zini qabul qilamiz va jarayonni jadvalda aks ettiramiz:

2-jadval

Shifrlash jarayoni

Harf	$T_i$ - ochiq matnning $i$ -belgisi	k	o	m	p	y	u	t	e	r
Kod		10	14	12	15	24	20	19	4	17
Harf	$G_i$ – gammaning $i$ -belgisi	s	h	i	f	r	l	a	s	h
Kod		18	7	8	5	17	11	0	18	7
Harf	$C_i$ – shifrmatnning $i$ -belgisi	2	21	20	20	15	5	19	22	24
Kod		c	v	u	u	p	f	a	w	y

$C_i$  – shifrmatnning  $i$ -belgisini hisoblab ko‘rsatamiz:  $C_1 = (10+18) \pmod{26} = 2$ ,  $C_2 = (14+7) \pmod{26} = 21$ ,  $C_3 = (12+8) \pmod{26} = 20$ ,  $C_4 = (15+5) \pmod{26} = 20$ ,  $C_5 = (24+17) \pmod{26} = 15$ ,  $C_6 = (20+11) \pmod{26} = 5$ ,  $C_7 = (19+0) \pmod{26} = 19$ ,  $C_8 = (4+18) \pmod{26} = 22$ ,  $C_9 = (17+7) \pmod{24} = 24$ .

Demak, shifrmatn: **cvuupfawy** (2 21 20 20 15 5 19 22 24).

Ushbu usulda gamma cheklangan yoki cheksiz bo‘lishi mumkin. Cheklangan gammada belgilar soni cheklangan bo‘lib, ochiq matnni shifrlashda

bitta gamma takroran qo'llaniladi. Cheksiz gammada belgilar tasodifiy sonlar generatori yordamida shakllantiriladi.

Gammani takroran qo'llash tavsiya etilmaydi. Masalan, “xor” operatori orqali  $Y$  gammasi orqali bajarilgan shifrlashda  $X_1$  va  $X_2$  ochiq matnlar uchun hosil qilingan  $Z_1$  va  $Z_2$  shifrmatnlar uchun quyidagilarga ega bo‘lamiz:

$$Z_1 = X_1 \oplus Y,$$

$$Z_2 = X_2 \oplus Y.$$

Aniqlangan shifrmatnlar yig‘indisi bevosita  $Y$  gammaga bog‘liq bo‘lmaydi, ya’ni

$$Z_1 \oplus Z_2 = (X_1 \oplus Y) \oplus (X_2 \oplus Y) = X_1 \oplus X_2.$$

Bu esa gammani bilmasdan turib ochiq matnni aniqlashga imkon yaratib beradi.

### **Topshiriq**

Berilgan ochiq matnni  $T_0$  bevosita 1-jadval va 1,2-formulalarga asoslanib gammalashtirish usuli orqali shifrlang va deshifrlang.

#### Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_0</math>)</b>	<b>Gamma</b>	<b>№</b>	<b>Shifrlanadigan so‘z (<math>T_0</math>)</b>	<b>Gamma</b>
1	sinflar	kabinet	12	axborot	joylash
2	avtomat	dasturi	13	virusni	formula
3	mashina	yuklash	14	xavfsiz	kabinet
4	markasi	yeterli	15	apparat	dasturi
5	satrlar	xavfsiz	16	texnika	yuklash
6	kitobda	kabinet	17	banklar	yeterli
7	xonalar	dasturi	18	menyusi	xavfsiz
8	asoslar	yuklash	19	telefon	joylash
9	sababli	yeterli	20	tugmali	formula
10	hujumni	xavfsiz	21	mavzuni	kabinet
11	bozorda	kabinet	22	raqamlı	dasturi

#### **3.6.2.Uitstonning “ikki kvadrat” usuli**

Shifrlashning Uitston usuli 1854-yilda ishlab chiqilgan va bigrammlarni shifrlashga asoslangan. Uitston usuli qariyb bir asr davomida harbiylar tomonidan qo’llanilib kelingan. Bu yerda kalit sifatida ikkita kvadrat jadval qabul qilingan.

Shu bois ushbu usulni “ikki kvadrat” usuli deb nomlashgan. Umumiy holda jadvallarni kvadrat shaklida bo‘lishi shart emas.

Uitston usuli bilan aniq misolda tanishib olamiz va buning uchun lotin alifbosini asos qilib olamiz. Kalit sifatida quyidagi 2 ta jadvalni shakllantiramiz:

M	.	H	X	E
A	I	K	‘	U
Y	V	R	D	
N	Q	C	Z	T
G	F	J	S	O
L	P	W	,	B

N		C	H	P
U	O	W	X	Y
F	G	D	.	J
Z	B	M	I	,
K	L	‘	A	R
E	Q	V	S	T

1-rasm. Lotin harflarining 2 ta jadvaldagi tasodifiy joylashuvi

Ushbu jadvallarda lotin harflari tasodifiy joylashgan bo‘ladi va hech bir harfning jadvallardagi o‘rinlari mos kelmasligi kerak (1-rasm). E’tibor bering, jadvallar harflardan tashqari o‘zbek tilida ko‘p uchraydigan belgilar bilan ham to‘ldirilgan.

Birinchi navbatda matn bigrammalarga taqsimlab chiqiladi. Bunda bo‘sh kataklar ham inobatga olinadi. Har bir bigramma alohida shifrlanadi. Bigrammaning birinchi harfini birinchi jadvaldan qidirib topamiz va ikkinchi harfini ikkinchi jadvaldan. Aniqlangan kataklardan foydalanib to‘g‘ri to‘rtburchak shakllantiramiz va bunda harflar qarama-qarshi burchaklarda bo‘lishi kerak. Qolgan ikki burchakdagi harflar shifrmattn bo‘ladi. Masalan, NO bigrammasi uchun natija AB bo‘ladi (2-rasm).

M	.	H	X	E
A	I	K	‘	U
Y	V	R	D	
N	Q	C	Z	T
G	F	J	S	O
L	P	W	,	B

N		C	H	P
U	O	W	X	Y
F	G	D	.	J
Z	B	M	I	,
K	L	‘	A	R
E	Q	V	S	T

2-rasm. NO bigrammasining shifrlanishi

Agar bigramma harflari bir qatorda joylashgan bo‘lsa, unda shifrmattn harflari ham shu qatordan olinadi (3-rasm). Masalan, OK bigrammasi uchun birinchi jadvaldan ikkinchi harfga mos keluvchi o‘rindagi harf tanlanadi, bu yerda

G. Ikkinchini jadvaldan birinchi harfga mos keluvchi o‘rindagi harf tanlanadi, bu yerda R. Natijada QR shifrlangan bigramma hosil qilindi.

M	.	H	X	E
A	I	K	‘	U
Y	V	R	D	
N	Q	C	Z	T
G	F	J	S	O
L	P	W	,	B

N		C	H	P
U	O	W	X	Y
F	G	D	.	J
Z	B	M	I	,
K	L	‘	A	R
E	Q	V	S	T

3-rasm. OK bigrammasining shifrlanishi

Misol sifatida KRIPTOTAHLIL matnni bigrammalarga taqsimlab chiqamiz:

KR IP TO TA HL IL

Oxirgi bigrammani bo‘sh katak bilan to‘ldirish mumkin. Yuqorida keltirilgan algoritm asosida har bir bigrammani shifrlaymiz va quyidagi natijaga erishamiz:

JY .Y UB OI J\_ FO

Taklif etilgan ikki kvadratli Uitston shifrlash usulining kriptobardoshligi yuqori hisoblanadi.

### Topshiriq

1-rasmida keltirilgan jadvallarga asoslanib matnni bigrammalarga taqsimlang va ularni ikki kvadratli Uitston usuli bilan shifrlang. Bunda bo‘sh kataklar ham inobatga olinsin.

### Variantlar

№	Shifrlanadigan so‘z	№	Shifrlanadigan so‘z
1	kompyuter virusi	17	maxfiy xabarlar
2	autentifikasiya	18	steganografiya
3	identifikasiya	19	superkompyuter
4	yashirin qurilma	20	kriptobardoshlik
5	himoyalanish asri	21	shifrlash usuli
6	xavfsiz axborot	22	himoya vositalari
7	algoritm haqida	23	shifrlangan matn
8	kriptotizim asosi	24	cloud computing
9	gamilton usullari	25	raqamli imzo usuli
10	analitik usullar	26	jadval elementi
11	tarmoq himoyasi	27	ikkilik tub sonlar

12	axborot himoyasi	28	almashtirish soni
13	shifrlash paroli	29	integral sxemalar
14	zamondoshlar	30	server kompyuter
15	rasmga tushirish	31	elektron pochta
16	himoyachi haqida	32	texnologiyalar

### 3.6.3. To‘rt kvadrat usuli

Ikki kvadrat usulining kengaytirilgan varianti sifatida to‘rt kvadrat usuli ishlab chiqilgan. Ushbu usulni aniq misolda ko‘rib chiqamiz va bunda lotin alifbosini asos qilib olamiz. Bu yerda kalit sifatida 4 ta jadval qabul qilingan. Umumiy holda jadvalni to‘g‘ri to‘rtburchak shakli uchun ko‘rib chiqamiz. Jadvalning kvadrat shaklida bo‘lishi bu xususiy hol hisoblanadi. 4 ta jadvalni quyidagi tartibda joylashtirish mumkin:

2		1	
3		4	

Jadvallarda qo‘llaniladigan alifbo va matn uchun zarur bo‘lgan belgilar bir xil bo‘lishi zarur. Belgilar alifbo deb yuritiladi. Bu yerda keltirilgan misollar uchun quyidagi variantni asos qilib olamiz:

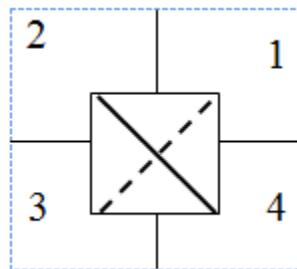
M	.	H	X	E	N	V	H	P	
‘	I	K	T	U	U	O	W	X	Y
V	R	D	W		L	G	D	.	J
S	Q	C	Z	A	Z	B	M	I	‘
G	F	J	N	O	K	F	‘	A	R
L	P	Y	‘	B	E	Q	C	S	T
C	A	P	Y	H	M	E	.	H	
Z	U		O	X	‘	A	I	U	K
D	F	J	G	.	X	Y	D	V	R
M	W	,	B	I	Z	N	Q	T	C
‘	K	R	L	N	S	G	F	O	J
V	E	T	Q	S	,	L	P	B	W

1-rasm. Lotin harflarining 4 ta jadvaldagagi tasodifiy joylashuvi

Yuqoridagi 1-rasmida keltirilgan jadvallarda lotin harflari tasodifiy joylashgan bo‘ladi va hech bir harfning jadvallardagi o‘rinlari mos kelmasligi

kerak. E'tibor bering, jadvallarda harflardan tashqari o'zbek tilida ko'p uchraydigan belgilar ham kiritilgan.

Birinchi navbatda matn bigrammalarga taqsimlab chiqiladi. Bunda bo'sh kataklar ham inobatga olinadi va uni matnda ostki chiziq bilan tasvirlaymiz. Har bir bigramma alohida shifrlanadi. Bigrammaning birinchi harfini ikkinchi jadvaldan qidirib topamiz va ikkinchi harfini to'rtinchi jadvaldan. Aniqlangan kataklardan foydalaniib to'g'ri to'rtburchakni shakllantiramiz va bunda harflar qarama-qarshi burchaklarda bo'ladi (chiziq bilan ko'rsatilgan). Qolgan ikki burchakdagi harflar shifrmatn bo'ladi (shtrix bilan ko'rsatilgan). Umumiyo'k ko'rinishda quyidagicha tasvirlash mumkin:



Masalan, NO bigrammasi uchun natija LA bo'ladi (2-rasm). E'tibor bering, bigramma belgilari to'g'ri to'rtburchakning diagonallarida joylashgan bo'ladi:

M . H X E	N V H P
' I K T U	U O W X Y
V R D W	L G D . J
S Q C Z A	Z B M I '
G F J N O	K F ' A R
L P Y , B	E Q C S T
C A P Y H	M E . H
Z U O X	' A I U K
D F J G .	X Y D V R
M W , B I	Z N Q T C
' K R L N	S G F O J
V E T Q S	, L P B W

2-rasm. NO bigrammasining shifrlanishi

Misol sifatida KRIPTOTAHLIL matnni bigrammalarga taqsimlab chiqamiz:

## KR IP TO TA HL IL

Agar oxirida bitta belgi qolsa, unda uni bo'sh katak bilan to'ldirish mumkin. Yuqorida keltirilgan algoritm asosida har bir bigrammani shifrlaymiz va quyidagi natijaga erishamiz (ostki chiziq bu bo'sh katak):

JY EW LX OO T\_ EO

Ushbu usulda kvadrat o'rniga har xil o'lchamli jadvalni qo'llanishi bevosita usulning kriptobardoshligini yanada oshiradi.

### Topshiriq

1-rasmda keltirilgan jadvallarga asoslanib matnni bigrammalarga taqsimlang va ularni To'rt kvadrat usuli bilan shifrlang (bo'sh katak ham inobatga olinsin).

Variantlar

<b>№</b>	<b>Shifrlanadigan so'z</b>	<b>№</b>	<b>Shifrlanadigan so'z</b>
1	kompyuter virus	17	maxfiyxabarlar
2	autentifikatsiya	18	steganografiya
3	identifikasiya	19	superkompyuter
4	yashirinqrilmalar	20	kriptobardoshlik
5	himoyalanish asri	21	shifrlash usuli
6	xavfsiz axborot	22	himoya vositalari
7	algoritmhaqida	23	shifrlanganmatni
8	kriptotizimasosi	24	cloud computing
9	gamilton usullari	25	raqamliimzo usuli
10	analitik usul	26	jadval elementi
11	tarmoqhimoyasi	27	ikkilik tub sonlar
12	axborot himoyachi	28	almashtirish soni
13	shifrlash parol	29	integral sxemalar
14	zamondoshlar	30	server kompyuterlar
15	rasmgatushir	31	elektron pochta
16	himoyachilar haqida	32	texnologiyalar

### 3.6.4.Xill usuli

Shifrlashning Xill usuli – bu poligramqli o'rniga qo'yish usuli bo'lib, chiziqli algebra va modul bo'yicha hisoblashga asoslangan va 1929-yilda matematik Xill tomonidan taklif etilgan. Ushbu usulda bir vaqtning o'zida ikki va undan ortiq belgilari bilan ishlash imkonii mavjud. Lekin katta o'lchovli matritsalar

uchun teskari matritsanı hisoblashdagi qiyinchiliklar usulning zaif tomoni hisoblanadi.

Bunda harflar, masalan faqatgina lotin harflari uchun, quyidagi jadval asosida raqamlanadi:

1-jadval

Harflarni sonlar bilan ifodalash

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Shifrlanadigan matn bir xil  $n$  uzunlikdagi bloklarga bo‘linadi va  $n \times n$  o‘lchamli kvadrat matritsaga  $m=26$  moduli bo‘yicha ko‘paytiriladi. Kvadrat matritsa Xill usulining kaliti hisoblanadi. Deshifrlashni bajarish uchun kalit matritsa teskari matritsaga ega bo‘lishi kerak. Xill usulida qo‘llaniladigan matritsa determinanti noldan farqli bo‘lishi kerak va determinant qiymati modul asosi bilan umumiyoq bo‘luvchiga ega bo‘lmasligi talab etiladi. Modul asosi  $m=26$  ga teng bo‘lishi ko‘p jihatdan noqulay bo‘lishi mumkin, shu bois, alifboni  $m=29$  gacha, ya’ni tub songacha kengaytirish maqsadga mufoviq bo‘ladi.

Misol uchun usulni  $n=2$  bo‘lganda ko‘rib chiqamiz. Eslatib o‘tamiz, umumiyoq holda kvadrat matritsa  $A$  teskarilanuvchi deb aytiladi, agar determinant  $D=\det A \neq 0$ , ya’ni  $A$  matritsa xosmas bo‘lsa. Masalan,  $2 \times 2$  o‘lchamli kvadrat matritsa uchun

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

agar  $D=ad-bc \neq 0$  bo‘lsa, unda teskari matritsa  $B = A^{-1}$  quyidagi ko‘rinishda bo‘ladi:

$$B = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$$

Endi, Xill usuliga qaytadigan bo‘lsak, unda bajariladigan amallar faqat  $(\text{mod } m)$  bo‘yicha bajariladi va matritsa uchun quyidagi cheklov kiritiladi, ya’ni  $\text{EKUB}(D, m) = 1$  bo‘lishi shart. Kalit so‘z sifatida quyidagi ketma-ketlikni

“CDHI” qabul qilamiz. Ushbu kalit so‘z asosida  $2 \times 2$  o‘lchamli kvadrat matritsani quydagicha shakllantiramiz (1-jadvalga binoan “CDHI” bu 2378 bo‘ladi):

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$$

Birinchi navbatda  $A$  matritsasining teskari matritsasini hisoblaymiz. Buning uchun determinantni hisoblaymiz:  $D = 2 \cdot 8 - 3 \cdot 7 = -5 \neq 0$ , demak teskari matritsa  $B = A^{-1}$  mavjud. Ammo.  $D$  ning qiymatini mod 26 bo‘yicha aniqlash talab etiladi, ya’ni

$$D \pmod{26} = -5 \pmod{26} = 21 \pmod{26}.$$

Bu yerda  $\text{EKUB}(21, 26) = 1$  bo‘lganligi sababli,  $21^{-1}$  mavjud bo‘ladi, ya’ni:  $21^{-1} = 5 \pmod{26}$ , chunki, bu yerdan  $1 = 5 \cdot 21 \pmod{26} = 105 \pmod{26}$ . Bu yerdan esa,  $1-105 = -104$  soni 26 ga qoldiqsiz bo‘linishi sababli  $21^{-1} = 5 \pmod{26}$  bo‘ladi. Endi teskari matritsani hisoblaymiz:

$$A^{-1} = \begin{pmatrix} 5 \cdot 8 & -5 \cdot 3 \\ -5 \cdot 7 & 5 \cdot 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix}$$

Endi teskari matritsani mod 26 bo‘yicha qayta hisoblaymiz:

$$A^{-1} \pmod{26} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \pmod{26} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}$$

Natijaviy  $A^{-1}$  matritsani teskari ekanligini tekshirib olamiz:

$$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 14 \cdot 2 + 11 \cdot 7 & 14 \cdot 3 + 11 \cdot 8 \\ 17 \cdot 2 + 10 \cdot 7 & 17 \cdot 3 + 10 \cdot 8 \end{pmatrix} = \begin{pmatrix} 105 & 130 \\ 104 & 131 \end{pmatrix} \pmod{26} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Endi  $A$  matritsadan foydalanib ochiq matnni shifrlashni bajaramiz. Buning uchun ochiq matnni, masalan, “TAHLIL” so‘zini  $x_i$  ( $i=1,..,3$ ) bigrammalarga bo‘laklab chiqamiz, ya’ni: TA HL IL.

Endi har bir bigrammaga uning sonli qiymatini yuqorida keltirilgan 1-jadval asosida taqsimlab olamiz: TA = 19 0; HL = 7 11; IL = 8 11. Bu yerdan  $x_i$  ( $i=1,..,3$ ) larni quyidagicha aniqlaymiz:

$$x_1 = \begin{pmatrix} 19 \\ 0 \end{pmatrix}; x_2 = \begin{pmatrix} 7 \\ 11 \end{pmatrix}; x_3 = \begin{pmatrix} 8 \\ 11 \end{pmatrix}.$$

Keltirilgan ochiq  $x_i$  bigrammalarni shifrmatnga almashtirish quyidagi formula bo'yicha amalga oshiriladi:

$$y_i = A \cdot x_i \pmod{26} \quad yoki \quad y_i = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \cdot x_i \pmod{26}.$$

Bu yerdan  $y_i$  lar quyidagicha aniqlanadi:

$$y_1 = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 0 \end{pmatrix} = \begin{pmatrix} 38 \\ 133 \end{pmatrix} \pmod{26} = \begin{pmatrix} 12 \\ 3 \end{pmatrix}.$$

$$y_2 = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 11 \end{pmatrix} = \begin{pmatrix} 47 \\ 137 \end{pmatrix} \pmod{26} = \begin{pmatrix} 21 \\ 7 \end{pmatrix}.$$

$$y_3 = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 11 \end{pmatrix} = \begin{pmatrix} 49 \\ 144 \end{pmatrix} \pmod{26} = \begin{pmatrix} 23 \\ 14 \end{pmatrix}.$$

Ushbu natijalarni 1-jadvalga asoslanib shifrmatn bigrammalariga aylantiramiz: MD VH XO.

Endi shifrmatnni ochiq matnga aylantiramiz. Keltirilgan  $y_i$  bigrammalarni ochiq matnga almashtirish quyidagi formula bo'yicha amalga oshiriladi:

$$x_i = A^{-1} \cdot y_i \pmod{26} \quad yoki \quad x_i = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot y_i \pmod{26}.$$

Bu yerdan  $x_i$  lar quyidagicha aniqlanadi:

$$x_1 = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 3 \end{pmatrix} = \begin{pmatrix} 201 \\ 234 \end{pmatrix} \pmod{26} = \begin{pmatrix} 19 \\ 0 \end{pmatrix}.$$

$$x_2 = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} 21 \\ 7 \end{pmatrix} = \begin{pmatrix} 371 \\ 427 \end{pmatrix} \pmod{26} = \begin{pmatrix} 7 \\ 11 \end{pmatrix}.$$

$$x_3 = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 14 \end{pmatrix} = \begin{pmatrix} 476 \\ 531 \end{pmatrix} \pmod{26} = \begin{pmatrix} 8 \\ 11 \end{pmatrix}.$$

E'tibor bering,  $x_i$  qiymatlari tiklanildi, ammo umumiy holda Xill usulining kriptobardoshligi zaif bo'ladi.

### Topshiriq

1-jadvalga asoslanib matnni bigrammalarga taqsimlang va ularni "CDHI" kalit so'ziga asoslanib Xill usuli bilan shifrlang.

Variantlar

<b>№</b>	<b>Shifrlanadigan so‘z</b>	<b>№</b>	<b>Shifrlanadigan so‘z</b>
1	kompyuterlar	16	maxfiy
2	algoritm	17	steganografiya
3	identifikasiya	18	superkompyuter
4	qurilmalar	19	kriptobardoshlik
5	himoyalanish	20	monoalifbo
6	xavfsizlik	21	simmetriyali
7	samarali	22	shifrlanganlik
8	kriptotizimlar	23	matritsa
9	gamilton	24	nosimmetriya
10	analitik	25	polialifbo
11	tarmoq	26	sxemalar
12	axborotlar	27	almashtirish
13	shifrlashlar	28	integral
14	tovush	29	serverning
15	himoyachilar	30	elektron

## **4-bob. KODLASHGA DOIR ODDIY MISOLLAR**

Ushbu bobda axborot nazariyasida o‘rin egallagan kodlash usullari haqida mavjud algoritmlar va ulardan foydalanishga doir misollar ko‘rib chiqilgan. Keltirilgan algoritm doirasida axborot hajmini qariyb 50 foizga kamaytirishga erishilganligi keltirilgan. Ma’lumotlarni kodlash usullari keng qo‘llaniladi, masalan, raqamlashtirilgan audio yozuvlarda. Keltirilgan misollarni o‘rganib chiqish orqali talabalarimiz kodlashga doir murakkab masalalarni o‘rganib olish imkoniga ega bo‘lishadilar. Bu yerda keltirilgan Xaffman usuli esa hozirgi kunda ham o‘z dolzarbligini yo‘qotmagan bo‘lib, ilmiy izlanishlarda ham o‘rin egallab kelmoqda. Keltirilgan usullar kelgusida yanada mukammal usullar yaratilishiga olib kelishiga umid qilamiz.

### **4.1. Kodlashga doir usullar**

Kodlash bilan bog‘liq bo‘lgan misollardan birini ko‘rib chiqamiz. Berilgan quyidagi natural sonlarni sonli faylda saqlash talab etiladi. Bu yerda har bir songa ikki bayt ajratilgan bo‘lsin:

1020 1012 1013 1013 1013 1008 1010 1020 1032 1050 1036 ...

Ushbu sonlarga nazar tashlaydigan bo‘lsak, ular bir-biridan katta farq qilmasligini kuzatish mumkin. Ya’ni, bu yerda farq 128 dan oshmaydi. Demak, faylda barcha sonlarni saqlash shart emas, faqatgina ularning farqini yozib qo‘yish kifoya bo‘ladi. Faqat bunda birinchi elementni belgilab olish kerak bo‘ladi. Agar bizda bu 1000 bo‘ladigan bo‘lsa, unda quyidagi natijani olamiz:

1000 +20 -8 +1 0 0 -5 +2 +10 +12 +18 -14 ...

Shunday qilib, oddiygina algoritm orqali sonlarni kodlab oldik va natijada faylning hajmini qariyb 50 foizga kamaytirdik.

Ma'lumotlarni bunday kodlash usuli keng qo'llaniladi, masalan, raqamlashtirilgan audio yozuvlarda.

Keyingi kodlash usullaridan biri bu RLE (Repeated Running Length Encoding, yoki qisqacharoq – Run Length Encoding deb yuritiladi). Bunda asosiy maqsad takrorlanuvchi belgilarni ixchamlash hisoblanadi. Masalan, matn bevosita bir baytli belgilardan iborat bo'lsin:

```
ABBCCCDDDDDEEEEEE ...
```

Bunda RLE usuli natijasi quyidagicha bo'ladi:

```
1A2B3C4D5E ...
```

Umumiy holda bu yerda siqilish koyeffitsiyentini oshirish faqatgina maxsus fayllarda amalga oshirilishi mumkin.

#### 4.2. Xaffman usuli

ASCII jadvalida keltirilgan asosiy matn belgilaridan tashkil topgan  $M$  to'plamidagi belgilarni ikkilik ko'rinishiga optimal kodlash talab etiladi. Bunda optimallikga erishish uchun  $M$  to'plamidagi har bir belgini maxsus algoritm orqali nol va birlar bilan kodlash zarur bo'ladi.  $M$  to'plamiga mos kelmagan belgilarni kodlash va natijaviy fayldan joylashtirish talab etilmaydi. Kodlangan natijadan birlamchi matn dekodlash orqali aniq bo'lishi kerak. Optimallik esa bu yerda kodlangan natijada nol va birlarning umumiy soni minimal bo'lishi kerakligini anglatadi. Bu yerda optimal algoritm quyidagi tamoyil asosida quriladi: ko'p uchraydigan belgilar kichik uzunlikdagi kod orqali belgilanishi shart. Buning uchun quyidagi qadamlar bajariladi:

1. Matnda uchraydigan barcha belgilar ro'yxatini shakllantiramiz va unda har bir belgi nechta borligini yozamiz.
2. Hosil qilingan ro'yxatdan ikkita eng kam uchraydigan belgilarni tanlab olamiz. Ularning yig'indisi ro'yxatga qo'shiladi va birlamchi ro'yxatdan o'chiriladi.
3. Ro'yxatda ikkita son qolguncha 2-band davom ettiriladi.
4. Ro'yxatda qolgan birinchi songa 0 beramiz va ikkinchisiga esa 1.

5. Bu yerda orqaga qaytish jarayonini boshlaymiz, ya’ni yig‘indini ajratib va ro‘yxatga elementni qo‘shib boramiz. Bunda, agar biz ajratadigan sonimiz  $X=a_1a_2..a_m$  ( $a_i= 0$  yoki  $1$ ) bo‘lsa, unda ajratib olingan birinchi songa nol qo‘shilgan  $X_0$  va ikkinchi songa esa bir qo‘shilgan  $X_1$  to‘g‘ri kelishi kerak.

6. Oxirgi 5-bandni barcha yig‘indilarni ajratib olguncha davom ettiramiz. Natijada ketma-ketlikdagi belgilar uchun ularning ikkilik ko‘rinishidagi kodlari shakllanadi.

Endi Xaffman (ingl. Huffman) algoritmini murakkab misolda ko‘rib chiqamiz. Bu yerda, birinchi navbatda, fayldagi ma’lumotlar to‘liq o‘qib olinadi. Faylni siqish uchun undagi har bir belgi necha marta takrorlanishini hisoblab chiqish talab etiladi. Shu bois ushbu algoritm orqali oddiy matnli va EXE fayllarni siqish bir xil amalga oshiriladi.

Har bir belgining chastotasini aniqlab, ularni kamayish tartibi bilan joylashtiramiz. Aniq qadamlarni bajarishni quyidagi misolda ko‘rib chiqamiz. Tarixiy manbalarda keltirilishicha, buyuk Amir Temurning uzukida forscha “rosti-rusti” degan so‘zlar bitilgan ekan. Keling, shu so‘zlarni kodlaymiz. Demak, bizga 11 baytdan iborat matn ROSTI-RUSTI berilgan va unda jami bo‘lib 7 ta har xil belgilar mavjud. Belgilarning chastotasini hisoblab, quyidagi jadvalni shakllantiramiz:

Belgi	R	U	S	T	I	O	-
Chastotasi	2	1	2	2	2	1	1

Bu yerdan eng kichik chastotalarni o‘ng tomonda yig‘ib quyidagi jadvalni hosil qilamiz:

Belgi	R	I	S	T	U	O	-
Chastotasi	2	2	2	2	1	1	1

Ushbu jadvaldan eng kichik chastotali ikkita belgini tanlaymiz, masalan, ‘O’ (1) va ‘-’ (1) bo‘lsin. Ularning chastotalarini yig‘indisini olamiz:

Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$

Ikkita belgini birlashtirish natijasida hosil bo‘lgan yangi belgining chastotasi  $1+1=2$  bo‘ldi (albatta, bu son chastotani anglatmaydi, ammo mazmunan chastota deb yuritsak xato bo‘lmaydi). Keyingi qadamda ‘O’ va ‘-‘ belgilari inobatga olinmaydi, faqatgina ularning yig‘indisi jarayonda ishtirok etadi.

Keyingi qadamda jadvaldan yana eng kichik chastotali ikkita belgini tanlaymiz, masalan, ‘U’ va ‘O-‘ bo‘lsin. Ularning chastotalarini yig‘indisini olamiz:

Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$
							$3=1+2$

Yuqoridagi jarayonni takrorlaymiz, ya’ni jadvaldan eng kichik chastotali ikkita belgini tanlaymiz, masalan, ‘R’ va ‘I’ bo‘lsin. Ularning chastotalarini yig‘indisini olamiz:

Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$
							$3=1+2$
		$4=2+2$					

Yuqoridagi jarayonni takrorlaymiz, ya’ni jadvaldan eng kichik chastotali ikkita belgini tanlaymiz, bunda faqatgina ‘S’ va ‘T’ bo‘lishi mumkin. Ularning chastotalarini yig‘indisini olamiz:

Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$
							$3=1+2$
		$4=2+2$					
			$4=2+2$				

Yuqoridagi jarayonni takrorlaymiz, ya’ni jadvaldan eng kichik chastotali ikkita belgini tanlaymiz, bunda faqatgina ‘ST’ va ‘UO-‘ bo‘lishi mumkin. Ularning chastotalarini yig‘indisini olamiz:

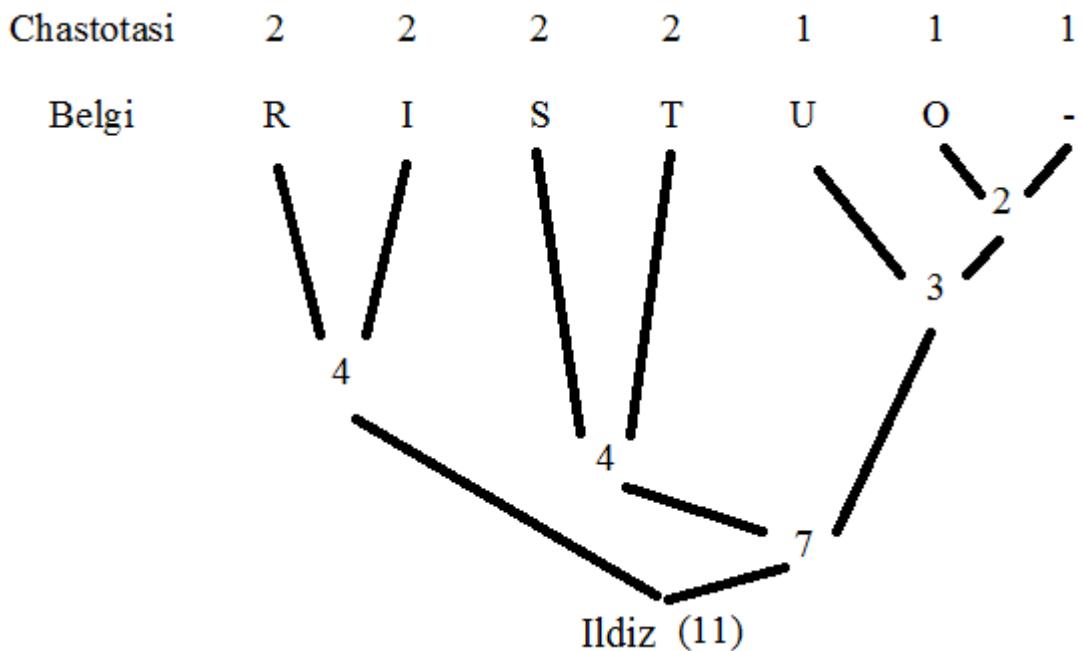
Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$
							$3=1+2$
	$4=2+2$						
			$4=2+2$				
							$7=4+3$

Hosil bo‘lgan jadvalda eng kichik chastotali faqatgina ikkita belgi mavjud, bular ‘RI’ va ‘STUO-‘ bo‘ladi. Ularning chastotalarini yig‘indisini olamiz:

Chastotasi	2	2	2	2	1	1	1
Belgi	R	I	S	T	U	O	-
							$2=1+1$
							$3=1+2$
	$4=2+2$						
			$4=2+2$				
							$7=4+3$
							Ildiz (11)

Endi jarayonni yaxshiroq tasavvur qilish uchun oxirgi jadvalni daraxt shaklida namoyon qilamiz (1-rasm).

Daraxt yaratildi va uning eng oxirgi nuqtasini **Ildiz** deb belgiladik. Daraxtning R nuqtasiga (yoki barg deb yuritiladi) o‘tish uchun biz ‘chap’ yoki ‘o‘ng’ tomonlarga burilishim kerak bo‘ladi. Agar ‘chap’ tomonga burilish bajarilsa, unda 0 bitni yozamiz. Agar ‘o‘ng’ tomonga burilish bajarilsa, unda 1 bitni yozamiz. Demak, R bargiga o‘tish uchun **Ildiz** nuqtasidan ‘chap’ tomonga o‘tamiz, ya’ni (4) nuqtasiga va 0 bitni yozamiz, undan yana ‘chap’ tomonga o‘tamiz va yana 0 bitni yozamiz. Demak, R belgisining Xaffman kodi 00 bo‘ladi. Keyingi I belgisi uchun ‘chap’ dan ‘o‘ng’ ga o‘tamiz. Demak, I belgisining Xaffman kodi 01 bo‘ladi.



1-rasm. Daraxt shakli

Shu algoritm orqali barcha belgilarning aniqlangan Xaffman kodlari va ularga ajratilgan bitlar soni quyidagi jadvalda jamlangan:

Belgi	R	I	S	T	U	O	-
Kod	00	01	100	101	110	1110	1111
Bitlar soni	2	2	3	3	3	4	4

Shunday qilib, natijaviy jadval orqali ROSTI-RUSTI matni quyidagi Xaffman kodiga aylantiriladi:

R	O	S	T	I	-	R	U	S	T	I
00	1110	100	101	01	1111	00	110	100	101	01
<b>0011101001010111110011010010101</b>										

Ilovada keltirilgan dasturdan olingan natijada Xaffman kodlari jadvalda keltirilgan natijadan ozgina farq qiladi. Bu farq harflarni tartiblab yozishdagi farqdan yuzaga keladi, ya’ni

Belgi	-	I	O	R	S	T	U
Kod	010	101	011	110	111	00	100
Bitlar soni	3	3	3	3	3	2	3

Bu jadval orqali ham ROSTI-RUSTI matni quyidagi Xaffman kodiga aylantiriladi: 110011110010101011010011100101. E'tibor bering, ikkala variantda natijaviy kodlarning uzunligi o'zgarmas qoldi. Ya'ni, jami bo'lib 31 ta bit orqali matn kodlandi, demak siqilish koyeffitsiyenti 2,8 bo'ladi ( $=11*8/31=2,8$ ).

Hosil qilingan koddan asl matnni tiklash uchun oxirgi keltirilgan jadvaldan foydalananamiz. E'tibor bering, har bir matn uchun ushbu jadval har xil shakllanishi mumkin, shu bois, arxivlash va dearxivlash masalalari uchun universal jadvalga ega bo'lish kerak bo'ladi.

Endi masalani murakkablashtirib, kattaroq matnni misol sifatida ko'rib chiqamiz:

### **SAMARQAND SAYQALI RO'YI ZAMIN AST**

Belgi	S	A	M	R	Q	N	D	Y	L	I	Z	T	O	'	space
Chastotasi	3	7	2	2	2	2	1	2	1	3	1	1	1	1	4

Matndagi belgilarni quyida keltirilgan dastur asosida olingan natijalari asosida quyidagicha kodlash mumkin bo'ladi:

Belgi	Chastotasi	Bitlar
A	7	00
Space	4	010
I	3	1110
S	3	1111
M	2	0110
N	2	0111
Q	2	1000
R	2	1001
Y	2	1010
D	1	10110
L	1	10111
O	1	11000
T	1	11001
Z	1	11010
'	1	11011

Ushbu algoritmni dasturini tuzishda kirish faylida bosh harflarda matn beriladi va chiqishda matnning bitlardagi hajmi, kodlangan variantidagi hajmi va siqilish koyeffitsiyenti verguldan keyin bitta raqam aniqlikda chiqariladi. Dasturning to‘liq matni ilovada keltirilgan. Olingan natijalarga ko‘ra bunda siqilish koyeffitsiyenti 1 ga 2,2 ga ( $=33*8/120 = 2,2$ ) teng bo‘ladi. Ya’ni koddagi bir bit axborot matnning 2,2 bitli axborotiga teng bo‘ladi.

### Topshiriqlar

1. Alifbo harflari chastotasi Fibonachchi sonlariga mos keladi, ya’ni  
 $a : 1 \quad b : 1 \quad c : 2 \quad d : 3 \quad e : 5 \quad f : 8 \quad g : 13 \quad h : 21$ .

Ushbu harflarning Xaffman kodlarini aniqlang.

2. Bahouddin Naqshbandning bosh g‘oyasi bo‘lmish “Dil-ba yor-u, dast-ba kor” matnni Xaffman kodlari bilan belgilang.

3. Bitlardan tashkil topgan  $a_1, a_2, \dots, a_n$  ketma-ketligi quyidagicha kodlanadi:  
 $b_1=a_1$  va

$$b_i = \begin{cases} 1, & \text{agar } a_i = a_{i-1} \text{ bo‘lganda,} \\ & \\ 1, & \text{agar } a_i \neq a_{i-1} \text{ bo‘lganda} \end{cases}$$

barcha  $i=2, \dots, n$  uchun. Ushbu algoritmga asoslangan kodlash dasturini tuzing.

4. Yuqoridagi misolda olingan kodli bitlar ketma-ketligini tiklaydigan dekodlash dasturini tuzing.

5. Xatoliklarni tuzatish. Berilgan bitlar ketma-ketligini uzatishda har bir bit uch marta uzatiladi. Masalan, 1,0,1 kodlari quyidagicha uzatiladi: 1,1,1,0,0,0,1,1,1. Agar uchtalikda qaysi bit ikki marta takrorlansa, o‘sha bit natija sifatida qabul qilinadi. Ya’ni yuqoridagi misolda qabul qilingan bitlar quyidagicha buzilgan bo‘lsada: 1,1,1,0,1,0,1,1,1 natija baribir 1,0,1 bo‘ladi.

Ushbu algoritmga asoslangan dekodlash dasturini tuzing.

## **5-bob. AMALIY MASHG‘ULOTLAR UCHUN KO‘RSATMALAR**

Ushbu bobda “Kriptografiya 1” fani bo‘yicha amaliy mashg‘ulotlarni o‘tkazish bo‘yicha to‘liq va batafsil tavsiyalar berilgan. Keltirilgan beshta mavzu doirasida topshiriqlar soni bir-biridan farq qiladi. Mavzuni to‘liq tushunib olish uchun barcha mavzularda jarayonlar qadamba-qadam yoritib berilgan. Talabalardan barcha jarayonlarni mustaqil bajarishlari talab etiladi. Keltirilgan mavzular juda murakkab bo‘lganligi sababli, ba’zida qisqartirilgan algoritmlar ham bayon etilgan.

### **5.1. N bitli skremblerni qurish va takrorlanish davrini hisoblash**

Hisoblash texnikasi va axborot texnologiyalarini keskin rivojlanishi bevosita kompyuterda mavjud axborotlarni himoyalash tizimini murakkablashtirishga olib kelmoqda. Dunyoda sodir bo‘layotgan moliyaviy inqirozlar mavjud raqobatni keskinlashishiga olib kelmoqda. Bu esa, o‘z navbatida, korxonalarda axborot xavfsizligi siyosatini birinchi darajali jarayonga ko‘tarmoqda.

Skremblerlashning mazmuni bevosita axborot tizimidan o‘tayotgan ma’lumotlar oqimining har bir bitini o‘zgartirishga qaratilgan. Ammo oxirgi paytlarda skremblerlash algoritmlari e’tiborsiz qolmoqda. Chunki, hozirgi kunda asosan ma’lumotlar paketlarda uzatiladi va ular uchun blokli shifrlash algoritmlari qo‘llaniladi. Ushbu algoritmlarning kriptobardoshligi skremblerlash usulidan yuqori hisoblanadi. Ammo skremblerlash usulining oddiyligi uning asosiy yutug‘i bo‘lib, amaliy jihatdan uni o‘rganish foydadan xoli emas.

#### **1. Bir martali shifrlash usuli**

1926 yilda Amerika telefon va telegraf kompaniyalaridan birining muhandisi Vernam o‘zining ikkilik sanoq sistemasi asosida yaratgan shifrlash algoritmini e’lon qildi. Vernamning shifrlash algoritmi Sezarning shifrlash algoritmiga o‘xhash bo‘lib, u quyidagi

$$y=x \oplus z, \quad (1)$$

formula bilan ifodalanadi va bunda x, y, z o‘zgaruvchilar ikkilik sanoq sistemasi alifbosida qiymatlar qabul qiladi,  $\oplus$  belgisi esa 2 moduli bo‘yicha qo‘sish amalini bildiradi. Bu algoritmning mohiyati deshiflash kalitining faqat bir marta ishlatilishiga asoslangan bo‘lib, bunda shifrlash har safar yangi tasodifiy bitlardan iborat kalit bilan amalga oshiriladi. Bunday shifrlash uslubidan ko‘rinib turibdiki, shifrlash va deshifrlash uchun ochiq matn uzunligi bilan teng bo‘lgan bitta kalitdan foydalaniladi, hamda bu kalitning foydalanuvchiga muhofazalangan aloqa kanali orqali uzatilishi talab etiladi. Bundan tashqari, shu usul bilan shifrlangan matnni deshifrlash imkoniyati murakkab bo‘lib, bu uning muallifi Vernam tomonidan ham e’tirof etilgan bo‘lsada, isboti keltirilmagan. K.E. Shennonning 1949 yilda chop etilgan «Maxfiy tizimlarda aloqa nazariyasi» deb nomlangan ilmiy maqolasi ilmiy asoslangan maxfiy kalitli kriptografiya davrini boshlab berdi. Shennon o‘zining elektrotexnika va matematikaga oid bilimlaridan kelib chiqib, maxfiy aloqa tizimi nazariyasining asosini 1948-yilda e’lon qilgan. Shennon o‘zining bu ilmiy maqolalarida Vernam uslubida shifrlashning ishonchliligi darajasiga to‘xtalib, deshifrlash maksimal murakkablikka egaligini, hamda shu uslubda shifrlashdan foydalanuvchiga maxfiy aloqa kanali orqali uzatiladigan maxfiy kalit hajmi (uzunligi) uchun aniq quyi chegaraning qanday bo‘lishini ilmiy asosda isbotlab berdi Shennonning 1948-yilda e’lon qilingan ilmiy maqolasi kriptologiya sohasidagi ilmiy maqlolarning paydo bo‘lishiga olib keldi.

Shifrlash jaryonida ochiq ma’lumot alifbosi belgilari yoki alifbo belgilari birikmalari biror amal bajarish bilan shifrmalumot alifbosi belgilari yoki ularning birikmalariga almashtirilsa, bunday shifrlash algoritmi gammalashtirilgan shifrlash sinfiga kiradi. Demak, gamma ketma-ketlikni tashkil etuvchi alifbo belgilarini ochiq ma’lumot mos alifbo belgilari bilan biror amal bajarish orqali shifrmalumot alifbo belgilariga almashtirish – gammalashtirish orqali amalga oshiriladi.

Gammalash - ochiq ma’lumotlarga ma’lum qonuniyat bo‘yicha gamma shifrini singdirish orqali yopiq ma’lumotlarni olish jarayoni. Bundan bir martali

“bloknot” tushunchasi yuzaga kelgan va ushbu algoritm bevosita Vernam nomi bilan bog‘liq.

So‘zsiz bardoshli kriptoalgoritm larning xavfsizligi kalitni ochish mumkin emasligini isbotlovchi teorema larga asoslanadi. Masalan, Vernam shifri (bir marta foydalaniladigan kalitli) so‘zsiz bardoshlidir. Xattoki, shifrmatnni bir qismini deshifrlashga erishilgan taqdirda ham to‘liq shifrmatnni ochish imkonim mavjud emas.

Bir martali kalit muammosini yechish maqsadida skremblerlash usuli ishlab chiqilgan.

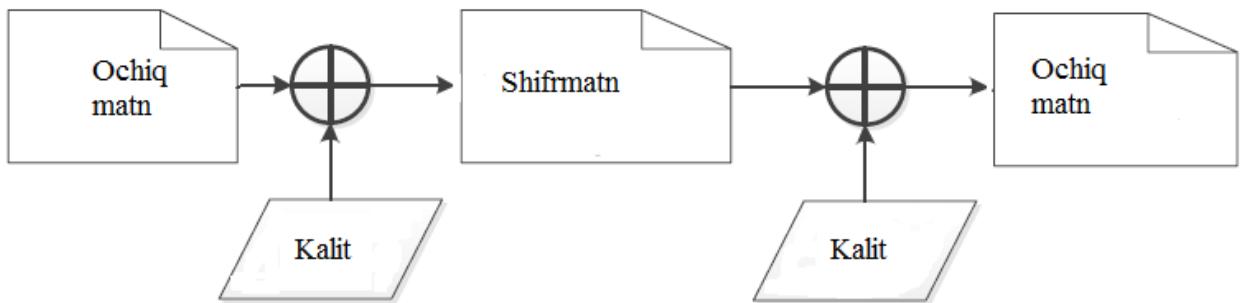
## 2. Skremblerlash algoritmini amaliy qo‘llash asoslari

**Skremblerlash** jarayoni (ingl. scramble - aralashtirish) – bu teskarilash xossasiga ega bo‘lgan jarayon bo‘lib, raqamli oqimda tasodifiylik xossasiga yaqin bo‘lgan bitlar ketma-ketligini shakllantirishga qaratilgan. Bunda raqamli oqim bilan ishslash tezligi o‘zgarmaydi. Eng muhimi, boshlang‘ich matnni tiklash uchun algoritm teskari qo‘llaniladi.

Skremblerlash jarayoni bevosita ma’lumotlar oqimidagi har bir bitni o‘zgartirishga yo‘naltirilgan. Bunda amaliyotda asosan XOR (formulalarda asosan  $\oplus$  deb belgilanadi) amali qo‘llaniladi. Ikki bit uchun Xor natijasi quyidagi jadvalda keltirilgan:

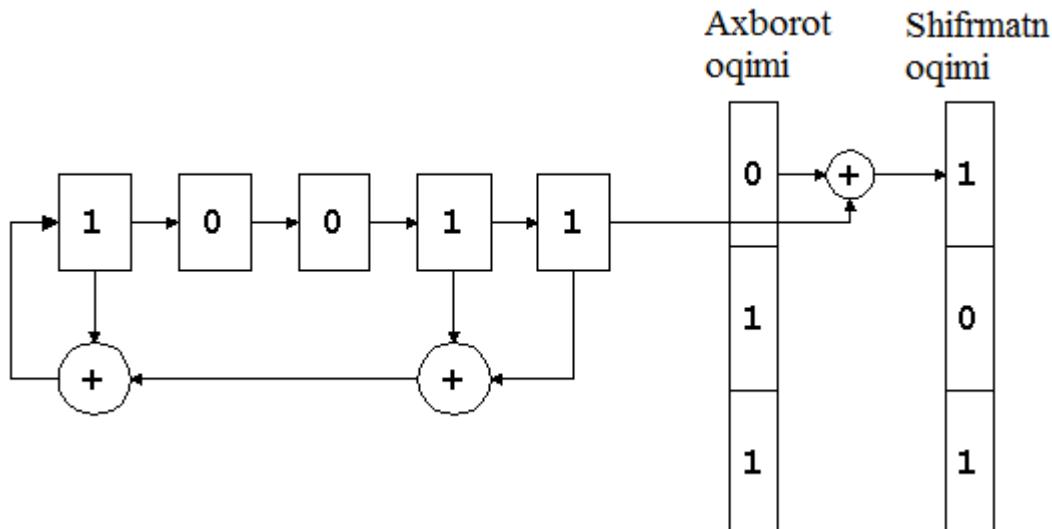
1-bit	2-bit	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

Skremblerlash jarayoni simmetrik algoritm bo‘lib, XOR amalining mohiyatidan kelib chiqadi, chunki Xor amalini 2 marta qo‘llash boshlang‘ich qiymatni qaytaradi. Ushbu jarayon 1-rasmida keltirilgan:



1-rasm. Bir martali gammalash sxemasi

Skrembler bevosita axborot oqimi bilan birgalikda parallel ravishda amalga oshiriladi. Natijada shifrmavn hosil qilinadi. Bunda to‘g‘ri va teskari jarayonlarda **Xor** amali qo‘llaniladi. Hosil qilinadigan bitlar takrorlanuvchi jarayon bo‘lib, bunda boshlang‘ich kalitdagi bitlar skremblerda berilgan sxema bo‘yicha **Xor** amali bilan qo‘shilib boriladi. Kalitdagi bitlar o‘ngga bir xonaga siljtiladi, olingan natijaviy bit esa chap tomondan qo‘shiladi. O‘ng tomondagi bit axborot oqimidagi bitga qo‘shiladi va shifrmavn tashkil etildi (2-rasm).



2-rasm. Skrembler sxemasi va shifrlash jarayoni

Skremblerning bunday oddiyligi natijasida uning elektron sxemalarda ham qo‘llash imkonini beradi. Boshlang‘ich matnni tiklash ham aynan shu usulda amalga oshiriladi.

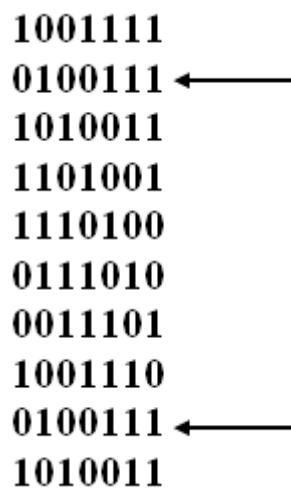
Kodlash bitlarini shakllantiradigan qurilmasidagi bitlar soni skremblerning razryadi deb ataladi. Yuqoridagi 2-rasmida keltirilgan skremblerning razryadi 5 ga

teng. Razryad qiymatini kattalashtirish bevosita kriptomustahkamlikni belgilab beradi.

Bu yerda e'tiborli jihat shundaki, skrembler kodlari ma'lum bir qadamdan so'ng takrorlanishni boshlaydi. Bu muammo bevosita bitlar soni bilan bog'liq, shu bois ushbu kamchilikni tuzatib bo'lmaydi. Haqiqatan, bitlar soni  $N$  bo'lsa, unda kombinatsiyalar soni  $2^N$  bo'ladi, demak ko'pi bilan  $2^N-1$  –qadamdan so'ng takrorlanish sodir bo'ladi. Bu yerda nollardan tashkil topgan kombinatsiya minus qilingan.

Skrembler orqali tashkil etiladigan bitlar ketma-ketligining uzunligini oshirish uchun  $N$  darajali polinom (mod 2) bo'yicha ikki polinom ko'paytmasiga tasvirlanmasligi kerak. Masalan, 3-darajali polinomni  $x^3+x+1$  ko'paytmalar shaklida tasvirlab bo'lmaydi. Keltirilgan polinomni ikkilik sanoq tizimida tasvirlash qabul qilingan, ya'ni  $1011_2$ . Bu yerdan, skrembler tashkil qilish uchun yuqori razryad o'chiriladi va  $011_2$  hosil qilinadi. Yaratilgan skremblerning sikli  $7 (=2^3-1)$  ga teng bo'ladi.

Quyidagi polinom  $x^7 + x^6 + x^2$  uchun skrembler siklining uzunligini hisoblashda boshlang'ich  $1001111_2$  holat uchun quyidagi ketma-ketliklarni shakllantiramiz (3-rasm):



3-rasm. Polinom  $x^7 + x^6 + x^2$  uchun skrembler holatlari

E'tibor bering, 7-qadamdan so'ng sonlar takrorlanadi. Demak, 3-rasmda keltirilgan skrembler orqali tashkil etilgan ketma-ketlikning uzunligi, davriyligi 7 ga teng bo'ladi.

### 3. Skrembler yordamida shifrlashga oddiy misol

Ushbu yondashuvdan foydalanib oddiy ikki baytli axborotni shifrlashni ko‘rib chiqamiz. Misol sifatida ‘uz’ ochiq matnni tanlaymiz. ASCII jadvalidan (1- ilova) ‘uz’ matni uchun quyidagi ikkilik kodini shakllantiramiz. Unga binoan ‘u’ - ‘01110101’ va ‘z’ - ‘01111010’, demak ‘uz’ - ‘0111010101111010’ bitlardan iborat bo‘ladi. Quyidagi polinom  $x^7 + x^6 + x^2$  uchun skremblerni shakllantiramiz va boshlang‘ich kalit 1001111<sub>2</sub> bo‘yicha ‘0111010101111010’ kodni shifrlaymiz.

Barcha jarayonlarni jadval shaklida tasvirlaymiz (1-jadval).

1- jadval

**Skrembler yordamida ‘uz’ matnnini shifrlash**

Skrembler $x^7 + x^6 + x^2$	Kalit	Qo‘sish- luvchi bit	‘uz’ matni bitlari	Natija
	1001111			
	0100111	1 ⊕	0	1
	1010011	1 ⊕	1	0
	1101001	1 ⊕	1	0
	1110100	0 ⊕	1	1
	0111010	0 ⊕	0	0
	0011101	1 ⊕	1	0
	1001110	0 ⊕	0	0
	0100111	1 ⊕	1	0
	1010011	1 ⊕	0	1
	1101001	1 ⊕	1	0
	1110100	0 ⊕	1	1
	0111010	0 ⊕	1	1
	0011101	1 ⊕	1	0
	1001110	0 ⊕	0	0
	0100111	1 ⊕	1	0
	1010011	1 ⊕	0	1

Shunday qilib, olingan natija ‘1001000010110001’ shifrmatn bo‘lib, ASCII jadvali bo‘yicha bu ‘ $\oplus$ ’ satriga aylantirildi.

Olingan shifrmatndan ‘1001000010110001’ boshlang‘ich matnni tiklash uchun skrembler ‘1110010111001011’ kodlari bilan qo‘sish  $\oplus$  amalini bajaramiz, ya’ni

$$\begin{array}{r}
 \oplus \quad 1001000010110001 \\
 \underline{1110010111001011} \\
 0111010101111010
 \end{array}$$

Oddiy misollarda, shu bilan birga umumiy holda skrembler yondashuvi orqali matnlarni shifrlash va deshifrlash imkoniyatlari yoritib berildi. Talabalar ushbu bilimlarga asoslanib dasturiy ta'minotni yaratishlari talab etiladi.

### **Amaliy mashg'ulot**

**Mavzu:** N bitli skremblerni qurish va takrorlanish davrini hisoblash.

**Ishdan maqsad:** Skrembler usulini o'rghanish va uning asosida matnni shifrlash.

- 1)Oqimli shifrlash usuli bilan tanishish va skrembler algoritmini tushunib olish;
- 2) Skrembler usulining kamchiliklarini tahlil qilish;
- 3)Amaliy dastur ishlab chiqish maqsadida oddiy misollar bilan tanishish.

### **Amaliy mashg'ulot ishini bajarish tartibi**

- 1.Nazariy ma'lumotlar bilan tarnishing.
- 2.Kompyuterni ishga tushiring.
- 3.Topshiriqlar ro'yxatidan variantni tanlang.
- 4.ASCII jadvalidan foydalanib matnni bitlar ketma-ketligini shakllantiring.
- 5.Skrembler yordamida boshlang'ich kalitdan bitlar ketma-ketligini tuzing.
- 6.Skrembler davriyligini aniqlang.
- 7.Internetga kiring.
- 8.Kripto-kalkulyatorlar bilan tarnishing.
- 9.Deshifrlash jarayionini bajaring.
- 10.Ma'lumotlarni kripto-kalkulyatorda tekshirib ko'chiring.
- 11.Bajarilgan ishlar bo'yicha hisobotlarni tayyorlang.
- 12.Hisobotni himoyaga tayyorlang.
- 13.Ishni tugating.

### **Hisobotni rasmiylashtirish tartibi**

- 1.Akademik jurnal bo'yicha variant tanlansin.

- 2.Hisobotning matn qismi standart o‘lchamdagи varaqlarga (A4 hajmida 210-297 mm) 1,5 intervalda Times New Roman 14 shriftida yozilishi lozim. Fayl formati .doc yoki .docx va .pdf bo‘lsin.
- 3.Hisobotdagi jadvallar va rasmlar tartib bilan raqamlashtirilsin va nomlansin.
- 4.Matnda rasm va jadvalga izoh berilishi kerak.
- 5.Matn rasm va jadval bilan boshlanmasin.
- 6.Matn qismi titul varaqasi bilan boshlanadi va betlar ketma-ket sonlar bilan raqamlashtiriladi.
- 7.Hisobot o‘qituvchining elektron manziliga «Kriptografiya 1 guruh –№-AX 4-amaliy» mavzusi bilan jo‘natilsin .
- 8.Hisobot yakuniy nazoratdan 5 kun oldin jo‘natilishi kerak.
- 9.O‘z vaqtida taqdim etilmagan hisobot baholanmaydi.

#### **Amaliy mashg‘ulot uchun variantlar**

<b>№</b>	<b>Ochiq matn</b>	<b>Polinom</b>	<b>Boshlang‘ich kalit</b>
1	DASTURIY	$x^8 + x^7 + x^6 + x^3 + x^2 + 1$	11001111 <sub>2</sub>
2	BIBLIOGRAFIYA	$x^9 + x^3 + 1$	111001111 <sub>2</sub>
3	MASHINA	$x^{10} + x^5 + x^4 + x^2 + 1$	1011001111 <sub>2</sub>
4	VOSITA	$x^5 + x^4 + x^2 + 1$	10111 <sub>2</sub>
5	DAFTARLAR	$x^{11} + x^5 + x^2 + 1$	10101001111 <sub>2</sub>
6	ALGEBRA	$x^7 + x^5 + x^2 + 1$	1001111 <sub>2</sub>
7	UNIVERSITET	$x^{12} + x^7 + x^3 + x + 1$	101011001111 <sub>2</sub>
8	JAMLANMA	$x^8 + x^6 + x^2 + 1$	11001111 <sub>2</sub>
9	AXBOROT	$x^{11} + x^3 + x^2 + 1$	11101001111 <sub>2</sub>
10	BILIMLAR	$x^6 + x^5 + x + 1$	1001111 <sub>2</sub>
11	MAHSULOT	$x^8 + x^5 + x^3 + x^2 + 1$	11001111 <sub>2</sub>
12	BIZNES	$x^9 + x^4 + 1$	111001111 <sub>2</sub>
13	ILOVALAR	$x^{10} + x^7 + 1$	1001001111 <sub>2</sub>
14	TARMOQ	$x^5 + x^2 + 1$	10111 <sub>2</sub>
15	SHARBAT	$x^{11} + x^2 + 1$	10011001111 <sub>2</sub>
16	RAQAMLAR	$x^7 + x + 1$	1001111 <sub>2</sub>
17	SHAFTOLI	$x^{12} + x^6 + x^4 + x + 1$	101001011111 <sub>2</sub>
18	FOTOAPPARAT	$x^8 + x^4 + x^3 + x^2 + 1$	10101111 <sub>2</sub>
19	TEXNOLOGIYA	$x^{11} + x^{10} + x^9 + x^2 + 1$	10101101111 <sub>2</sub>

20	BOSHQARUV	$x^6 + x + 1$	$101111_2$
21	BANKLARARO	$x^8 + x^2 + 1$	$10011111_2$
22	REKLAMA	$x^8 + x^5 + x^3 + 1$	$11101111_2$
23	SOZLASH	$x^{10} + x^7 + x^3 + 1$	$1001100111_2$
24	TELEFON	$x^8 + x^6 + x^5 + 1$	$10010111_2$
25	DIREKTOR	$x^{10} + x^6 + x^4 + 1$	$1001110111_2$
26	TELEVIZOR	$x^{10} + x^6 + x^4 + 1$	$1101100111_2$
27	YULDUZLAR	$x^{10} + x^7 + x^6 + x^4 + 1$	$1010010111_2$
28	KASALXONA	$x^8 + x^6 + x^4 + x^2 + 1$	$100111101_2$
29	KUTUBXONA	$x^{10} + x^8 + x^4 + 1$	$1011001101_2$
30	MATEMATIKA	$x^{12} + x^8 + x^4 + 1$	$111001010101_2$
31	TESTLASH	$x^{12} + x^9 + x^5 + 1$	$111010100111_2$
32	BUYRUQLAR	$x^{12} + x^{10} + x^6 + 1$	$110010011001_2$

## 5.2. Blokli shifrlar yordamida ma'lumotlarni shifrlash

Blokli shifrlash algoritmlari kriptografik algoritmlar orasida keng tarqalgan algoritm turi bo'lib, mohiyat jihatdan ma'lum uzunlikdagi ma'lumot bitlari ustida qayta-qayta amallar bajarilish orqali amalga oshiriladi. Blokli simmetrik shifrlash algoritmlari ma'lumotni maxfiyligini ta'minlashda keng foydalanilib, boshqa shifrlash algoritmlariga qaraganda o'zining tezkorligi va kriptobardoshligi bilan ajralib turadi.

Blokli simmetrik shifrlash algoritmlariga xos bo'lgan xususiyatlardan biri bu – ma'lum uzunlikdagi ma'lumot bloki ustida qayta-qayta amallar bajarilishi bo'lib, bu raund deb ataladi. Ushbu raund funksiyasi o'zgarmas sanalib, har raundda kiruvchi parametrlar o'zgarishi natijasida ma'lum marta amalga oshiriladi.

Blokli simmetrik shifrlash algoritmlari raund funksiyalarida ARX (add-rotate-xor) amallaridan foydalaniladi, bular:

- Modul asosida qo'shish;
- Surish (siklik surish, mantiqiy surish);
- XOR amali.

Bundan tashqari blokli simmetrik shifrlash algoritmlarida maxsus almashtirish jadvallaridan keng foydalaniladi.

Hozirda simmetrik blokli shifrlash algoritmlari amalda keng qo'llanilib, ularni yaratish quyidagi asoslarga bo'linadi:

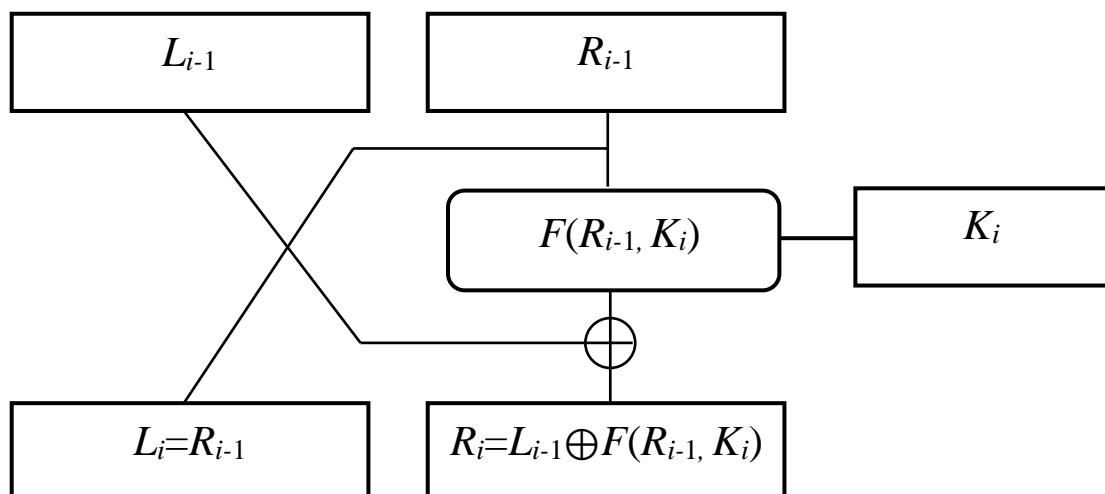
- Almashtirish-o'rniga qo'yish tarmog'iga asoslangan (Substitution-permutation networks, SPN);
- Feystel tarmog'iga asoslangan shifrlash algoritmlari;
- Lai-Massey tarmog'iga asoslangan shifrlash tizimlari.

## 1. Feystel tarmog'i asosi

Feystel tarmog'iga asoslangan blokli simmetrik shifrlash algoritmlari. Ilk yaratilgan va hozirda ham keng foydalanilayotgan blokli simmetrik shifrlash algoritmlari ushbu usul asosida yaratilgan bo'lib, mohiyat jihatdan ma'lumot bloki teng uzunlikdagi ikki qismda ajratilib (chap va o'ng qismlarga), ular ustida ma'lum amallar ketma-ketligi bajariladi. Raund amallari turli kalitlar bilan bir qism bo'lak ustida amalga oshiriladi.

Feystel tarmog'i asosida qurilgan simmetrik blokli shifrlash algoritmlarida shifrlash va deshifrlash uchun bir xil algoritmdan foydalaniladi. Farqli tomoni, raund kalitlarining qo'llanilishi teskarisiga o'zgaradi, ya'ni deshifrlashda 1-raundda  $K_m$  va 2-raundda  $K_{m-1}$  va hokazo oxirgi raundda  $K_1$  ishlataladi.

$F(R_{i-1}, K_i)$  funksiya bir tomonlama bo'lsa ham, deshifrlash natijasida bu funksiya qaytadi. Feystel tarmog'i g'oyasi quyidagicha ifodalanadi. Shifrlanadigan blok ikkita  $L_0, R_0$  qismlarga ajratiladi. Feystel tarmog'i  $i$ -raundi iterativ blokli shifrlash almashtirishi quyidagi sxema bo'yicha aniqlanadi:



1-rasm. Feystel tarmog'inining  $i$ - raundi

Bu yerda  $X_i = (L_{i-1}, R_{i-1})$  -  $i$ -raund uchun  $L_{i-1}$  va  $R_{i-1}$  qismlarga ajratilgan kiruvchi ma'lumot,  $Y_i = (L_i, R_i)$  esa  $X_i$  ni  $i$ - raund kaliti  $K_i$  bilan  $F$  akslantirish natijasida hosil bo'lgan shifrma'alumot. Feystel tarmog'i  $i$  - raundining matematik modeli quyidagicha ifodalanadi:

$$\begin{cases} L_i = R_{i-1} , \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) . \end{cases} \quad (1)$$

Feystel tarmog'iga asoslangan algoritmlar bir necha iteratsiyadan tashkil topgan  $K_i$  kalitlarda shifrlanadigan funksiyadan tashkil topadi. Har bir  $i$ - raunddagи shifrma'lumot ( $i+1$ ) - raund uchun kiruvchi (ochiq) ma'lumot hisoblanadi yoki  $i$  - raunddagи kiruvchi ma'lumot ( $i-1$ )-raund uchun shifrma'lumot hisoblanadi.  $K_i$  raund kalitlari dastlabki  $K$ -kalitdan algoritmda ko'rsatilgan qoida bilan hosil qilinadi.

Feystel tarmog'i akslantirishlarining asosiy xossasi shundan iboratki,  $F$ -raund funksiyasi qaytmas bo'lsa ham, Feystel tarmog'i bu akslantirishlarini qaytarib beradi. Haqiqatan ham, (1) ifodada keltirilgan  $i$ - raund matematik modelida  $\oplus$  - ikkilik sanoq sistemasida qo'shish amali xossasidan foydalangan holda quyidagi tenglikni olish mumkin:

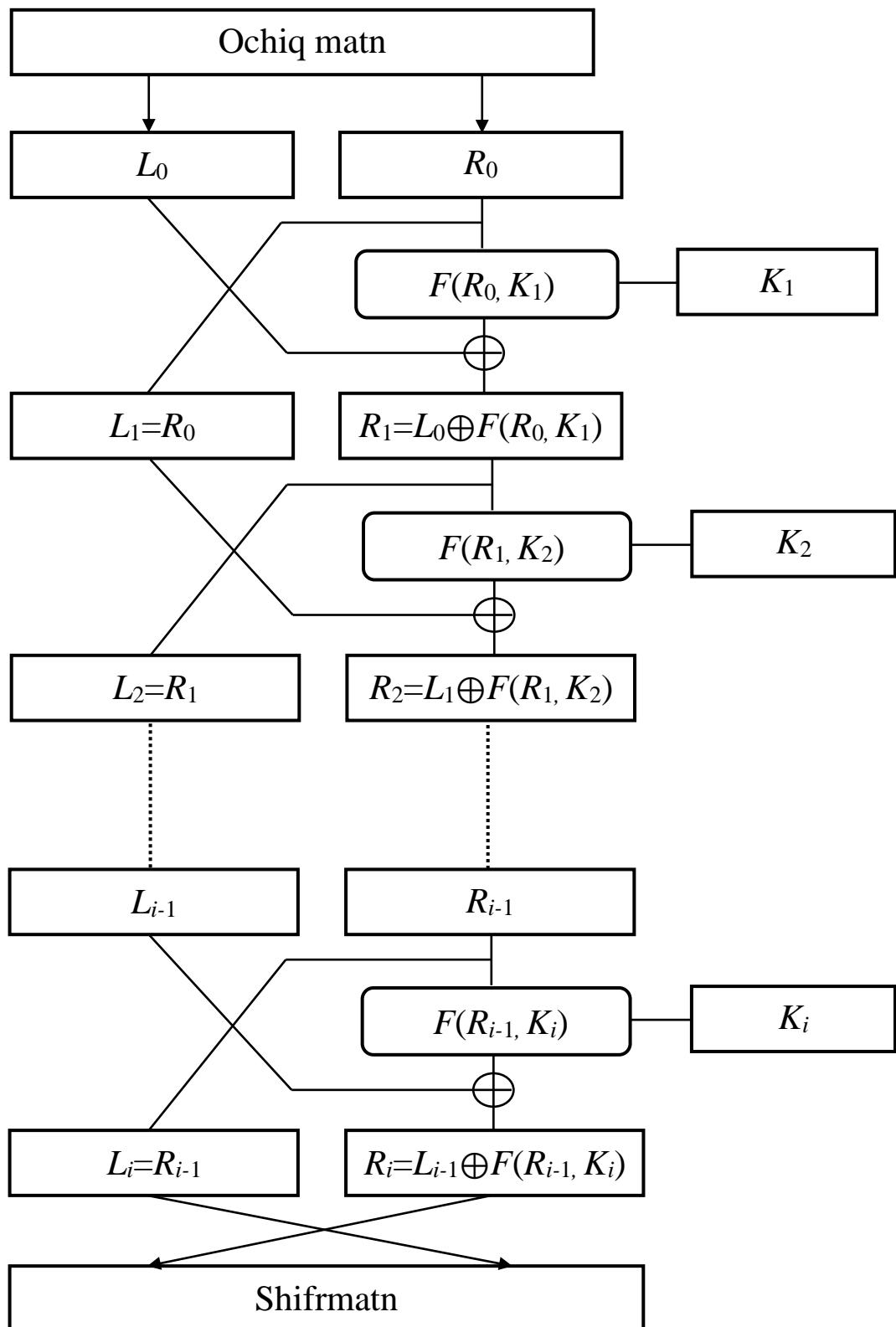
$$\begin{cases} R_{i-1} = L_i , \\ L_{i-1} = R_i \oplus F(L_i, K_i) . \end{cases} \quad (2)$$

Bu oxirgi tengliklar sistemasi Feystel tarmog'i asosida qurilgan shifrlash algoritmlarini deshifrlashining matematik modelini ifodalaydi. Umumiyl holatda  $m$ -raundli Feystel tarmog'inining funksional sxemasi 2-rasmda keltirilgan.

Feystel tarmog'i asosida qurilgan shifrlash algoritmlarida shifrlash va deshifrlash uchun bir xil algoritmdan foydalanilib, faqat raund kalitlarining qo'llanilishi teskarisiga o'zgaradi, ya'ni deshifrlashda 1- raundda  $K_m$ , 2-raundda  $K_{m-1}$  va hokazo oxirgi raundda  $K_1$  ishlataladi.  $F(R_{i-1}, K_i)$  funksiya bir tomonlama bo'lsa ham, deshifrlash natijasida bu funksiya qaytadi.

## **2. Feystel tarmog'i asosida oddiy shifrlash misoli**

Bu yerda uch raundli jarayon bilan tanishish maqsadida oddiy misolni keltiramiz.



2-rasm.  $i$  raundli Feystel tarmog‘i

0) Boshlang‘ich ochiq matnni ikki baytli uzunlikda deb qabul qilamiz. Masalan, ASCII kodlash jadvali asosida ikki baytning kodlarini 100 va 200 ga teng deb olamiz. Ushbu ikki baytni ikki qismga ajratamiz va ularni  $L$  и  $R$  deb olamiz va quyidagicha qiymatlaymiz:  $L=100$  va  $R=200$ . Feystel tarmog‘i uchun  $L$  va n raundlar soniga bog‘liq bo‘lgan  $F$  funksiyasini, masalan, quyidagi shaklda ta’riflaymiz:  $F(L, n) = (L+n) \text{ mod } 256$  ( mod - qoldiqli bo‘lish).

Hisoblash jarayonlarida mantiqiy qo‘sishni inkor etish Xor yoki  $\oplus$  amalidan foydalanamiz. Xor amalini eslatib o‘tamiz:

1-біт	2-біт	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

### Birinchi raund ( $n = 1$ )

1) Demak,  $L = 100$ ,  $R = 200$ . Bundan  $R(200)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo‘shamiz, ya’ni  $200 \oplus ((100+1) \text{ mod } 256)$  ni hisoblab **173**. natijani olamiz. Haqiqatan ham, 200 va 101 sonlarini ikkilik sanoq tizimiga o’tkazib, quyidagi jadvalni hosil qilamiz:

	Ikkilik son							
200	1	1	0	0	1	0	0	0
101	0	1	1	0	0	1	0	1
$\oplus$	1	0	1	0	1	1	0	1

Bu yerdan,

$$10101101_2 = 1*2^7 + 0*2^6 + 1*2^5 + 0*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0 = 128 + 32 + 8 + 4 + 1 = \mathbf{173}$$

2) aniqlangan qiymatlar o‘rni almashtiriladi, ya’ni  $R = 100$  va  $L = 173$  bo‘ladi.

### Ikkinchи raund ( $n = 2$ )

1) Demak,  $L = 173$ ,  $R = 100$ . Bundan  $R(100)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo'shamiz, ya'ni  $100 \oplus ((173 + 2) \bmod 256)$ , ni hisoblab **203** natijani olamiz.

Haqiqatan ham, 173 va 100 sonlarini ikkilik sanoq tizimiga o'tkazib, quyidagi jadvalni hosil qilamiz:

	Ikkilik son							
175	1	0	1	0	1	1	1	1
100	0	1	1	0	0	1	0	0
$\oplus$	1	1	0	0	1	0	1	1

Bu yerdan,

$$11001011_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 128 + 64 + 8 + 2 + 1 = \mathbf{203}$$

2) aniqlangan qiymatlar o'rni almashtiriladi, ya'ni  $R = 173$  va  $L = 203$  bo'ladi.

### Uchinchi raund ( $n = 3$ )

1)  $L = 203$ ,  $R = 173$ . Bundan,  $R(173)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo'shamiz, ya'ni  $173 \oplus ((203 + 3) \bmod 256)$  ni hisoblab **99** natijani olamiz.

Haqiqatan ham, 203 va 173 sonlarini ikkilik sanoq tizimiga o'tkazib, quyidagi jadvalni hosil qilamiz:

	Ikkilik son							
206	1	1	0	0	1	1	1	0
173	1	0	1	0	1	1	0	1
$\oplus$	0	1	1	0	0	0	1	1

Bu yerdan,

$$01100011_2 = 0 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 64 + 32 + 2 + 1 = \mathbf{99}$$

2) Ushbu qadam oxirgi raund bo'lganligi sababli olingan natija  $R$  ga beriladi.

Shunday qilib, quyidagi shifrlangan natija olindi:  $L = 203$ ,  $R = 99$ .

Barcha qadamlarni tasavvur qilish uchun natijalarni jadval shakliga keltiramiz:

<b>Raund</b>	Boshlang‘ich qiymatlar		Natijaviy qiymatlar	
	<b>L</b>	<b>R</b>	<b>L</b>	<b>R</b>
Berilgan	<b>100</b>	<b>200</b>		
1	100	200	173	100
2	173	100	203	173
3	203	173	203	99
Natija			<b>203</b>	<b>99</b>

Hisoblashlar natijasida blokli shifrlash orqali ASCII jadvalidan boshlang‘ich “**Id**” matn “**Лс**” shifrmatnga o‘zgartirildi. .

Endi deshifrlash qadamlari bilan tanishamiz. Buning uchun jarayonlarni teskari bajarish talab etiladi va raundlar 3 dan 1 gacha o‘zgaradi.

### Birinchi raund ( $n = 3$ ).

1)  $L = 203$ ,  $R = 99$ . Bundan,  $R(99)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo‘shamiz, ya’ni  $99 \oplus ((203 + 3) \bmod 256)$  ni hisoblab **173** natijani olamiz.

Haqiqatan ham, 99 va 206 sonlarini ikkilik sanoq tizimiga o‘tkazib, quyidagi jadvalni hosil qilamiz:

	<b>Ikkilik son</b>								
99	0	1	1	0	0	0	1	1	
206	1	1	0	0	1	1	1	0	
$\oplus$	1	0	1	0	1	1	0	1	

Bu yerdan,

$$10101101_2 = 1 * 2^7 + 0 * 2^6 + 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 128 + 32 + 8 + 4 + 1 = \mathbf{173}$$

2) aniqlangan qiymatlar o‘rnii almashtiriladi, ya’ni  $L = 173$  va  $R = 203$  bo‘ladi.

### Ikkinchchi raund ( $n = 2$ )

1)  $L = 173$ ,  $R = 203$ . Bundan,  $R(203)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo‘shamiz, ya’ni  $203 \oplus ((173 + 2) \bmod 256)$  ni hisoblab **100** natijani olamiz.

Haqiqatan ham, 203 va 175 sonlarini ikkilik sanoq tizimiga o‘tkazib, quyidagi jadvalni hosil qilamiz:

	Ikkilik son							
203	1	1	0	0	1	0	1	1
175	1	0	1	0	1	1	1	1
$\oplus$	0	1	1	0	0	1	0	0

Bu yerdan,

$$01100100_2 = 0*2^7 + 1*2^6 + 1*2^5 + 0*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 0*2^0 = 64 + 32 + 4 = \mathbf{100}$$

2) aniqlangan qiymatlar o‘rnii almashtiriladi, ya’ni  $L = 100$  va  $R = 173$  bo‘ladi.

### Uchinchi raund ( $n = 1$ )

1)  $L = 100$ ,  $R = 173$ . Bundan,  $R(173)$  qiymatini  $F(L, n)$  qiymati bilan  $\oplus$  amali bilan qo‘shamiz, ya’ni  $173 \oplus ((100 + 1) \bmod 256)$  ni hisoblab quyidagi natijani olamiz:

$$R = \mathbf{200}.$$

Haqiqatan ham, 173 va 101 sonlarini ikkilik sanoq tizimiga o‘tkazib, quyidagi jadvalni hosil qilamiz:

	Ikkilik son							
173	1	0	1	0	1	1	0	1
101	0	1	1	0	0	1	0	1
$\oplus$	1	1	0	0	1	0	0	0

Bu yerdan,

$$11001000_2 = 1*2^7 + 1*2^6 + 0*2^5 + 0*2^4 + 1*2^3 + 0*2^2 + 0*2^1 + 0*2^0 = 128 + 64 + 8 = \mathbf{200}$$

Sunday qilib, deshifrlash natijalari boshlang‘ich matnga mos keldi:  $L = 100$ ,  $R = 200$ .

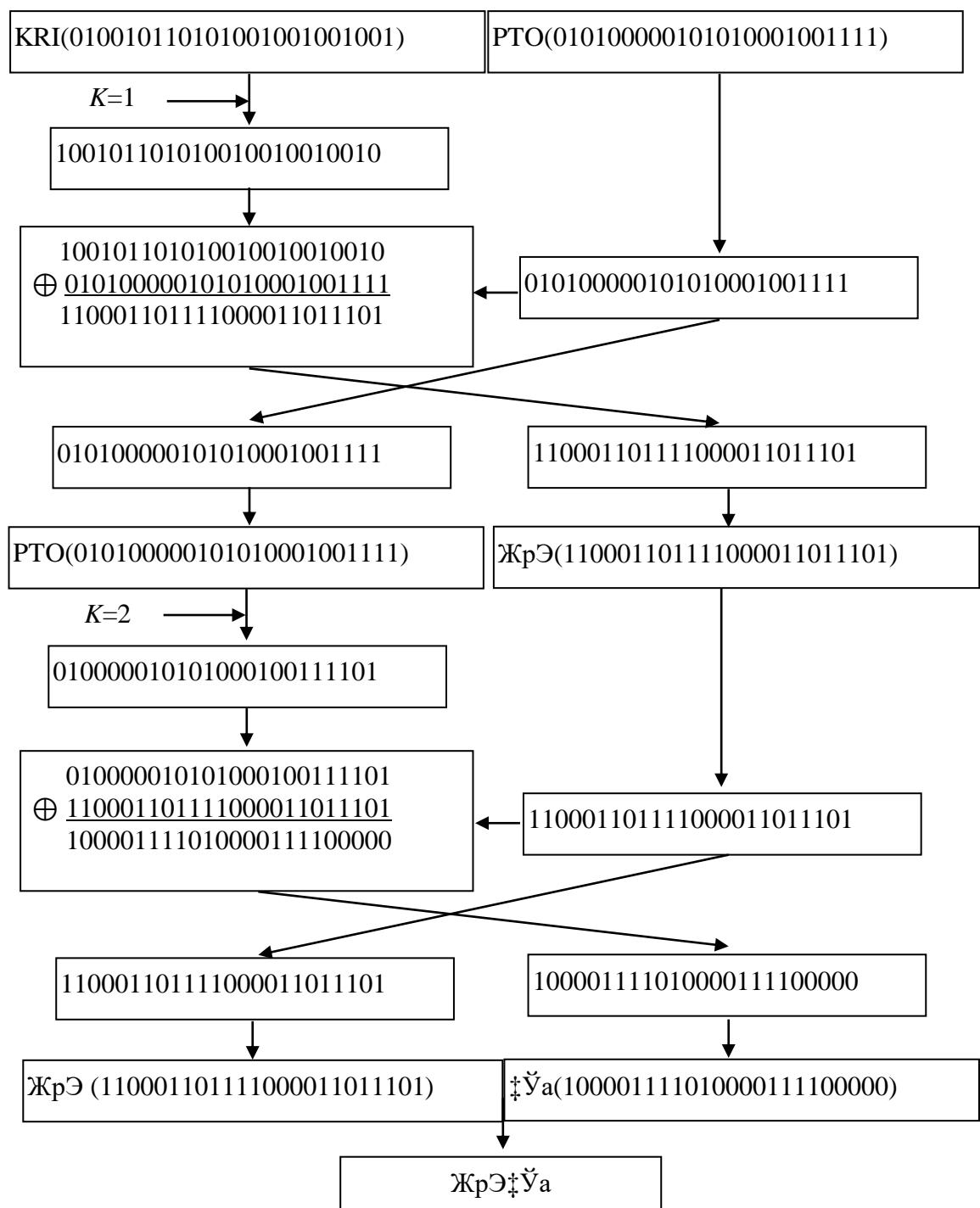
### 3. Feystel tarmog‘i asosida murakkab shifrlash jarayoniga misol

Bu yerda Feystel tarmog‘i uchun blokli shifrlashda murakkab misolni keltiramiz. Bunda ‘**KRIPTOTAHLLIL**’ boshlang‘ich matnni asos qilib olamiz va uni teng ikki qismga, blokga bo‘lamiz: **KRIPTO+TAHLIL**. Funksiya sifatida bitlarni raund kalitida berilgan songa siljитish amalini qabul qilamiz. Maxfiy kalit sifatida  $K = [1, 2]$  deb qabul qilamiz, ya’ni  $K[0] = 1$  va  $K[1] = 2$ . Jarayon davomida Xor amalidan foydalanamiz, shu bois matnni ASCII standarti bo‘yicha

ikkilik sanoq tizimida keltiramiz. Demak, **KRIPTO** matni uchun quyidagini hosil qilamiz:

<b>K</b>	<b>R</b>	<b>I</b>	<b>P</b>	<b>T</b>	<b>O</b>
01001011	01010010	01001001	01010000	01010100	01001111

Ushbu birinchi blokni Feystel tarmog‘idan o‘tkazamiz (3-rasm).

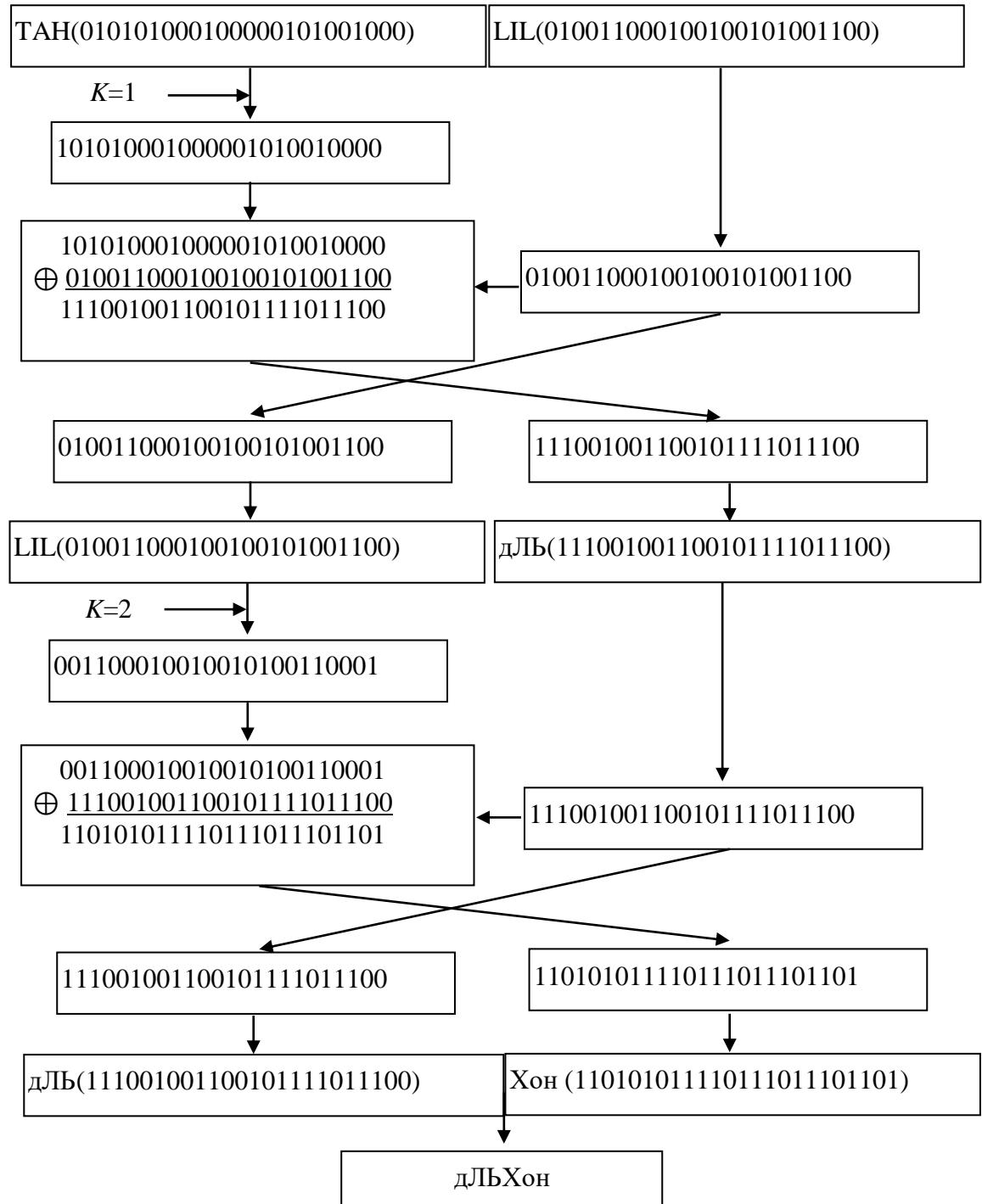


3-rasm. ‘**KRIPTO**’ ni Feystel tarmog‘idan o‘tkazish jarayoni

Shunday qilib, birinchi blok ‘**KRIPTO**’ quyidagi ‘**ЖрЭ‡Ўа**’ shifrmatnga aylandi. Bu yerda lotin harflari uchun 7 bitli kodlarni ham qo‘llash mumkin.

T	A	H	L	I	L
01010100	01000001	01001000	01001100	01001001	01001100

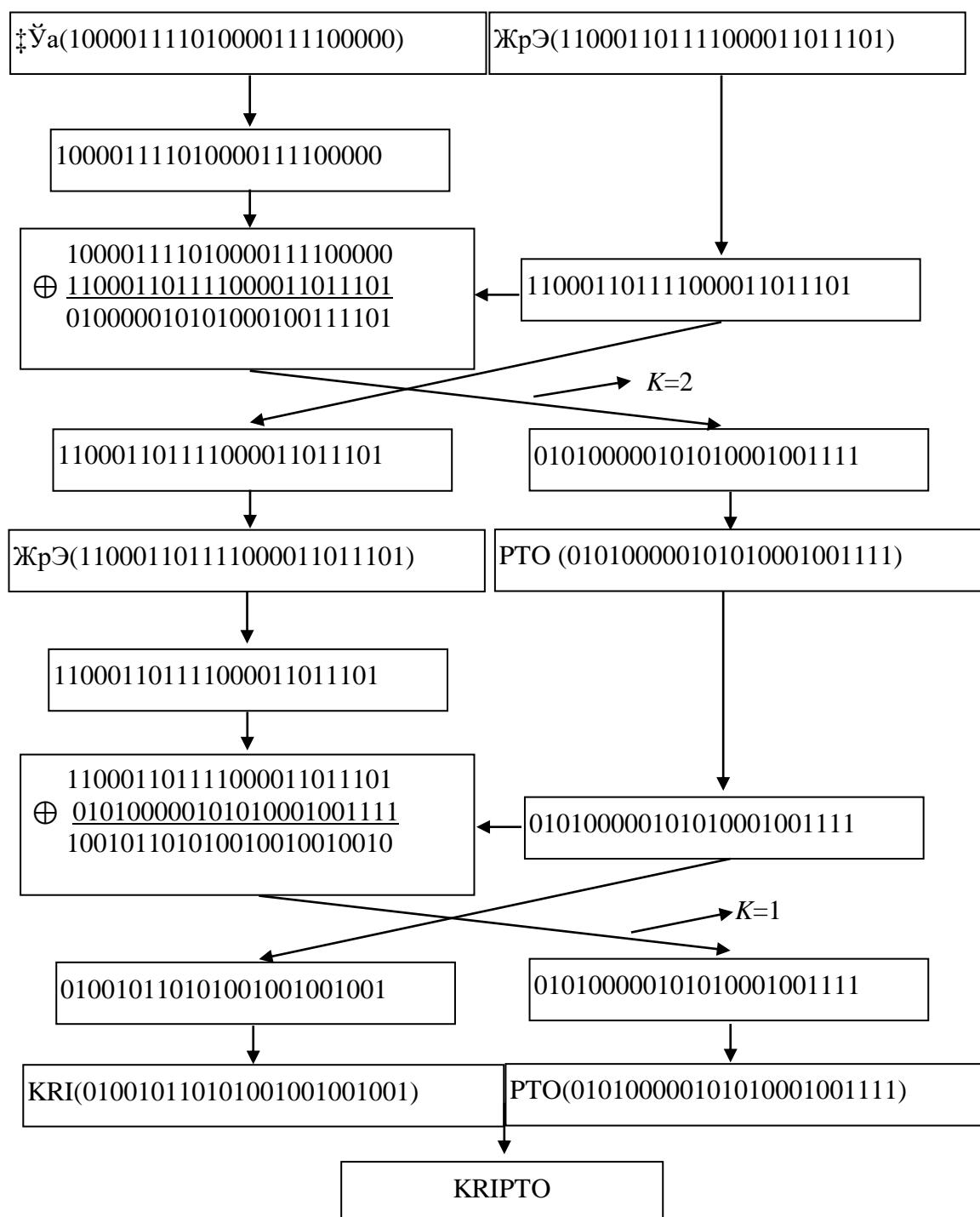
Ushbu ikkinchi blokni Feystel tarmog‘idan o‘tkazamiz:



4-rasm. ‘**TAHLIL**’ ni Feystel tarmog‘idan o‘tkazish jarayoni.

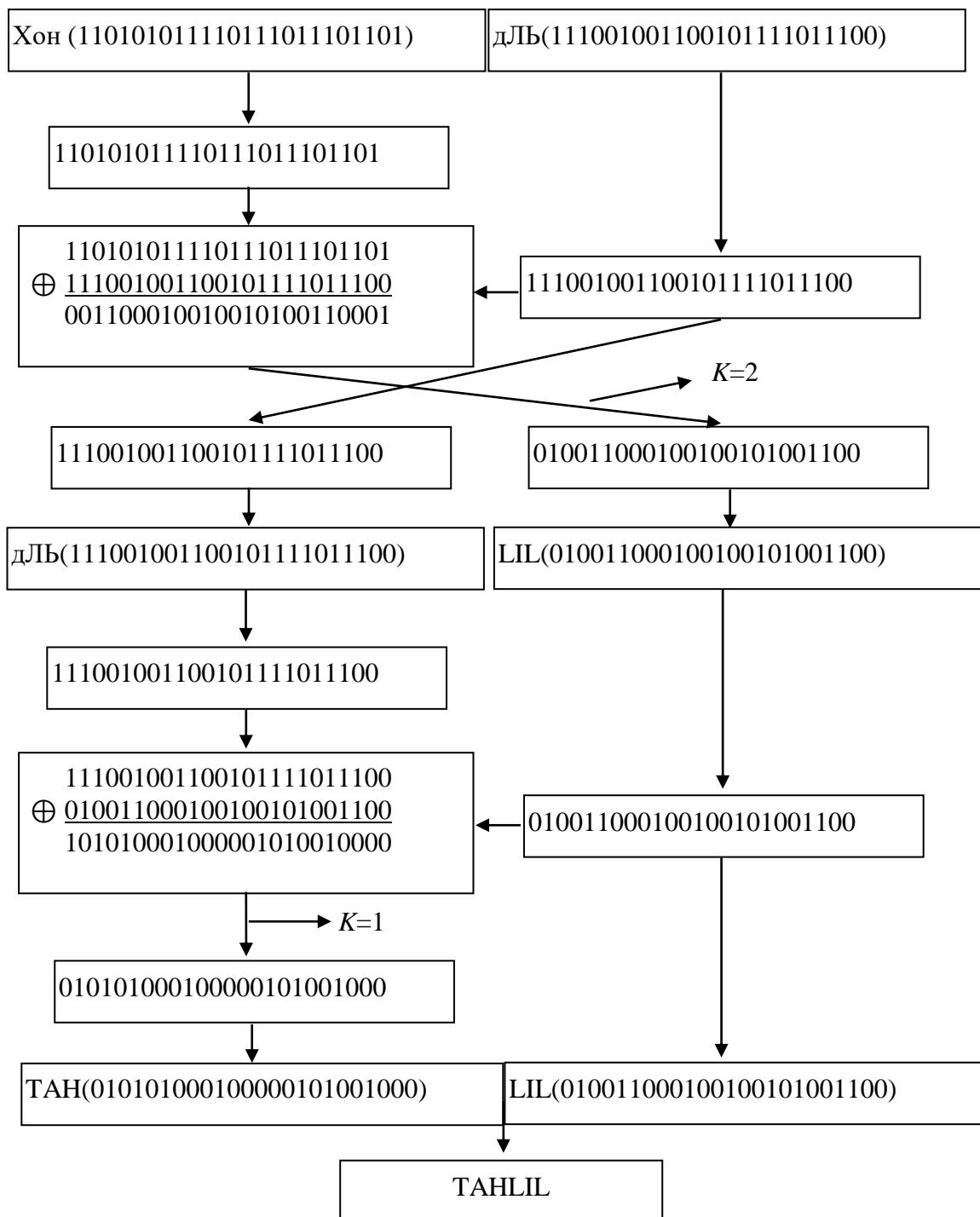
Endi ikkinchi blokga o'tamiz. Ushbu ‘**TAHLIL**’ blokida mavjud bir xil harflarni har xil kodlashini kuzatish mumkin bo'ladi. Bunda ‘**TAHLIL**’ matni ASCII standarti bo'yicha ikkilik sanoq tizimiga o'tkaziladi (4-rasm).

Shunday qilib, ‘**KRIPTOTAHLIL**’ ochiq matni quyidagi ‘**ЖрЭ‡ЎадЛъХон**’ shifrmatniga aylantirildi. Olingan natijani to'g'ri ekanligini tekshirish uchun keltirilgan jarayon teskari amalga oshiriladi.



5-rasm. ‘**KRIPTO**’ so‘zini Feystel tarmog‘idan tiklash jarayoni.

Demak, deshifrlash bevosita yuqorida keltirilgan algoritmga deyarli mos holda bajariladi. Ya’ni shifrmatn ikki blokga bo‘linadi va har bir blok bilan Feystel tarmog‘idan o’tkaziladi. Faqatgina raund kalitlari teskari tartibda kiritiladi, ya’ni birinchi raundda  $K = 2$  va ikkinchi raundda  $K = 1$  bo‘ladi.



6-rasm. ‘TAHLIL’ so‘zini Feystel tarmog‘idan tiklash jarayoni.

Demak, shifrmatn ‘ЖрЭ‡ЎадЛЬХон’ ikki blokka bo‘linadi , ya’ni – **ЖрЭ‡Ўа + дЛЬХон**. Funksiya sifatida bitlarni raund kalitida berilgan songa teskari siljitish amalini qabul qilamiz. Birinchi ‘ЖрЭ‡Ўа’ blokni ASCII standarti asosida ikkilik sanoq tizimiga o‘tkazamiz:

<b>Ж</b>	<b>Р</b>	<b>Ә</b>	<b>‡</b>	<b>Ӯ</b>	<b>а</b>
11000110	11110000	11011101	10000111	10100001	11100000

Endi Feystel tarmog ‘idan ushbu birinchi blokni o‘tkazamiz va bunda  $K=2$  kaliti birinchi bo‘lib qo‘llaniladi (5-rasm).

Barcha jarayonlar bajarilgandan so ‘ng shifrmatndan ‘ЖрЭ‡Ўа’ ochiq matn ‘**KRIPTO**’ natijasi olindi. E’tibor beramiz, bu yerda kalit bo‘yicha bitlarni siljitish teskari tomonga amalga oshirildi va bu jarayon Xor amalidan so‘ng bajarildi.

Endi ikkinchi blokga ‘дЛЬХон’ o‘tamiz. Bu yerda ham yuqoridagidek barcha jarayonlarni bajaramiz:

<b>Д</b>	<b>Л</b>	<b>Ь</b>	<b>Х</b>	<b>О</b>	<b>Н</b>
11100100	11001011	11011100	11010101	11101110	11101101

Feystel tarmog‘ida baajarilgan jarayonlar 6-rasmida aks ettiriladi.

Shunday qilib, ikkinchi blok ‘дЛЬХон’ bevosita ‘TAHLIL’ ochiq matnga qaytib keldi. Demak, boshlang‘ich ochiq matn to‘liq tiklandi.

Umumiy holda Feystel tarmog‘ida raund kalitlari o‘zaro bog‘liq bo‘lmasa va kriptomustahkam psevdotasodifiy  $F$  funksiyasi uchun shifrmatn psevdotasodifiy bo‘lishi uchun bevosita uchta raund yetarli hisoblanadi.

## Amaliy mashg‘ulot

**Mavzu: Feystel tarmog‘i asosida chiziqli kriptotahlil usulini o‘rganish**

**Ishdan maqsad:** Feystel tarmog‘ini o‘rganish orqali ochiq matnni shifrlash va deshifrlash jarayonlarini o‘rganish:

- 1) Feystel tarmog‘ini o‘rganish va blokli shifrlash usulini tushunib olish;
- 2) Feystel tarmog‘ining kamchiliklarini o‘rganish;

- 3) Bajarilgan ishlar asosida hisobotni shakllantirishni o‘rganish.
- 4) OpenSSL kutubxonasidan foydalangan holda blokli shifrlar yordamida ma’lumotlarni shifrlash dasturini tuzish.

### **Amaliy mashg‘ulot ishini bajarish tartibi**

1. Nazariy ma’lumotlar bilan tarnishing.
2. Kompyuterni ishga tushiring.
3. Topshiriqlar ro‘yxatidan variantni tanlang.
4. ASCII belgilarni kodlash jadvalidan matnning ikkilik qiymatini aniqlang.
5. Blokli shifrlash usuli bilan tanishing.
6. Feystel ususlidan foydalanib blokli shifrlashni amalga ohsiring.
7. Internetga kiring.
8. Kripto-kalkulyatorlar bilan tarnishing.
9. Deshifrlash jarayionini bajaring.
10. Ma’lumotlarni kripto-kalkulyatorda tekshirib ko‘chiring.
11. Bajarilgan ishlar bo‘yicha hisobotlarni tayyorlang.
12. Hisobotni himoyaga tayyorlang.
13. Ishni tugating.

### **Hisobotni rasmiylashtirish tartibi**

1. Akademik jurnal bo‘yicha variant tanlansin.
2. Hisobotning matn qismi standart o‘lchamdagи varaqlarga (A4 hajmida 210-297 mm) 1,5 intervalda Times New Roman 14 shriftida yozilishi lozim. Fayl formati .doc yoki .docx va .pdf bo‘lsin.
3. Hisobotdagi jadvallar va rasmlar tartib bilan raqamlashtirilsin va nomlansin.
4. Matnda rasm va jadvalga izoh berilishi kerak.
5. Matn rasm va jadval bilan boshlanmasin.
6. Matn qismi titul varaqasi bilan boshlanadi va betlar ketma-ket sonlar bilan raqamlashtiriladi.
7. Hisobot o‘qituvchining elekton manziliga «Kriptoanaliz usuli guruh –№-AX 1-lab» mavzusi bilan jo‘natilsin .

8.Hisobot yakuniy nazoratdan 5 kun oldin jo‘natilishi kerak.

9.O‘z vaqtida taqdim etilmagan hisobot baholanmaydi.

### **Amaliy mashg‘ulotlari uchun variantlar**

#### **1-topshiriq**

Ikki belgini Feystel tarmog‘idan foydalanib shifrlash va deshifrlash jarayonini amalga ohiring va bunda quyidagi funksiyadan foydalaning  $F(L, n) = (L+n) \bmod 256$ . Bunda raundlar soni 3 ga teng.

Variantlar

<b>№</b>	<b>Matn</b>										
1	Ek	9	ha	17	oB	25	Oq	33	oz	41	uN
2	eK	10	It	18	ob	26	oQ	34	Pi	42	un
3	ek	11	iT	19	Ok	27	oq	35	pI	43	Uz
4	Ez	12	it	20	oK	28	Ot	36	pi	44	uZ
5	eZ	13	Iz	21	ok	29	oT	37	Ta	45	uz
6	ez	14	iZ	22	Ol	30	ot	38	tA	46	Va
7	Ha	15	Iz	23	oL	31	Oz	39	ta	47	vA
8	hA	16	Ob	24	ol	32	oZ	40	Un	48	va

#### **2-topshiriq**

Ikki raundli Feystel tarmog‘idan foydalanib shifrlash va deshifrlash jarayonini amalga oshiring va bunda maxfiy  $K = [1, 2]$  kalitini qo‘llang. Belgilarni kodlashda 7 bitli ASCII jadvalini qo‘llang.

Variantlar

<b>№</b>	<b>Ochiq matn</b>	<b>№</b>	<b>Ochiq matn</b>
1	DASTURIY	16	KOSMONAVTLAR
2	SINFXONA	17	BILIMLAR
3	QAROQCHI	18	DIREKTOR
4	VOSITANI	19	TIZIMLAR
5	TAQINCHOQLAR	20	QIZIQCHI
6	INSTITUT	21	RAQAMLAR
7	UNIVERSITETI	22	SHAFTOLI
8	JAMLANMA	23	APPARAT

9	AXBOROTI	24	AYIRMASI
10	BUTUNLIK	25	BOSHQARUVCHI
11	MAHSULOT	26	MUHARRIR
12	AGENTLIK	27	TESTLASH
13	ILOVALAR	28	TARMOQLI
14	QULUPNAY	29	SAHIFASI
15	SHARBATI	30	ASKARLAR

### 5.3. Psevdotasodifiy sonlar generatorini va uning dasturiy ta'minotini yaratish

Hozirgi kunda tasodifiy va psevdotasodifiy generatorlar ilm-fanning rivojlanishida muhim ahamiyat kasb etadi. Qo'llash sohasiga nazar tashlaydigan bo'lsak, misol sifatida quyidagi yo'nalishlarni keltirish mumkin: modellashtirish, sonli usullar, tanlash usullari, dasturlash, kriptografiya. Axborot xavfsizligini ta'minlashda tasodifiy va psevdotasodifiy ketma-ketliklari keng qo'llaniladi. Masalan, parollarni generatsiya qilish, kriptografik kalitlarni ishlab chiqish shularga misol bo'ladi. Shu bois, ushbu sohada mukammal generatorlarni yaratish muhim hisoblanadi.

Tasodifiy son – bu sonlarning ma'lum to'plamidagi har bir son bir xil ehtimollik bilan tanlab olinishi mumkin bo'lgan sonlar to'plamidan tanlab olingan son.

Tasodifiy sonlar generatori – bu berilgan ehtimoliy va algebraik xarakteristikalar bilan tasodifiy vektorlar (qiymatlar, sonlar) ni hosil qilish (ishlab chiqish) algoritmi.

Psevdotasodifiy sonlar generatori – bu elementlari deyarli bir-biridan mustaqil bo'lgan va berilgan taqsimotga bo'ysunadigan sonlarning ketma-ketligini generatsiyalaydigan algoritm.

Tasodifiy sonlarni qo'llashda quyidagi sohalarni keltirish mumkin:

1. Ijtimoiy va ilmiy izlanishlar. Ma'lumotlarni to'plash va ularni qayta ishslash, so'rovnomalar o'tkazish yoki fizikaviy tajribalarni o'rghanishda tasodifiy sonlar qo'llaniladi.

2. Modellashtirish. Fizik jarayonlarni kompyuterda modellashtirishda tasodifiy sonlar orqali matematik modellarni fizik modellarga mosligini ta'minlash mumkin bo'ladi.
3. Kriptografiya va axborot xavfsizligi. Kriptografiyada mavjud shifrlash algoritmlarida tasodifiy sonlarni keng qo'llanishi orqali axborot xavfsizligi ta'minlash mumkin.
4. Ekspert tizimlarida qaror qabul qilish. Tasodifiy sonlar orqali o'yin strategiyasini ishlab chiqish yoki optimallashtirish masalalarida funksiya ekstremumini aniqlash imkonini beradi.
5. Xordiq va o'yinlar. Kompyuter o'yinlarida tasodifiy sonlar haqqoniylilikni va xilma-xillikni ta'minlaydi.

Tasodifiy sonlarni matematik yondashuv orqali shakllantirishda ilk bor 1946-yilda Jon fon Neyman tomonidan amalga oshirilgan. Bunda sonning kvadrati hisoblanadi va undagi o'rta raqamlar navbatdagi tasodifiy son hisoblanadi. Masalan, 259 sonining kvadrati 67081 ga teng bo'ladi va keyingi tasodifiy son 708 ga teng bo'ladi.

Samarali va tezkor tasodifiy sonlarni generatsiya qilish hozirgi kungacha murakkab masalalardan biri hisoblanadi.

### **1.Tasodifiy ketma-ketliklar tasnifi**

Tasodifiy sonlar ketma-ketligi – sonlarning ketma-ketligini, ularning har birini faqat ushbu ketma-ketlikning oldingi sonlarini bilish asosida oldindan aytib (hisoblab) bo'lmaydi.

Psevdotasodifiy sonlar ketma-ketligi – muayyan holda tasodifiy sonlar ketma-ketligi o'rniga foydalaniladigan qaysidir hisoblash jarayonini bajarish natijasida olingan sonlar ketma-ketligi.

Psevdotasodifiy ketma-ketlik – muayyan arifmetik qoida bo'yicha hisoblangan, ammo yechiladigan masala doirasida tasodifiy sonlar ketma-ketligining barcha xususiyatlariga ega bo'lgan sonlar ketma-ketligi.

Psevdotasodifiy sonlar – qandaydir algoritm bo'yicha olingan, amalda esa tasodifiy sonlar sifatida foydalaniladigan sonlar.

Umumiy holda tasodifiy sonlar generatorlari ishlash muhit bo'yicha quyidagicha tasniflanadi:

- apparatli;
- jadvalli;
- algoritmlı.

Apparatli generatorlarda tasodifiy sonlarni yaratishda maxsus texnik manba talab etiladi. Bunday texnik qurilmani yaratish, birinchidan murakkab masala, ikkinchidan bunday qurilmaning xavfsizligini ta'minlash muammosi paydo bo'ladi.

Jadvalli generatorlar bevosita oldindan tayyorlanilgan tasodifiy sonlardan iborat jadvallarga asoslanadi. Bunday yondashuvning asosiy kamchiliklari sifatida quyidagilar e'tirof etilgan: jadvallar tashqi qurilmada saqlanishi, tasodifiy sonlarning cheklanganligi, har bir qadamda keyingi qadamda qanday son kelishi aniqligi.

Algoritmlı generatorlar qandaydir fizikaviy qurilmadan olingan boshlang'ich chekli ma'lumotlarni qayta ishlash asosida sonlar ketma-ketligini shakllantiradi.

## **2. Psevdotasodifiy sonlarning algoritmlı generatorlari**

Algoritmlı generatorlarni yaratish apparatli generatorlarni yaratishdan ham murakkab masala bo'lishi mumkin. Ushbu algoritm uchun zarur bo'ladigan boshlang'ich chekli ma'lumotlarni yaratadigan manba sifatida kompyuter tizimida mavjud quyidagi apparatli vositalar qo'llaniladi:

1. tizimli soat holati;
2. klaviatura tugmalarini bosilishi yoki "sichqoncha" ning harakati;
3. kirish/chiqish buferining tarkibi;
4. tizimning holati, masalan, tizimning yuklanish vaqtiga, tarmoqning faolligiga va b.

Tasodifiylik katta rol o'ynaganligi sababli, birinchi navbatda muhim bo'lgan tasodify ketma-ketliklarni ishlab chiqaruvchi generatorlarning turlari bilan tanishish muhim hisoblanadi.

Psevdotasodifiy sonlar generator algoritmining umumiy formulasi quyidagi shaklda bo‘ladi:

$$X_{i+1} = f(X_{i-k+1}, X_{i-k+2}, \dots, X_i),$$

bu yerda  $f$  – boshlang‘ich k ta ma’lumotlarni qayta ishlaydigan funksiya.

Bundan hosil bo‘lgan sonlar ketma-ketligida takrorlanish mavjud bo‘ladi va uning uzunligi davriylik deb nomlanadi.

### 3.Son kvadratining o‘rta qismi

Yuqorida e’tirof etilgan usul 1946-yilda Jon fon Neyman tomonidan taklif etilgan. Unda quyidagi qadamlar bajariladi:

1. Boshlang‘ich  $n$  raqamli  $X_0$  qiymati tanlanadi.
2. Ushbu  $X_i$  soni kvadratga oshirilib  $2n$  ta raqamdan iborat yangi son  $Y_i$  taskil etiladi.
3. Keyingi  $X_{i+1}$  sonini olish uchun  $Y_i$  sonining o‘rta  $n$  ta raqami tanlanadi.

Masalan,  $X_0 = 3485$  soni uchun  $Y_1 = 3485^2 = 12145225$  ga teng bo‘ladi, bu yerdan  $X_1 = 1452$ , xuddi shunday  $X_2 = 1083$  va h.k.

Odatda boshlang‘ich son uchun o ‘nlik kasrlar tanlanadi. Masalan,  $X_0 = 0,3485$ ,  $X_1 = 0,1452$ ,  $X_2 = 0,1083$  va h.k.

Ushbu amallarni oddiy arifmetik formulalar orqali ham amalga oshirish mumkin.

Ko‘rilgan usulda sonlar orasida korrelyatsion bog‘lanish mavjud, ba’zi variantlarda umuman tasodiylik ham o‘rinsiz bo‘ladi, masalan,  $X_0 = 0,4500$ ,  $X_1 = 0,2500$ ,  $X_2 = 0,2500$ ,  $X_3 = 0,2500$  va h.k. Bularidan tashqari, ketma-ketlikning davriyligi ham juda kichik bo‘ladi. Shu bois, bu usul faqatgina tarixiy nuqtayi nazardan qiziqlarlidir.

Tasodify ketma-ketliklar haqiqiy tasodify ketma-ketliklarga va psevdotasodifiy ketma-ketliklarga bo‘linadi.

Tasodify ketma-ketlikni bevosita fizik generatorlar va dasturiy generatorlardan foydalanib hosil qilish mumkin.

Fizik hodisalarining o‘zgarish majmuyiga asoslangan generatorlar orqali ishlab chiqilgan ketma-ketlik haqiqiy tasodify bo‘lib, bu ketma-ketlik bir martagina ishlab chiqilib, uni keyinchalik biror bir usul yoki vosita bilan xuddi

shunday tarzda takrorlanishini boshqarish murakkab hisoblanadi. Shu sababli ma'lumotlarni shifrlash jarayonida bevosita fizik generatorlar bilan ishlab chiqilgan ketma-ketlikni kalitlar gammasi sifatida qo'llash maqsadga muvofiq emas. Chunki, deshifrlash jarayonida qo'llaniladigan fizik generatorning aynan shifrlash jarayonida qo'llanilgan ketma-ketlikni ishlab chiqishi kafolatlanmaydi.

Haqiyqiy tasodifiy ketma-ketliklar (HTKK), ularning chiqishdagi qiymatlarini takrorlab bo'lmashligi bilan harakterlanadi. Masalan tangani 100 marta tashlab, uning qanday holatda tushishini 100 bitli ketma-ketlik holatida ifodalasak, yer yuzida har bir kishi bir xil 100 bitli ketma-ketlikni hosil qila olmaydi. Muvoffaqiyat ehtimoli

$2^{-100}$ , bu son juda kichik ehtiollikdir. HTKK lar fizik jarayonlarga asoslangan. Bunga misollar: tangani tashlash, o'yin toshlarini tashlash, yarim o'tkazgich shovqini va h.k.

Biror noma'lum parametrga (kalitga) bog'liq bo'lgan matematik model asosida psevdotasodifiy ketma-ketlik ishlab chiquvchi dasturiy generatorlar hosil qilgan psevdotasodifiy ketma-ketlikni, noma'lum parametr qiymatini bilgan holda, xuddi shu matematik model va uning dasturiy ta'minoti asosida ketma-ketlikning qayta takrorlanishini boshqarish mumkin. Bunday holat, ma'lumotlarni shifrlash jarayonida bevosita dasturiy generatorlar bilan ishlab chiqilgan psevdotasodifiy ketma-ketlikni kalitlar gammasi sifatida qo'llash maqsadga muvofiqligini anglatadi va deshifrlash jarayonida qo'llaniladigan dasturiy generatorning aynan shifrlash jarayonida qo'llanilgan psevdotasodifiy ketma-ketlikni ishlab chiqishi kafolatlanadi.

Psevdotasodifiy ketma-ketliklar generatori (PTKK, PRNG(ingl.) - Pseudo-random number generators) boshlang'ich berilgan qiymatdan foydalangan holda ketma-ketliklarni generatsiya qiladi. Ko'pincha ular quyidagicha rekursiv holda hisoblanadi:

$$s_{i+1}=f(s_i), i=0,1,\dots$$

bu yerda  $s_0$  boshlang'ich qiymat bo'ladi. Tasodifiylik darajasi yuqori bo'lgan psevdotasodifiy ketma-ketlikni ishlab chiqaruvchi generatorlar zamonaviy

kriptotizimlarning ajralmas qismi hisoblanadi. Tasodifiy ketma-ketliklar kriptografiyada quydagи maqsadlarda qo'llaniladi:

- simmetrik kriptotizimlar uchun tasodifiylik darajasi yuqori bo'lgan seans kalitlari va boshqa kalitlarni generatsiya qilishda;
- asimmetrik kriptotizimlarda qo'llaniladigan katta qiymatlar qabul qiluvchi parametr larning tasodifiy boshlang'ich qiymatlari generatsiyasida;
- blokli shifrlash algoritmlarining boshlang'ich tasodifiy qiymat talab qiluvchi CBC, OFB va boshqa qo'llanish tartib-qoidalari uchun tasodifiylik darajasi yuqori bo'lgan boshlang'ich vektorlar hosil qilishda;
- elektron raqamli imzo tizimlarida katta qiymatga ega parametr lar uchun dastlabki tasodifiy qiymatlarni generatsiyasida;
- bitta protokol orqali bir xil ma'lumotlarni har-xil kalitlar qo'llash bilan shifrlab har-xil ko'rinishda uzatish uchun talab qilinadigan holatlarda kalit uchun yetarli uzunlikdagi tasodifiy ketma-ketlik hosil qilishda, masalan SSL va SET protokollarida.

Elementar rekurrent hisoblashlarga asoslangan psevdotasodifiy ketma-ketlik generatorlari ularda qo'llanilgan akslantirishlarga ko'ra chiziqli, multiplikativ va chiziqsiz turkumlarga bo'linadi.

#### **4. Chiziqli kongruent generator**

Chiziqli kongruent generatorlar umumiy holatda  $x_{i+1} = (ax_i + c) \bmod N$  formula bilan aniqlanuvchi rekurrent hisoblashga asoslangan. Bu yerda dastlabki berilgan kirish parametrleri asosida ketma-ketliklar hosil qilinadi.

Bunda kirish parametrleri:

$N$  – chekli maydon xarakteristikasini ifodalovchi son ( $N > 0$ ),  $a$  va  $c$  - o'zgarmas musbat butun sonlar,  $x_0$  – boshlang'ich butun qiymatli son ( $0 \leq a, c, x_0 \leq N$ );

Boshlang'ich butun qiymatli son  $x_0$  bu yerda kalit sifatida qabul qilinadi.

Ketma-ketlikni tashkil etuvchi chiqish qiymatlari esa quyidagi rekurrent formula bilan aniqlanadi:

$$x_{i+1} = (ax_i + c) \bmod N, i = 0, 1, 2, 3, \dots$$

Bu yerda mavjud parametrlarni tanlash juda muhim hisoblanadi, masalan  $a=8$ ,  $x_{i0} = 7$ ,  $c = 9$ ,  $N = 10$  uchun quyidagi natijalar olinadi: 7, 5, 9, 1, 7, 5, 9, 1...

Ushbu chiziqli kongruent generator uchun  $N$  sonini qanday tanlash lozimligi haqida to‘xtalib o‘tamiz. Birinchidan,  $N$  juda katta son bo‘lishi kerak. Masalan,  $N=2$  uchun eng yaxshi ketma-ketlik quyidagi ko‘rinishda bo‘lishi mumkin: 0,1,0,1....

Ikkinchidan,  $N$  sonini  $2^q$  ko‘rinishda, bu yerda  $q$  – mashina so‘zi uzunligi, bo‘lishi modul bo‘yicha bo‘lishni osonlashtiradi.

Parametrlarni tanlashda ketma-ketlikning davriyiligiga e’tibor beriladi. Ammo boshqa faktorlarni ham inobatga olish kerak, masalan,  $a = c = 1$  uchun

$$x_{i+1} = (x_i + 1) \bmod N$$

ketma-ketligi maksimal davriylikga ega bo‘ladi, ammo tasodifiylik buziladi.

Misol sifatida quyidagi parametr qiymatlarini keltirish mumkin:

$$a = 1103515245, \quad x_{i0} = 12345, \quad c = 12345, \quad N = 2^{31}.$$

Chiziqli kongruent generatorning kirish parametri  $c=0$  bo‘lsa, ya’ni  $x_{i+1} = (ax_i) \bmod N$ , ( $i = 0, 1, 2, 3, \dots$ ) bo‘lsa, bu generator chiziqli multiplikativ generator deyiladi. Bunda  $2^{31}-2$  davrga ega bo‘lgan quyidagi koeffisiyentlar taklif etiladi:

$$a = 7^5 = 16807, \quad N = 2^{31}-1 = 2147483647.$$

Berilgan  $x_i$  ketma-ketlik  $p$  davriy bo‘ladi, agarda eng kichik  $p$  natural son uchun  $x_{i+p} = x_i$  tenglik barcha  $i \geq 0$  uchun bajarilsa.

Kriptografiyada  $x_i$  ketma-ketlik quyidagi xossalarga ega bo‘lishi kerak:

1. Ketma-ketlikning davri juda katta bo‘lishi kerak (0 va 1 lardan tashkil topgan ketma-ketlik uchun taxminan  $10^{50}$ );

2.  $x_i$  ketma-ketlik oson generatsiya qilinishi kerak;

3.Ochiq va shifrmatnning bir qismini bilish (ochiq matnga asoslangan hujum) bevosita  $x_i$  ketma-ketlikni to‘liq tiklash mumkin bo‘lmassligi kerak.

### Chiziqli kongruent generator parametrlari

$(a, c, N)$	$(a, c, N)$	$(a, c, N)$
(106, 1283, 6075)	(625, 6571, 31104)	(1277, 24749, 117128)
(211, 1663, 7875)	(1541, 2957, 14000)	(2041, 25673, 121500)
(421, 1663, 7875)	(1741, 2731, 12960)	(2311, 25367, 120050)
(430, 2531, 11979)	(1291, 4621, 21870)	(1597, 51749, 244944)
(936, 1399, 6655)	(205, 29573, 139968)	(2661, 36979, 175000)
(1366, 1283, 6075)	(421, 17117, 81000)	(4081, 25673, 121500)
(171, 11213, 53125)	(1255, 6173, 29282)	(3661, 30809, 145800)
(859, 2531, 11979)	(281, 28411, 134456)	(3613, 45289, 214326)
(419, 6173, 29282)	(1093, 18257, 86436)	(1366, 150889, 714025)
(967, 3041, 14406)	(421, 54773, 259200)	(8121, 28411, 134456)
(141, 28411, 134456)	(1021, 24631, 116640)	(4561, 51349, 243000)

Chiziqli kongruent generator tashkil qilayotgan ketma-ketlikning davri katta bo‘lishi uchun ( $N$  ga teng bo‘lishi uchun) quyidagilar bajarilishi kerak:

- EKUB( $c, n$ )=1 bo‘lishi keerak;
- $a-1$  soni  $p$  tub soniga karra bo‘ladi, bunda  $p$  bevisita  $N$  ning tub bo‘luvchisi bo‘ladi;
- $N$  soni 4 ga karra bo‘lsa, unda  $a-1$  soni ham 4 ga karra bo‘ladi.

Shulardan kelib chiqqan holda quyidagi 1-jadvalda keltirilgan parametrlar taklif qilinadi.

Xususan, Microsoft Visual C++ dasturlash tiilida chiziqli kongruent generatori koeffisiyentlari quyidagicha qabul qilingan:

```
return (((holdrand = holdrand * 214013L + 2531011L) >> 16) & 0x7fff);
```

bu yerda boshlang‘ich qiymat bevosita tizim vaqtidan olinadi.

## 5. Chiziqsiz kongruent generator

Bu yerda quyidagi kirish parametrlari asosida:

$N$  – chekli maydon xarakteristikasini ifodalovchi son;

$d, a$  va  $c$  - o‘zgarmas musbat butun sonlar,  $x_0$  – boshlang‘ich qiymat; ketma-ketlikni tashkil etuvchi chiqish qiymatlari quyidagi formula bilan aniqlanishi mumkin:  $x_{i+1}=(dx_i^2+ax_i+c) \bmod N$ , bu yerda  $i=0,1,2,\dots$ .

Bu generator kvadratik kongruent generator deb ham ataladi.

Ushbu jarayonni umumlashtirib quydagilarni taklif qilish mumkin:

Kub darajali kongruent generator:

$$x_{i+1} = (ax_i^3 + bx_i^2 + cx_i + d) \bmod N,$$

r darajali polinomial kongruent generator:

$$x_{i+1} = (a_r x_i^r + a_{r-1} x_i^{r-1} + \dots + a_1 x_i + d) \bmod N, \quad N \geq 1.$$

Chiziqsiz kongruent generatorlarga nisbatan chiziqli kongruent generatorlar oddiyligi va tezkorligi bilan ajralib turadi. Ammo bu formulalarni kriptografiyada qo'llash tavsiya etilmaydi. Chunki ushbu ketma-ketliklarning bir necha qiymati ma'lum bo'lsa, unda generator parametrlarini qisqa vaqt mobaynida tiklash mumkin bo'ladi.

## 6. Additiv psevdotasodifiy ketma-ketliklar generatori

Chiziqli kongruent generatorni murakkablashtirishda oldingi ikki qiymatni inobatga olish mumkin. Masalan,  $X_{n+1}$  qiymatini hisoblashda  $X_n$  va  $X_{n-1}$  larning chiziqli kombinatsiyasini kiritish mumkin. Bunda ketma-ketlikning uzunligi ko'pi bilan  $N^2$  ga teng bo'lishi mumkin, chunki ketma-ketlikning takrorlanishi quyidagini ( $X_{n+k}, X_{n+k+1}$ ) = ( $X_n, X_{n+1}$ ) bajarilishi bilan boshlanadi. Misol sifatida Fibonachchi ketma-ketligini keltirish mumkin:

$$X_{n+1} = (X_n + X_{n-1}) \bmod N.$$

Ushbu generator 1950-yillarda ishlab chiqilgan bo'lib, asosan davriyili  $N$  dan katta bo'ladi. Ammo bunday sonlarda tasodifiylik yetarli darajada emas. Fibonachchi ketma-ketligini quyidagicha umumlashtirish mumkin:

$$X_{n+1} = (X_{n-k} + X_{n-j}) \bmod N, \quad j > k \geq 1.$$

1958-yilda J. J.Mitchel va D.F.Mur umumlashtirilgan formulaning quyidagi shaklini taklif qilishdilar:

$$X_n = (X_{n-24} + X_{n-55}) \bmod N, \quad n \geq 55.$$

Bu yerda  $N$  – juft son,  $X_0, \dots, X_{54}$  – istalgan butun sonlar.

Bunday sonlar ketma-ketligi kechikuvchi Fibonachchi ketma-ketligi deb nomlanadi va parametrlar  $k$  va  $j$  kechikuvchi deyiladi.

## 7. Siljитish registrlariga asoslangan generatorlar

Hozirgi paytgacha taklif etilgan va muvaffaqiyatli ravishda ishlatilib kelinayotgan uzlusiz shifrlash algoritmlarining asosini siljitish registrlari yoki aniq qilib aytganda teskari chiziqli bog‘lanishli siljitish registrlari tashkil qiladi.

Bu yerdagи tushunchalarga to‘xtalib o‘tamiz.

Siljitish registri – tartiblangan bitlar to‘plami bo‘lib, unda bitlarni bitta xonaga chapga yoki o‘ngga siljitish amali o‘rinlidir.

Teskari chiziqli bog‘lanishli siljitish registrlari (TCBSR) – bitli so‘zлarni siljitish registri bo‘lib, undagi chiqishda hosil qilingan bit bevosita boshqa bitlardan tashkil topgan chiziqli funksiya qiymatidir. Ushbu bit nolinchi razryadga kiritiladi. Razryadlar soni  $p$  registrning uzunligi deb ataladi.

Quyidagi tenglikni  $X_{n+N} = X_n$  barcha  $n$  uchun qanoatlantiruvchi eng kichik musbat  $N$  soni ketma-ketlikning davri hisoblanadi. Ushbu ketma-ketlik  $M$  ketma-ketlik deb nomланади, agarda uning davri  $(2^p - 1)$  ga teng bo‘lsa. Bu yerda ‘ $M$ ’ harfi “maximum” so‘zidan olingan.

Bunday teskari bog‘lanishli siljitish registrlarini bevosita uzlusiz shifrlash algoritmlarida ommaviy qo‘llanilishiga ikki sababni ko‘rsatish mumkin:

1. Teskari bog‘lanishli siljitish registrlariga asoslangan generatorlar hosil qilgan ketma-ketliklar yaxshi tasodifiylik statistik xarakteristikalarini beradi;
2. Siljitish registrlariga asoslangan generatorlarning xossalariни tahlil qilish oson.

Teskari chiziqsiz bog‘lanishli siljitish registrlari ham ishlab chiqilgan bo‘lib, undagi chiziqsiz funksiya, masalan, quyidagi shaklda bo‘lishi mumkin

$$f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_2 x_3 x_4 .$$

Ushbu funksiyaning chiziqsizlik darajasi 3 ga teng.

## **8. Psevdotasodifiy ketma-ketliklarni testdan o‘tkazish**

Generatsiya qilingan sonlar ketma-ketligini tasodifiylikka tekshirishda ko‘plab algoritmlar mavjud bo‘lib, ular asosida maxsus dasturiy ishlanmalar yaratilgan. Ulardan quyidagi testlar keng tarqalgan: NIST STS, DIEHARD, CRYPT-X, D. Knut testlari va boshqalar.

Psevdotasodifiy ketma-ketliklar generatori orqali olingan sonlarni testdan o‘tkazish bevosita ularning kriptobardoshlik darajasini baholash mumkin bo‘ladi. Algoritmni oshkora qilmaslik generatorning kriptobardoshlikligini oshirish uchun yetarli hisoblanmaydi. Chunki maxsus usullar orqali taklif etilgan ketma-ketlikda mavjud va ko‘zga tashlanmaydigan qonuniyatlarni aniqlash mumkin bo‘ladi.

Kriptobardoshlikni tekshirish testlaridan biri – bu keyingi bit testi hisoblanadi. Unga binoan ma’lum bo‘lgan  $k$  ta tasodiy sonlar asosida  $k+1$  – bitni  $1/2$  dan ortiq ehtimoli bilan aniqlashda polinomial algoritm mavjud bo‘lmasligi bilan belgilanadi.

Shu bilan birga maxsus statistik testlar ham mavjud, masalan, DIEHARD yoki NIST. Internetda bunday testlar bilan <http://www.cacert.at/random/> manzilidan tanishish mumkin.

Psevdotasodifiy sonlarni NIST (Statistical Testing Suite of Random Number Generators yoki NIST STS) bilan tekshirishda 15 ta statistik testlardan o‘tkazadi. Bular quyida testlar:

1) Bitlar chastotasi testi (**The Frequency Monobit Test**) – ketma-ketlikdagi nollar va birlar sonlari nisbati hisoblanadi. Bunda nollar va birlar sonlari keskin farq qilsa, demak tasodifiylik buzilgan hisoblanadi. Testda taklif qilinadigan bitlar uzunligi 1000000 bo‘lishi kerak va har bir testdan o‘tish uchun 100 ta ketma-ketlik tahlil qilinadi.

2) Blok ichidagi chastotali test (**Test for Frequency within a Block**) – ketma-ketlik  $M$  uzunlikdagi bloklarga taqsimlanadi va  $M$  uzunli blokdagi birlar chastotasi taxminan  $M/2$  ga teng ekanligini tekshiriladi. Bunda ketma-ketlik uzunligi 100 dan ortiq va blok uzunligi 20 dan ortiq bo‘lishi kerak.

3) Seriyalar testi (**Runs Test**) – nollar va birlardan tashkil topgan seriyalarning umumiy soni, bunda seriya bu bir xil bitdan tashkil topgan uzlusiz ketma-ketlikdir.

Bunda ketma-ketlik uzunligi 100 dan ortiq bo‘lishi kerak.

4) Matritsaning rankli testi (**Random Binary Matrix Rank Test**) – bir xil uzunlikdagi qism qatorlar orasida chiziqli bog‘lanish tekshiriladi. Bunda  $32 \times 32$

bitli matritsalar tahlil qilinadi. Bitlar ketma-ketligi uzunligi 38912 dan ortiq bo‘lishi kerak, ya’ni kamida 38 ta matritsa tahlil uchun ajratib olinadi.

5) Spektral testi (Diskret Furye almashtirishi testi) – davriylikga tekshiriladi. Ushbu yondashuvning asosiy maqsadi takrorlanuvchi bloklarning mavjudligini aniqlashga qaratilgan. Buning uchun bitlar ketma-ketligi Furye formulasi orqali qayta ishlanadi va natijalar tahlil qilinadi, masalan, grafik chizmalarda takrorlanuvchi qismlar mavjudligi tekshiriladi.

6) Nodavriy shablon bilan taqqoslash testi (**Non-overlapping Template Matching Test**) – berilgan qism qatorning, ya’ni shablonning ketma-ketlikda nechta mavjudligi tekshiriladi. Shablonga mos qism ketma-ketlikda mavjudligi aniqlansa, unda tekshiruv bevosita mos kelgan qismdan keyingi bitdan davom ettiriladi.

7) Davriy shablon bilan taqqoslash testi (**Overlapping (Periodic) Template Matching Test**) – berilgan davriy qism qatorning, ya’ni davriy shablonning nechta mavjudligi tekshiriladi. Shablonga mos qism ketma-ketlikda mavjudligi aniqlansa, unda tekshiruv bevosita keyingi bitdan davom ettiriladi.

8) Maurerning universal statistik testi (**Maurer's Universal Statistical Test**) – mos keladigan kombinatsiyalar orasidagi bitlar soni aniqlanadi. Ushbu qiymatlar orqali bitlar ketma-ketligining qay darajada siqish mumkinligi tahlil qilinadi.

9) Lempel-Zivning kompleks testi (**Lempel-Ziv Complexity Test**) – bitlar ketma-ketligini qay darajada siqish mumkinligi aniqlanadi. Agar ketma-ketlik yuqori darajada siqilsa, unda ketma-ketlik tasodifiy deb hisoblanmaydi.

10) Chiziqli murakkablik testi (**Linear Feedback Shift Register**) – generatsiyalangan teskari bog‘lanishli registr uzunligi. Bu yerda bitlar ketma-ketligining chiziqli murakkabligi baholanadi, bunda ketma-ketlik bevosita LFSR-ketma-ketlik sifatida qaraladi. Tasodifiy ketma-ketlikda teskari chiziqli bog‘lanishli siljitish registrlari bevosita uzunligi bilan ajralib turadi. Agar registr uzunligi kichik bo‘lsa, unda ketma-ketlik tasodifiy bo‘lmaydi.

11) Seriyali test (**The Serial Test**) – ketma-ketlikda barcha  $m$ -bitli kombinatsiyalar chastotasi aniqlanadi. Tasodifyi ketma-ketlikda  $m$ -bitli barcha shablonlar ehtimoli teng bo‘lishi asos qilib olingan.

12) Taxminiy entropiya testi (**The Approximate Entropy Test**) - ketma-ketlikda barcha  $m$ -bitli kombinatsiyalar chastotasi aniqlanadi.  $m$ -bitli blok chastotasi bilan u bilan kesishgan  $m+1$ -bitli blok chastotasi bevosita tasodifyi ketma-ketlikda aynan shunday bloklar chastotasi bilan taqqoslanadi.

13) Jamlangan summa testi (**The Cumulative Sums Test**) – berilgan ketma-ketlikdan qism ketma-ketliklar yig‘indisi hisoblanadi. Olingan natijalar tasodifyi ketma-ketlikda aynan shunday bloklar yig‘indisi bilan taqqoslanadi. Agar ketma-ketlikmi  $-1$  va  $+1$  lardan tashkil topgan deb qabul qilsak, unda istalgan tasodifyi qism ketma-ketlikda yig‘indi nolga yaqin bo‘ladi.

14) Tasodifyi farqlanish testi (**The Random Excursions Test**) – qandaydir holatning paydo bo‘lish soni bevosita tasodifyi ketma-ketlik uchun kutiladigan natijaga tengligi taqqoslanadi.

15) Qo‘sishmcha tasodifyi farqlanish testi (**The Random Excursions Variant Test**) – har xil holatlarning paydo bo‘lish sonining bevosita tasodifyi ketma-ketlik uchun kutiladigan natija bilan farqi aniqlanadi.

Shunday qilib, yuqorida ko‘rib o‘tilgan generatorlar qabul qilingan testlardan har xil darajada qoniqarli o‘tishlari mumkin, ammo keng foydalananadigan generatorlar testlardan mufaqqiyatli o‘ta ololmaydi.

## **9. Generator algoritmlarini amaliy qo‘llashga misollar**

Psevdotasodifyi ketma-ketlik generatorlarini 0 dan 9 gacha bo‘lgan raqamlarni tanlashda qo‘llanishni tahlil qilamiz. O‘tkaziladigan tajribalar sonini 20 bilan chegaralaymiz, ya’ni  $i=0,1,\dots,19$  bo‘ladi. Bu tajribalar soni qancha katta bo‘lda, natijalarni tahlil qilish shu darajada aniq bo‘ladi.

$x_{i+1} = (ax_i + c) \bmod N$				$x_{i+1} = (dx_i^2 + ax_i + c) \bmod N$			
$x_0=7, N=10, a=9, c=8$				$x_0=7, N=10, d=5, a=9, c=8$			
$i$	$xi$	$i$	$xi$	$i$	$xi$	$i$	$xi$
0	7	10	7	0	7	10	5

1	1	11	1	1	5	11	3
2	7	12	7	2	3	12	9
3	1	13	1	3	9	13	5
4	7	14	7	4	5	14	3
5	1	15	1	5	3	15	9
6	7	16	7	6	9	16	5
7	1	17	1	7	5	17	3
8	7	18	7	8	3	18	9
9	1	19	1	9	9	19	5

Keltirilgan natijaviy ketma-ketliklarning davrini aniqlashda quyidagi tenglikni  $X_{n+p} = X_n$  asos qilib olamiz. Birinchi misolda  $X_{n+2} = X_n$  barcha  $n$  uchun bajariladi, demak davr  $p = 2$  ga teng. Ikkinci misolda esa davr  $p = 3$  ga teng.

### Amaliy mashg‘ulot

**Mavzu:** Psevdotasodifiy sonlar generatorini va uning dasturiy ta’minotini yaratish.

**Ishdan maqsad:** Psevdotasodifiy sonlar generatorlari bilan bog ‘liq funksiyalar bilan tanishish va ular asosida dasturiy ta’mot ishlab chiqish:

- 1) Psevdotasodifiy sonlarni yaratish usulini tushunib olish;
- 2) Psevdotasodifiy sonlar generatorlarining kamchiliklarini o‘rganish;
- 3) Psevdotasodifiy sonlarni yaratish dasturini tuzish;
- 4) NIST dasturidan foydalangan ketma-ketliklarni tasodifiylikga tekshirish;
- 5) Bajarilgan ishlar asosida hisobotni shakllantirishni o‘rganish.

### Amaliy mashg‘ulot ishini bajarish tartibi

1. Nazariy ma’lumotlar bilan tarnishing.
2. Kompyuterni ishga tushiring.
3. Topshiriqlar ro‘yxatidan variantni tanlang.
4. Chiziqli kongruent generator bilan tanishing.
5. Chiziqli kongruent generator dasturini tuzing.
6. Natijaviy ketma-ketlikning davriyligini aniqlang va tahlil qiling .
7. Internetga kiring.

8. NIST dasturi bilan tarnishing.
9. Ma'lumotlar ketma-ketligini NIST dasturidan foydalanib tasodifiylikga tekshiring.
10. Bajarilgan ishlar bo'yicha hisobotlarni tayyorlang.
11. Hisobotni himoyaga tayyorlang.
12. Ishni tugating.

### **Hisobotni rasmiylashtirish tartibi**

1. Akademik jurnal bo'yicha variant tanlansin.
2. Hisobotning matn qismi standart o'lchamdagiga varaqlarga (A4 hajmida 210-297 mm) 1,5 intervalda Times New Roman 14 shriftida yozilishi lozim. Fayl formati MS Office 2003 bo'lsin.
3. Hisobotdagi jadvallar va rasmlar tartib bilan raqamlashtirilsin va nomlansin.
4. Matnda rasm va jadvalga izoh berilishi kerak.
5. Matn rasm va jadval bilan boshlanmasin.
6. Matn qismi titul varaqasi bilan boshlanadi va betlar ketma-ket sonlar bilan raqamlashtiriladi.
7. Hisobot o'qituvchining elekton manziliga «Kriptografiya guruh –№-AX 6-amaliy» mavzusi bilan jo'natilsin .
8. Hisobot yakuniy nazoratdan 5 kun oldin jo'natilishi kerak.
9. O'z vaqtida taqdim etilmagan hisobot baholanmaydi.

### **Amaliy mashg'ulotlari uchun variantlar**

#### **1-topshiriq**

Quyidagi formula bo'yicha chiziqli kongruent generatorini ketma-ketligini hisoblang:

$$x_{i+1} = x_i * a + c \pmod{N}$$

Olingan natijalarni tahlil qiling.

Variantlar

<b>№</b>	<b>x<sub>0</sub>, N,a,c</b>						
1	21,41,11,31	11	31,37,13,31	21	13,31,17,23	31	24,33,31,21

2	23,34,17,31	12	13,34,27,31	22	14,34,27,31	32	23,34,27,31
3	13,35,17,31	13	15,37,17,30	23	15,37,19,30	33	22,37,17,30
4	23,31,17,21	14	23,33,14,21	24	16,33,14,29	34	21,33,14,31
5	13,29,17,23	15	17,29,27,23	25	17,29,27,28	35	20,29,27,28
6	15,29,19,31	16	25,29,19,31	26	18,29,19,30	36	19,29,19,30
7	23,37,27,31	17	27,37,17,11	27	19,37,17,31	37	18,37,17,19
8	33,34,27,11	18	33,37,27,31	28	20,37,27,11	38	17,37,27,31
9	13,23,17,21	19	11,25,17,21	29	21,25,17,23	39	16,25,17,23
10	22,37,27,23	20	23,37,25,25	30	22,37,25,27	40	15,37,25,29

## 2-topshiriq

C++ dasturlash tilida chiziqli kongruent generatorini quyidagi formula bo‘yicha hisoblash dasturini tuzing:

$$((x_{i+1} = x_i * 214013L + 2531011L) >> 16) \& 0x7fff$$

Olingan natijalarни тahlil qiling va rand() funksiyasi bilan taqqoslang.

Variantlar

№	x <sub>0</sub>								
1	21411	11	23411	21	23011	31	13011	41	29011
2	21421	12	24421	22	24121	32	14121	42	28121
3	21431	13	25431	23	25331	33	15331	43	27331
4	21441	14	27441	24	27441	34	17441	44	26441
5	21451	15	29451	25	29551	35	19551	45	25551
6	21461	16	21461	26	21661	36	11661	46	24661
7	21471	17	23471	27	23771	37	13771	47	22771
8	21481	18	25481	28	25881	38	15881	48	23881
9	21491	19	27491	29	27991	39	17991	49	24991
10	21401	20	27401	30	27091	40	19991	50	24091

## **5.4. RC4 shifrlash algoritmi asosida ma'lumotni shifrlash va deshifrlash dasturini yaratish**

RC4 uzlusiz shifrlash algoritmi Ron Rivest tomonidan 1987 yilda yaratilgan va shuning uchun RC4 (Rivest Cipher 4, bu yerda “4” avlodni bildiradi) deb nomlangan.

RC4 algoritmi oqimli generator bo‘lib, o‘zgaruvchan uzunlikdagi kalitga asoslangan. RC4 algoritmi orqali yaratilgan psevdotasodifiy sonlar generatorlari blokli shifrlashga asoslan generatorlarga nisbatan tezroq ishlaydi. Shu bilan birga algoritm OFB sinfiga mansub, ya’ni hosil qilingan gamma bevosita ochiq matnga bog‘liq emas.

RSA Data Security kompaniyasining ma'lumotlariga qaraganda, chiziqli RC4 algoritmi differentsiyal va chiziqli kriptotahlillarga bardoshli hisoblanadi. RC4 algoritmi hosil qiladigan holatlar soni taxminan  $2^{1700}$  ta.

RC4 algoritmi oqimli shifrlash bo‘lib, psevdotasodifiy bitlarni generatsiya qilishga asoslangan. Generatorga kirish ma'lumoti sifatida kalit beriladi va chiqishda psevdotasodifiy bitlar olinadi. Bunda kalitning uzunligi 40 dan 2048 bitgacha bo‘lishi mumkin. Generatsiya qilingan bitlar bir tekis taqsimlangan bo‘ladi. RC4 algoritmining quyidagi afzalliklari e’tirof etilgan:

- yuqori tezligi;
- kalitning o‘zgaruvchan uzunligi.

RC4 algoritmi quyidagi vaziyatlarda mustahkam bo‘lmaydi:

- tasodifiy kalitlar qo‘llanilmasa;
- bitta kalit ikki marotaba qo‘llanilsa.

RC4 uzlusiz shifrlash algoritmi quyidagi tizimlarda keng foydalaniladi.

- |                                   |                              |
|-----------------------------------|------------------------------|
| • BitTorrent protocol encryption; | • SASL mechanism digest-MD5; |
| • WEP;                            | • RDP;                       |
| • MPPE;                           | • Kerberos;                  |
| • Opera Mini;                     | • PDF;                       |
| • SSL;                            | • Skype.                     |
| • SSH;                            |                              |

## 1. RC4 algoritmini amaliy qo'llashga misollar

Umumiy holda RC4 – bu algoritmlar sinfi bo‘lib, blok uzuni  $n$  parametri bilan belgilanadi. Odatda  $n=8$  ga teng deb olinadi. Algoritm bilan tanishish uhcun  $n=4$  variantini ko‘rib chiqamiz.

RC4 algoritmining mazmuni so‘zlardan iborat  $2^n$  o‘lchamli massiv va 2 ta hisoblagichdan iborat. Bu obyektlarning asosini so‘z tashkil qiladi.  $n=4$  bo‘lganda hisoblagichlar 4 bitli so‘z bo‘lib, ularni  $i$  va  $j$  deb belgilaymiz. Barcha jarayonlarda hisoblashlar  $2^n$  moduli bo‘yicha bajariladi. Kiritilgan massiv  $S$ -blok deb nomlanadi va almashtirish jadvali sifatida qo‘llaniladi va  $S$  deb belgilanadi.  $S$  jadvali har bir qadamda  $n$  bitli sonlarning har xil tartibidan tashkil topgan bo‘ladi. Ushbu o‘rin almashtirishlar tartibi kalit bilan belgilanadi. Jadvaldagagi har bir element qiymati 0 dan 15 gacha o‘zgaradi.

RC4 algoritmi ikki bosqichdan iborat. Birinchi bosqichda  $S$  jadvali shakllanadi, ikkinchi bosqichda esa tasodifiy sonlar hisoblanadi.

Jarayon boshlanishida  $S$  jadvali 0 dan 15 gacha bo‘lgan sonlar bilan to‘ldiriladi. Kalit esa 4 bitli sonlardan iborat bo‘ladi va  $2^n$  o‘lchamli  $K$  jadvalida joylashtiriladi. Agar kalit uzunligi yetarli bo‘lmasa, unda uni zarur bo‘lgancha takrorlash talab etiladi. Keyin quyidagi psevdokoddagi operatorlar bajariladi (1-algoritm):

1.  $j = 0; i = 0;$
2.  $j = (j + S_i + K_i) \text{ mod } 16;$
3.  $S_i$  va  $S_j$  o‘rnlari almashtiriladi;
4.  $i = i + 1;$
5. agar  $i < 16$  bo‘lsa, unda 2-bandga o‘tilsin;

Psevdokod bajarilishi natijasida boshlang‘ich  $S$  jadvali elementlari, maxviy kalit bilan bog‘liq ravishda, aralashtiriladi.

Shunday qilib,  $S$  jadvali shakllantirildi, endi  $n$ -bitli psevdotasodifiy sonlarni generatsiya qilishga o‘tish mumkin. Birinchi navbatda  $i$  va  $j$  hisoblagichlariga nol qiymati beriladi.

Keyingi bosqichda  $z_i$  qiymatini hisoblashda quyidagi psevdokod bajariladi (2-algoritm):

1.  $i = (i + 1) \bmod 16$ ;
2.  $j = (j + S_i) \bmod 16$ ;
3.  $S_i$  va  $S_j$  o'rnlari almashtiriladi;
4.  $a = (S_i + S_j) \bmod 16$ ;
5.  $z_i = S_a$ .

Natijaviy 4 bitli  $z_i$  qiymati bevosita navbatdagi 4 bitli blokni shifrlashda qo'llanishi mumkin. Misol sifatida aniq qiymatlar bilan ish yuritamiz. Masalan, maxfiy kalit 6 ta 4 bitli sonlardan iborat bo'lsin: 1, 2, 3, 4, 5, 6 (- bu sonlarning o'nlik ko'rinishi). Shular asosida RC4 algoritmi yordamida tasodifiy sonlar ketma-ketligini generatsiya qilamiz.

Birinchi qadamda  $S$  jadvalini 0 dan 15 gacha to'ldiramiz.

1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Keyingi qadamda  $K$  jadvalini kalit bilan to'ldiramiz, bu yerda kalitning uzunligi kichik bo'lganligi sababli, takroran yozib jadvalni to'ldiramiz:

2-jadval

$K$  kalit jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4

Endi  $S$  jadvalini 1-algoritmga binoan aralashtiramiz. Har bir qadamda olinadigan qiymatlarni jadvalga kiritib boramiz (3.x-jadvallari). Eslatib o'tamiz, qo'shish amali modul 16 bo'yicha bajariladi. Bu yerda algoritmning har bir 5-bandidan so'ng vaqtincha shakllangan  $S$  jadvalini kuzatib boramiz.

3.1-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo'yicha)	Yangi qiymati	
		$i$	$j$
1	$j = 0; i = 0$	0	
2	$j = j + S_i + K_i = 0 + 0 + 1 = 1$		1
3	$S_i$ va $S_j$ o'rnlari almashtiriladi, ya'ni $S_0$ va $S_1$		
4	$i = i + 1$	1	
5	$i < 16$ , demak 2-bandga o'tamiz		

Bajarilgan qadamdan so‘ng  $S$  jadvalining ko‘rinishi 3.1.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.1.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	0	2	3	4	5	6	7	8	9	10	11	12	13	14	15

RC4 algoritmini davom ettiramiz:

3.2-jadval. RC4 algoritmining birinchi bosqichi	
Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)
2	$j = j + S_i + K_i = 1 + 1 + 1 = 3$
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S1 va S3
4	$i = i + 1$
5	$i < 16$ , demak 2-bandga o‘tamiz

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.2.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.2.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	2	0	4	5	6	7	8	9	10	11	12	13	14	15

RC4 algoritmini davom ettiramiz:

3.3-jadval. RC4 algoritmining birinchi bosqichi	
Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)
2	$j = (j + S_i + K_i) \bmod 16 = (3 + 2 + 3) \bmod 16 = 8$
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S2 и S8
4	$i = i + 1$
5	$i < 16$ , demak 2-bandga o‘tamiz

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.3.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.3.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	<b>8</b>	0	4	5	6	7	<b>2</b>	9	10	11	12	13	14	15

RC4 algoritmini davom ettiramiz:

3.4-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	Yangi qiymati	
		$i$	$j$
2	$j = (j + Si + Ki) \text{ mod } 16 = (8 + 0 + 4) \text{ mod } 16 = 12$		12
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S3 va S12		
4	$i = i + 1$	4	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Ushbu qadamdan so‘ng  $S$  jadvalining ko‘rinishi 3.4.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.4.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	<b>12</b>	4	5	6	7	2	9	10	11	<b>0</b>	13	14	15

RC4 algoritmini davom ettiramiz:

3.5-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	Yangi qiymati	
		$i$	$j$
2	$j = (j + Si + Ki) \text{ mod } 16 = (12 + 4 + 5) \text{ mod } 16 = 5$		5
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S4 va S5		
4	$i = i + 1$	5	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.5.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.5.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	12	<b>5</b>	<b>4</b>	6	7	2	9	10	11	0	13	14	15

RC4 algoritmini davom ettiramiz:

3.6-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	i ning yangi qiymati	j ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (5 + 4 + 6) \text{ mod } 16 = 15$		15
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S5 va S15		
4	$i = i + 1$	6	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan qadamdan so‘ng  $S$  jadvalining ko‘rinishi 3.6.1-jadvalida keltirilgan.

Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.6.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	12	5	<b>15</b>	6	7	2	9	10	11	0	13	14	<b>4</b>

RC4 algoritmini davom ettiramiz:

3.7-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	i ning yangi qiymati	j ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (15 + 6 + 1) \text{ mod } 16 = 6$		6
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S6 va S6		
4	$i = i + 1$	7	
5	$i < 16$ , demak 2-bandga o‘tamiz		

E'tibor bering,  $i=j$  bo'lganligi sababli  $S$  jadvali o'zgarmaydi. Bajarilgan hisoblashlardan so'ng  $S$  jadvalining ko'rinishi 3.7.1-jadvalida keltirilgan.

### 3.7.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	12	5	15	6	7	2	9	10	11	0	13	14	4

RC4 algoritmini davom ettiramiz:

3.8-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo'yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (6 + 7 + 2) \text{ mod } 16 = 15$		15
3	Si va Sj o'rnlari almashtiriladi, ya'ni S7 va S15		
4	$i = i + 1$	8	
5	$i < 16$ , demak 2-bandga o'tamiz		

Bajarilgan hisoblashlardan so'ng  $S$  jadvalining ko'rinishi 3.8.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko'rsatilgan.

### 3.8.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	12	5	15	6	<b>4</b>	2	9	10	11	0	13	14	<b>7</b>

RC4 algoritmini davom ettiramiz:

3.9-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo'yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (15 + 2 + 3) \text{ mod } 16 = 4$		4
3	Si va Sj o'rnlari almashtiriladi, ya'ni S8 va S4		
4	$i = i + 1$	9	
5	$i < 16$ , demak 2-bandga o'tamiz		

Bajarilgan qadamdan so‘ng  $S$  jadvalining ko‘rinishi 3.9.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.9.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	3	8	12	<b>2</b>	15	6	4	<b>5</b>	9	10	11	0	13	14	7

RC4 algoritmini davom ettiramiz:

3.10-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (4 + 9 + 4) \text{ mod } 16 = 1$		1
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S9 va S1		
4	$i = i + 1$	10	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.10.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.10.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	1	<b>9</b>	8	12	2	15	6	4	5	<b>3</b>	10	11	0	13	14	7

RC4 algoritmini davom ettiramiz:

3.11-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (1 + 10 + 5) \text{ mod } 16 = 0$		0
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S10 va S0		
4	$i = i + 1$	11	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.11.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.11.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	<b>10</b>	9	8	12	2	15	6	4	5	3	<b>1</b>	11	0	13	14	7

RC4 algoritmini davom ettiramiz:

3.12-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + S_i + K_i) \text{ mod } 16 = (0 + 11 + 6) \text{ mod } 16 = 1$		1
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S11 va S1		
4	$i = i + 1$	12	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.12.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.12.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	<b>11</b>	8	12	2	15	6	4	5	3	1	<b>9</b>	0	13	14	7

RC4 algoritmini davom ettiramiz:

3.13-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + S_i + K_i) \text{ mod } 16 = (1 + 0 + 1) \text{ mod } 16 = 2$		2
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S12 va S2		
4	$i = i + 1$	13	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.13.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.13.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	11	<b>0</b>	12	2	15	6	4	5	3	1	9	<b>8</b>	13	14	7

RC4 algoritmini davom ettiramiz:

3.14-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	$i$ ning yangi qiymati	$j$ ning yangi qiymati
2	$j = (j + Si + Ki) \text{ mod } 16 = (2 + 13 + 2) \text{ mod } 16 = 1$		1
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S13 va S1		
4	$i = i + 1$	14	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.14.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.14.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	<b>13</b>	0	12	2	15	6	4	5	3	1	9	8	<b>11</b>	14	7

RC4 algoritmini davom ettiramiz:

3.15-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	Yangi qiymati	
		$i$	$j$
2	$j = (j + Si + Ki) \text{ mod } 16 = (1 + 14 + 3) \text{ mod } 16 = 2$		2
3	Si va Sj o‘rinlari almashtiriladi, ya’ni S14 va S2		
4	$i = i + 1$	15	
5	$i < 16$ , demak 2-bandga o‘tamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.15.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.15.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	13	<b>14</b>	12	2	15	6	4	5	3	1	9	8	11	<b>0</b>	7

RC4 algoritmini davom ettiramiz:

3.16-jadval. RC4 algoritmining birinchi bosqichi

Algoritm bandi	Bajariladigan operator ( mod 16 bo‘yicha)	Yangi qiymati	
		$i$	$j$
2	$j = (j + Si + Ki) \text{ mod } 16 = (2 + 7 + 4) \text{ mod } 16 = 13$		13
3	Si va Sj o‘rniali almashtiriladi, ya’ni S15 va S13		
4	$i = i + 1$	16	
5	$i < 16$ – bajarilmaydi, demak tugatamiz		

Bajarilgan hisoblashlardan so‘ng  $S$  jadvalining ko‘rinishi 3.16.1-jadvalida keltirilgan. Jadvalda almashtirilgan elementlar kattalashtirib va qalin qilib ko‘rsatilgan.

### 3.16.1-jadval

$S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	13	14	12	2	15	6	4	5	3	1	9	8	<b>7</b>	0	<b>11</b>

Sunday qilib, ushbu qadamlar bajarilgandan so‘ng  $S$  jadvali quyidagi natijaviy ko‘rinishda bo‘ladi:

### 4-jadval

Natijaviy  $S$  jadvali qiymatlari

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Qiymati	10	13	14	12	2	15	6	4	5	3	1	9	8	7	0	11

$S$  jadvali shakllanildi, endi tasodifiy 4 bitli sonlarni generatsiya qilishni boshlaymiz. Yuqorida keltirilgan 2-algoritm asosida psevdotasodifiy sonlarni 5 tasini generatsiya qilamiz (5-jadval).

5-jadval. RC4 algoritmining asosiy bosqichi  
(psevdotasodifiy sonlarni hisoblash)

	Bajariladigan operator ( mod 16 bo'yicha)	Yangi qiymati		
		<i>i</i>	<i>j</i>	<i>a</i>
z1 hisobi	1. $i = (i + 1) = 0+1=1$	1		
	2. $j = (j + Si) \text{ mod } 16 = (0+13) \text{ mod } 16 = 13$		13	
	3. o'rirlar almashtiriladi S1 va S13			
	4. $a = (Si + Sj) \text{ mod } 16 = (7+13) \text{ mod } 16 = 4$			4
	5. $z1 = S4 = 2$			
z2 hisobi	1. $i = (i + 1) = 1+1=2$	2		
	2. $j = (j + Si) \text{ mod } 16 = (13+14) \text{ mod } 16 = 11$		11	
	3. o'rirlar almashtiriladi S2 va S11			
	4. $a = (Si + Sj) \text{ mod } 16 = (9+14) \text{ mod } 16 = 7$			7
	5. $z2 = S7=4$			
z3 hisobi	1. $i = (i + 1) = 2+1=3$	3		
	2. $j = (j + Si) \text{ mod } 16 = (11+12) \text{ mod } 16 = 7$		7	
	3. o'rirlar almashtiriladi S3 va S7			
	4. $a = (Si + Sj) \text{ mod } 16 = (4+12) \text{ mod } 16 = 0$			0
	5. $z3 = S0=10$			
z4 hisobi	1. $i = (i + 1) = 3+1=4$	4		
	2. $j = (j + Si) \text{ mod } 16 = (7+2) \text{ mod } 16 = 9$		9	
	3. o'rirlar almashtiriladi S4 va S9			
	4. $a = (Si + Sj) \text{ mod } 16 = (3+2) \text{ mod } 16 = 5$			5
	5. $z4 = S5=15$			
z5 hisobi	1. $i = (i + 1) = 4+1=5$	5		
	2. $j = (j + Si) \text{ mod } 16 = (9+15) \text{ mod } 16 = 8$		8	
	3. o'rirlar almashtiriladi S5 va S8			
	4. $a = (Si + Sj) \text{ mod } 16 = (5+15) \text{ mod } 16 = 4$			4
	5. $z5 = S4 = 3$			

Natijada quyidagi sonlar olindi: 2, 4, 10, 15, 3. Ushbu jarayonni davom ettirib psevdotasodifiy sonlarni hisoblash mumkin. Demak,  $n=4$  bo‘lganda psevdotasodifiy sonlar ham 4 bitli bo‘ladi, ya’ni 0 dan 15 ga o‘zgaradi. Umumiy holda  $n$  ning qiymati 8 yoki 16 ga teng bo‘lishi mumkin. Masalan, agar  $n=8$  bo‘lsa, unda  $S$  jadvali  $2^8=256$  qiymatlari bo‘ladi va 0 dan 255 gacha o‘zgaradi. Hisoblagichlar  $i$  va  $j$  ham 8 bitli bo‘ladi. Bularidan tashqari  $n=8$  bo‘lganda hisoblar modul 256 bo‘yicha amalgalashtiriladi.

### **Amaliy mashg‘ulot**

**Mavzu: RC4 shifrlash algoritmi asosida ma’lumotni shifrlash va deshifrlash dasturini yaratish.**

**Ishdan maqsad:** RC4 algoritmi asosida psevdotasodifiy sonlar generatorlari bilan bog‘liq amallar bilan tanishish va ular asosida dasturiy ta’minot ishlab chiqish:

- 1) Psevdotasodifiy sonlarni yaratish usulini tushunib olish;
- 2) Psevdotasodifiy sonlar generatorlarining kamchiliklarini o‘rganish;
- 3) Psevdotasodifiy sonlarni yaratish dasturini tuzish;
- 4) Yaratilgan dasturdan foydalanib har xil ketma-ketliklarni tashkil qilishni o‘rganish;
- 5) Bajarilgan ishlar asosida hisobotni shakllantirishni o‘rganish.

### **Amaliy mashg‘ulot ishini bajarish tartibi**

- 1.Nazariy ma’lumotlar bilan tarnishing.
- 2.Kompyuterni ishga tushiring.
- 3.Topshiriqlar ro‘yxatidan variantni tanlang.
- 4.RC4 algoritmi bilan tanishing.
- 5.RC4 algoritmidagi generator dasturini tuzing.
- 6.Natijaviy ketma-ketlikning davriyligini aniqlang va tahlil qiling .
- 7.Internetga kiring.
- 8.NIST dasturi bilan tarnishing.
- 9.Ma’lumotlar ketma-ketligini NIST dasturidan foydalanib tasodifiylikga tekshiring.

10.Bajarilgan ishlar bo‘yicha hisobotlarni tayyorlang.

11.Hisobotni himoyaga tayyorlang.

12.Ishni tugating.

### **Hisobotni rasmiy lashtirish tartibi**

1.Akademik jurnal bo‘yicha variant tanlansin.

2.Hisobotning matn qismi standart o‘lchamdagи varaqlarga (A4 hajmida 210-297 mm) 1,5 intervalda Times New Roman 14 shriftida yozilishi lozim. Fayl formati .doc yoki .docx va .pdf bo‘lsin.

3.Hisobotdagi jadvallar va rasmlar tartib bilan raqamlashtirilsin va nomlansin.

4.Matnda rasm va jadvalga izoh berilishi kerak.

5.Matn rasm va jadval bilan boshlanmasin.

6.Matn qismi titul varaqasi bilan boshlanadi va betlar ketma-ket sonlar bilan raqamlashtiriladi.

7.Hisobot o‘qituvchining elektron manziliga «Kriptografiya guruh –№-AX 6-amaliy» mavzusi bilan jo‘natilsin .

8.Hisobot yakuniy nazoratdan 5 kun oldin jo‘natilishi kerak.

9.O‘z vaqtida taqdim etilmagan hisobot baholanmaydi.

### **Amaliy mashg‘ulotlari uchun variantlar**

#### **1-topshiriq**

Berilgan 6 ta 4 bitli maxfiy kalit sonlari asosida RC4 algoritmi yordamida 6 ta tasodifiy sonlar ketma-ketligini generatsiya qiling.

#### **Variantlar**

<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>
1	2,1,3,4,5,6	11	3,1,2,4,5,6	21	4,1,3,2,5,6	31	5,1,3,4,2,6
2	2,1,3,4,6,5	12	3,1,2,4,6,5	22	4,1,3,2,6,5	32	6,1,3,4,2,5
3	2,1,3,5,4,6	13	3,1,2,5,4,6	23	5,1,3,2,4,6	33	4,1,3,5,2,6
4	2,1,4,3,5,6	14	4,1,2,3,5,6	24	3,1,4,2,5,6	34	5,1,4,3,2,6
5	2,3,1,4,5,6	15	3,2,1,4,5,6	25	4,3,1,2,5,6	35	5,3,1,4,2,6
6	2,6,3,4,5,1	16	3,6,2,4,5,1	26	4,6,3,2,5,1	36	5,6,3,4,2,1
7	2,5,3,4,1,6	17	3,5,2,4,1,6	27	4,5,3,2,1,6	37	1,5,3,4,2,6
8	2,4,3,1,5,6	18	3,4,2,1,5,6	28	1,4,3,2,5,6	38	5,4,3,1,2,6
9	2,3,1,5,4,6	19	3,2,1,5,4,6	29	5,3,1,2,4,6	39	4,3,1,5,2,6
10	2,3,1,6,5,4	20	1,3,2,6,5,4	30	6,3,1,2,5,4	40	5,3,1,6,2,4

## **2-topshiriq**

1-topshiriqda hosil qilingan psevdotasodifiy bitlar asosida uch baytli ochiq so‘zni ASCII kodlaridan foydalanib shifrlang va deshifrlang.

Variantlar

<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>	<b>№</b>	<b>Kalit</b>
1	ONA	11	NON	21	OHA	31	HOH
2	Ona	12	Non	22	Она	32	Нон
3	OTA	13	MOY	23	OTA	33	МОЙ
4	Ota	14	Moy	24	Ота	34	Мой
5	OPA	15	MAY	25	ОПА	35	МАЙ
6	Opa	16	May	26	Опа	36	Май
7	AKA	17	NOK	27	AKA	37	НОК
8	Aka	18	Nok	28	Ака	38	Нок
9	UKA	19	ASR	29	УКА	39	ACP
10	Uka	20	Asr	30	Ука	40	Acp

### **5.5. OpenSSL kutubxonasidan foydalangan holda ma’lumotlarni xesh qiymatini hisoblash**

Kriptografiyada, xesh-funksiya deb ixtiyoriy uzunlikdagi (bitlar yoki baytlar birliklarida) ma’lumotni biror fiksirlangan (belgilangan) uzunlikdagi (bitlar yoki baytlar birliklariga) qiymatga o’tkazib beruvchi funksiyaga aytildi. Xesh funksiyalardan amalda statistik tajribalar o’tkazishda, mantiqiy qurilmalarni tekshirishda, ma’lumotlar bazasida tez qidirib topish algoritmlarini yaratishda va ma’lumotlar bazasidagi ma’lumotlarning butunligini tekshirishda foydalaniladi.

Xesh funksiya (ingl. hash function) deb, ixtiyoriy uzunlikdagi  $M$  ma’lumotni fiksirlangan uzunlikdagi  $h(M)=H$  qiymatga akslantirib beruvchi, oson hisoblanadigan bir tomonlama funksiyaga aytildi.

Xesh funksiya: “xesh qiymat”, “daydjest”, “barmoq izlari” deb ham ataladi.

Xesh funksiyaga nisbatan quyidagi talablar qo‘yiladi:

1. Ixtiyoriy uzunlikdagi matn uchun qo‘llab bo‘lishlik.
2. Chiqishda belgilangan uzunlikdagi qiymatni berishlik.
3. Ixtiyoriy berilgan  $x$  bo‘yicha  $h(x)$  oson hisoblanishlik.

4. Ixtiyoriy berilgan  $H$  bo'yicha  $h(x) = N$  tenglikdan  $x$  ni hisoblab topib bo'lmashlik. (Bir tomonlamalik xususiyati).

5. Olingan  $x$  va  $y \neq x$  matnlar uchun  $h(x) \neq h(y)$  munosabat o'rinni bo'lishi. (Kolliziyaga bardoshlilik xususiyati).

Demak, xesh qiymat yoki xabar daydjesti (ingl. message digest) – bu muayyan usul yordamida beriladigan bir tomonloma xesh-funksiya yordamida ma'lumotlarni qayta ishlash natijasi hisoblangan qayd etilgan uzunlikdagi belgilarning noyob ketma-ketligi.

Xeshlash algoritmi (ingl. Hashing algorithm) – chekli uzunlikdagi dastlabki ketma-ketligini qayd qilingan uzunlikdagi bitlarning ketma-ketligiga almashtiruvchi kriptografik algoritm.

Agar kolliziyalarni aniqlash murakkab bo'lsa, xesh-funksiya ziddiyatsiz hisoblanadi. Bu yerda kolliziya – bu ikki turli dastlabki ma'lumotlar uchun bir tomonlama funksianing qiymatlari teng bo'lgan voqeasi.

Bir tomonlama funksiya – bu berilgan  $x$  argument bo'yicha  $f(x)$  funksianing qiymatini hisoblash oson, lekin  $f(x)$  dan  $x$  ni aniqlash qiyin bo'lgan funksiya.

Xesh, xesh qiymat (ingl. hash, hash value) – bu ma'lumotlar ketma-ketligidan ishlab chiqariladigan va boshqa kirish ma'lumotlaridan xuddi shunday qiymatini hosil qilish ehtimoli kamayadigan tarzda generatsiyalanadigan son.

Xesh-kod – bu xesh-funksianing chiqish natijasi bo'lgan bitlar satri.

Xeshlash – bu xesh-funksiya qiymatini hisoblash jarayoni.

Xesh-funksiya (ingl. Hash function) – bu chekli uzunlikdagi bitlar satrini aniq qayd qilingan uzunlikdagi bitlar satriga o'zgartirish funksiyasidir. Asosan xesh qiymati 64 yoki 128 bitdan tashkil topgan bo'ladi.

Xesh-funksianing mazmun-mohiyati bevosita xesh-kodga asoslangan holda xesh-kodni hosil qiluvchi funksiya argumenti haqida qandaydir xulosa qilish. Masalan, ikkita massivning xesh-kodlari har xil bo'lsa, demak ushbu massivlar bir-biriga teng bo'lmaydi. Ammo, xesh-kodlari teng bo'lsa, bu massivlar ham teng ekanligini bildirmaydi. Chunki, umumiy holda xesh-kodlarning soni kiruvchi qiymatlar sonidan ancha kam bo'ladi. Shu bois, ikkita har xil kiruvchi qiymatlar

bitta xesh-kodga ega bo‘lishi mumkin, ya’ni kolliziya sodir bo‘ladi. Bunday holatning sodir bo‘lish ehtimoli bevosita xesh-funksiyani tahlil qilishda juda muhim ahamiyatga ega.

Eng oddiy xesh-funksiya sifatida quyidagini taklif qilish mumkin, masalan, berilgan belgilar qatoridagi har bir baytni Xor amali bilan qo‘shib chiqsak, natijada bir bayt olinadi. Natijada 8 bitli xesh-kod hosil bo‘ladi va kirish qatorining uzunligi qanday bo‘lishidan qat’iy nazar doimo bir bayt bo‘ladi. Masalan, quyidagi o‘n otilik qator berilgan bo‘lsin: 3E 54 A0 1F B4. Ushbu qatorni ikkilik ko‘rinishiga o‘tkazib, **Xor** bilan qo‘shamiz:

**0011 1110**

**0101 0100**

**1010 0000**

**0001 1111**

**1011 0100**

**0110 0101**

Bu yerdagi natija  $0110\ 0101_2$  yoki  $65_{16}$  xesh-kod bo‘ladi. Ammo bunday oddiy xesh-funksiyani kriptografiyada qo‘llash tavsiya etilmaydi. Shu bois xesh-funksiyaga quyidagi talablar qo‘yiladi:

- har qanday uzunlikdagi xabarga xesh-funksiyani qo‘llash mumkin bo‘lishi kerak;
- xesh-funksiyani hisoblash oz vaqt talab qilishi kerak;
- xesh-funksiya  $f(M)$  ma’lum bo‘lsa, uning argumentini  $M$  aniqlash murakkab bo‘lishi kerak;
- agar  $M$  ma’lum bo‘lsa, unda  $f(M)$  ga teng bo‘lgan boshqa  $M^*$  xabarni aniqlash murakkab masala bo‘lishi kerak;
- xesh-funksiyalari teng bo‘lgan tasodifiy ikki xabarning mavjudligini aniqlash murakkab masala bo‘lishi kerak.

Keltirilgan talablarga javob beradigan xesh-funksiyani yaratish murakkab masala hisoblanadi. Hozirgi kunda xabarni bloklarga taqsimlab, so‘ng bloklar bo‘yicha xesh-funksiyani hisoblash amalyotda taklif qilingan. Bunda har bir xabar

uchun  $M_i$  xesh-funksiya  $h_i$  quyidagicha hisoblanadi  $h_i = H(M_i, h_{i-1})$ . Natijada olingan  $h_n$  qiymati barcha bloklarga bog'liq bo'ladi.

## 1. MD5 xesh funksiyasi

MD5 algoritmida kiruvchi ma'lumot uzunligi ixtiyoriy bo'lib, xesh qiymat uzunligi 128 bit bo'ladi. MD5 xesh funksiyasi algoritmida kiruvchi ma'lumot 512 bitlik bloklarga ajratilib, ular 16 ta 32 bitlik qism bloklarga ajratiladi va bular ustida amallar bajariladi.

MD5 algoritmda "so'z" tushunchasi sifatida 32 bitli ma'lumot deb qabul qilinadi. Algoritmda boshiga kirish ma'lumotlar oqimi  $N$  bitdan iborat bo'lib, ularni qadamba-qadam qayta ishlab xesh-kod tashkil qilinadi. Barcha qadamlar bilan tanishamiz.

### 1-qadam: oqimni to'ldirish.

Oqimni to'ldirishda bevosita oqim oxirida 1 va nollar qo'shiladi. Bunda hosil qilingan oqim uzunligi  $512*n+448$  ga, ya'ni 512 moduli bo'yicha 448 ga teng bo'lishi kerak. Oqim uzunligi ushbu shartni bajargan holda ham, oqimni to'ldirish bari-bir amalga oshiriladi.

### 2-qadam: uzunlikni oshirish.

Boshlang'ich qator uzunligining ikkilik ko'rinishi qator oxiridan qo'shiladi va 64 bitli son shaklida yoziladi. Bunda 64 bitli son ikki 32 bitli "so'z" ga ajratiladi va ular o'rnlari bilan almashtiriladi. Natijada tashkil qilingan bitlar oqimi uzunligi 32 bitli "so'z" lardan tashkil etilgan bo'ladi va ular 16 soniga karrali bo'ladi, Keyinchalik bajariladigan hisoblashlar uchun  $N$  ta so'zdan tashkil topgan  $A[0...N-1]$  massivi qo'llaniladi.

### 3-qadam: MD buferini to'ldirish.

Keyingi hisoblashlarda ma'lumotlarni buferda vaqtinchalik saqlash uchun 4 ta so'zlik uzunlikdagi o'zgaruvchilar kiritiladi: A, B, C, D. O'zgaruvchilarining boshlang'ich qiymatlari quyidagicha qabul qilingan:

**A = 0x67452301**

**B = 0xEFCDAB89**

**C = 0x98BADCFE**

**D = 0x10325476**

#### 4-qadam: 16 ta so‘zdan iborat blokni qayta ishlash.

Keyingi hisoblashlarda 3 ta so‘zli argumentdan iborat quyidagi funksiyalar kiritiladi va natija ham so‘z bo‘ladi:

$$F(x, y, z) = (x \wedge y) \vee (\neg x \wedge z)$$

$$G(x, y, z) = (x \wedge z) \vee (y \wedge \neg z)$$

$$H(x, y, z) = x \oplus y \oplus z$$

$$I(x, y, z) = y \oplus x \vee \neg z$$

Bu yerda « $\wedge$ » belgisi bit amali AND, « $\vee$ » belgisi bit amali OR, « $\oplus$ » belgisi bit amali XOR, « $\neg$ » belgisi bit amali NOT. Kiritilgan funksiyalarning haqiqiylik jadvali quyidaicha bo‘ladi:

1-jadval

F, G, H, I funksiyalari uchun haqiqiylik jadvali

x	y	z	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

x	y	z	G
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

x	y	z	H
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

x	y	z	I
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Ushbu qadamda quyidagi o‘zgarmas qiymatlar T[1...64] kerak bo‘ladi va ular

$$T[i] = [4294967296 * \text{abs}(\sin(i))]$$

formula asosida hisoblanadi, bu yerda  $[x]$  – bu  $x$  qiymatining butun qismi. Shu bilan birga  $X$  va  $Y$  so‘zlari uchun siklik surish  $X <<< Y$  amali kiritiladi. Keyingi bajariladigan jarayonlarni psevdokod shaklida keltiramiz:

// oqimni 16 ta so‘zdan iborat bloklarga taqsimlaymiz:

for i = 0 to N/16 - 1 do {

// i-blokni X[] massiviga kiritamiz

for j = 0 to 15 do

X[j] = M[i \* 16 + j]

// A, B, C, D qiymatlarini saqlaymiz

AA = A

BB = B

CC = C

DD = D

// 1-raund

// yozuv [abcd k s i] quyidagini anglatadi:

```

//      a = b + ((a + F(b, c, d) + X[k] + T[i]) <<< s)
// 16 ta amal bajariladi:
[ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
[ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
[ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]
// 2- raund
// yozuv [abcd k s i] quyidagini anglatadi
//      a = b + ((a + G(b, c, d) + X[k] + T[i]) <<<s)
// 16 ta amal bajariladi:
[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]
// 3- raund
// yozuv [abcd k s i] quyidagini anglatadi
//      a = b + ((a + H(b, c, d) + X[k] + T[i]) <<< s)
// 16 ta amali bajariladi:
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]
// 4-raund
// yozuv [abcd k s i] quyidagini anglatadi
//      a = b + ((a + I(b, c, d) + X[k] + T[i]) <<< s)
// 16 ta amali bajariladi:
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]
A = AA + A
B = BB + B
C = CC + C
D = DD + D
}

```

**5-qadam:** MD5 natijasi chop etiladi.

Olingan natija ABCD buferida saqlanadi, faqatgina teskari chiqarish talab etiladi, ya'ni md5hash=DCBA.

MD5 algoritmiga asoslangan on-line kalkulyatorlar ham mavjud bo'lib, ular quyidagi veb-saytlarda keltirilgan:

<http://crypt-online.ru/crypts/md5/>

<http://sitespy.ru/md5/>

<https://pr-cy.ru/md5/>

Quyida MD5 xesh funksiyasi orqali olingan natijalarga misollar keltirilgan:

1)MD5("md5") = 1bc29b36f623ba82aaf6724fd3b16718

2) Bitta bitga farq qiladigan matn bilan ularning natijalariga e'tibor bering:

`MD5("abc") = 900150983CD24FB0D6963F7D28E17F72`

`MD5("acc") = 1673448EE7064C989D02579C534F6B66`

## **2. Qisqartirilgan MD5 algoritmini amaliy qo'llashga misol**

Yuqorida keltirilgan jarayonni aniq misolda ko‘rib chiqamiz va quyidagi ‘ota’ qatorini kirish ma’lumotlari sifatida olamiz. ASCII jadvali asosida str=‘ota’ qatorni ikkilik sanoq tizimida  $010011110111010001100001_2$  va o‘n otilik sanoq tizimidagi shaklida yozamiz, ya’ni str= 4f 74 61. Umuman, keyingi yozuvlarni ixcham yozish uchun o‘n otilik sanoq tizimidan foydalanamiz, ammo hisoblashlar bitlar bilan amalga oshiriladi. Ko‘rildigan qatorning bitlardagi uzunligi Length = 24 ga teng. Bu sonni ham ikkilik sanoq tizimiga o‘tkazamiz,  $Length_2 = 11000_2$ . Bu bitlarni 64 gacha uzaytiramiz (ixcham shakli-000000000000000018<sub>16</sub>):

Birinchi va ikkinchi so‘zlarni o‘rnini bilan almashtiramiz va  $\text{Length}^{-1}$  deb belgilaymiz:

Endi dasturda qayta ishlanadigan 512 bitdan iborat M[] massivini shakllantiramiz va shu bilan X[] massivini aniqlaymiz, ya’ni str & 10...0 & Length<sup>-1</sup> :

<b>X[8] =</b>	<b>00000000000000000000000000000000</b>
<b>X[9] =</b>	<b>00000000000000000000000000000000</b>
<b>X[10] =</b>	<b>00000000000000000000000000000000</b>
<b>X[11] =</b>	<b>00000000000000000000000000000000</b>
<b>X[12] =</b>	<b>00000000000000000000000000000000</b>
<b>X[13] =</b>	<b>00000000000000000000000000000000</b>
<b>X[14] =</b>	<b>0000000000000000000000000000000011000</b>
<b>X[15] =</b>	<b>00000000000000000000000000000000</b>

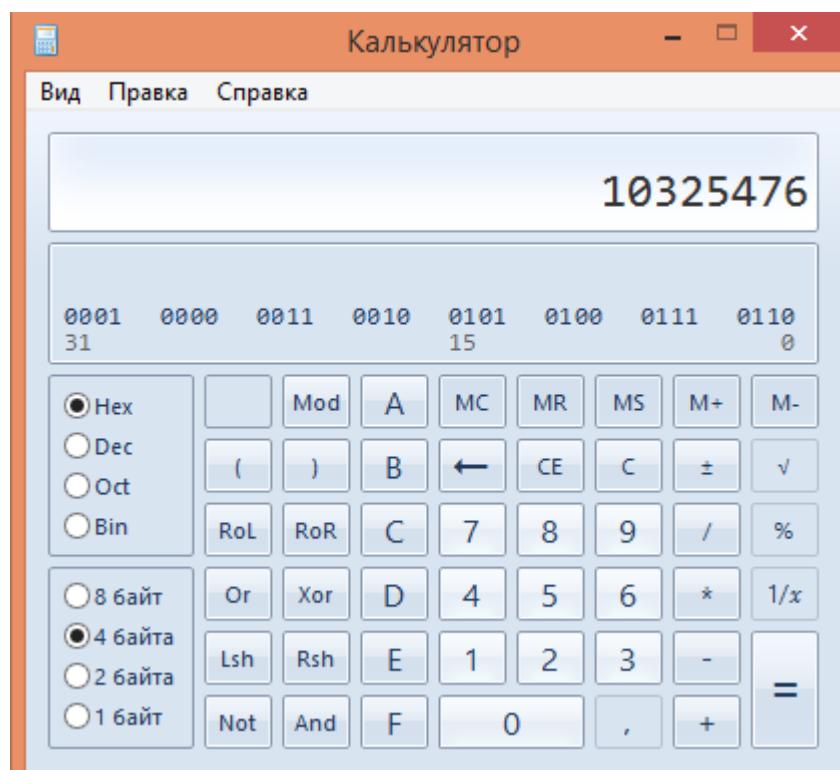
A, B, C, D qiymatlarini ikkilik tizimida yozamiz, bunda kalkulyatorning dasturlovchi (1-rasm) bandidan foydalanish mumkin:

$$\text{AA} = A = \text{0x67452301} = 01100111010001010010001100000001$$

$$\text{BB} = B = \text{0xEFCDAB89} = 1110111110011011010101110001001$$

$$\text{CC} = C = \text{0x98BADCCE} = 1001100010111010110111001111110$$

$$\text{DD} = D = \text{0x10325476} = 00010000001100100101010001110110$$



1-rasm. Kalkulyator

Hisoblashlarda zarur bo‘lgan T[i] massiv elementlarini MS Excel dasturidan foydalanim aniqlaymiz:

<b>i</b>	<b>T[i]</b>	<b>i</b>	<b>T[i]</b>	<b>i</b>	<b>T[i]</b>	<b>i</b>	<b>T[i]</b>
1	3614090360	17	4129170786	33	4294588738	49	4096336452
2	3905402710	18	3225465664	34	2272392833	50	1126891415
3	606105819	19	643717713	35	1839030562	51	2878612391
4	3250441966	20	3921069994	36	4259657740	52	4237533241
5	4118548399	21	3593408605	37	2763975236	53	1700485571
6	1200080426	22	38016083	38	1272893353	54	2399980690
7	2821735955	23	3634488961	39	4139469664	55	4293915773
8	4249261313	24	3889429448	40	3200236656	56	2240044497
9	1770035416	25	568446438	41	681279174	57	1873313359
10	2336552879	26	3275163606	42	3936430074	58	4264355552
11	4294925233	27	4107603335	43	3572445317	59	2734768916
12	2304563134	28	1163531501	44	76029189	60	1309151649
13	1804603682	29	2850285829	45	3654602809	61	4149444226
14	4254626195	30	4243563512	46	3873151461	62	3174756917
15	2792965006	31	1735328473	47	530742520	63	718787259
16	1236535329	32	2368359562	48	3299628645	64	3951481745

Endi 1-raundda keltirilgan hisoblashlarni bajaramiz va faqatgina birinchi qatoriga to‘xtalamiz. Yuqorida e’tirof etilganidek, [abcd k s i] yozuvi quyidagini anglatadi:

$$a = b + ((a + F(b, c, d) + X[k] + T[i]) \lll s) \quad (1*)$$

Algoritmda mavjud 16 ta amaldan faqatgina bittasini bajaramiz, ya’ni [ABCD 0 7 1]

Yuqoridagi (1\*) formula bo‘yicha [ABCD 0 7 1] yozuvi quyidagi ko‘rinishga ega bo‘ladi:

$$a = b + ((a + F(b, c, d) + X[0] + T[1]) \lll 7) \quad (1**)$$

Bu yerdagi  $F(b, c, d)$  funksiya qiymatini F, G, H, I funksiyalari uchun haqiqiylik jadvaliga asoslanib hisoblaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
b	<b>11101111100110110101110001001</b>
c	<b>1001100010111010110111001111110</b>
d	<b>00010000001100100101010001110110</b>
$F(b, c, d)$	<b>1001100010111010110111001111110</b>

Yuqoridagi (1\*\*) formula bo‘yicha hisoblashni jadval orqali amalga oshiramiz va qavsdan boshlaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
a	01100111010001010010001100000001
F(b, c, d)	100110001011101011011001111110
X[0]	01001111011101000110000110000000
T[3]	0010010000100000011000011011011
a+F(b,c,d)+X[0]+T[1]	0110011111000010011101000000111
(a+F(b,c,d)+X[0]+T[1])<<<7	11110000100111010000001110110011
b	11101111100110110101110001001
b+((a+F(b,c,d)+X[0]+T[3])<<<7)	00011111010100001010100000111010

**Izoh.** 1)  $T[1] = 3614090360$  soni ikkilik sanoq tizimiga o‘tkazilgan (1-rasm).

2) Qo‘shish amali **Xor** orqali amalga oshiriladi.

Demak,  $A = \text{00011111010100001010100000111010}$  ga teng bo‘ladi.

Endi 2-raundda keltirilgan hisoblashlarni bajaramiz va faqatgina birinchi qatoriga to‘xtalamiz. Yuqorida e’tirof etilganidek, [abcd k s i] yozuvini quyidagini anglatadi:

$$a = b + ((a + G(b, c, d) + X[k] + T[i]) <<< s) \quad (2*)$$

Algoritmda mavjud 16 ta amaldan faqatgina bittasini bajaramiz, ya’ni [DABC 6 9 18]. Yuqoridagi (2\*) formula bo‘yicha [DABC 6 9 18] yozuvini quyidagi ko‘rinishga ega bo‘ladi:

$$d = a + ((d + G(a, b, c) + X[6] + T[18]) <<< 9) \quad (2**)$$

Bu yerdagi  $G(a, b, c)$  funksiya qiymatini F, G, H, I funksiyalari uchun haqiqiylik jadvaliga asoslanib hisoblaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
a	<b>00011111010100001010100000111010</b>
b	<b>11101111100110110101110001001</b>
c	<b>1001100010111010110111001111110</b>
$G(a, b, c)$	<b>0111111010101011010101100111011</b>

Yuqoridagi (2\*\*) formula bo‘yicha hisoblashni jadval orqali amalga oshiramiz va qavsdan boshlaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
d	00010000001100100101010001110110
$G(a, b, c)$	01111110101010110101100111011
X[6]	00000000000000000000000000000000
T[18]	1100000001000001011001101000000
$d + G(a, b, c) + X[6] + T[18]$	10101111001001110100110000001101
$(d + G(a, b, c) + X[6] + T[18]) <<< 9$	01001110100110000001101101011110
a	00011111010100001010100000111010
$a + (d + G(a, b, c) + X[6] + T[18]) <<< 9$	01010001110010001011001101100100

**Izoh.** 1)  $T[18]=3225465664$  soni ikkilik sanoq tizimiga o'tkazilgan.  
 2) Qo'shish amali **Xor** orqali amalga oshiriladi.

Demak, **D = 01010001110010001011001101100100** ga teng bo'ladi.

Keyingi 3-raundda o'tamiz va unda keltirilgan hisoblashlarni bajaramiz. Bunda faqatgina birinchi qatorga to'xtalamiz. Yuqorida e'tirof etilganidek, [abcd k s i] yozuvi quyidagini anglatadi:

$$a = b + ((a + H(b, c, d) + X[k] + T[i]) <<< s) \quad (3^*)$$

Algoritmda mavjud 16 ta amaldan faqatgina bittasini bajaramiz, ya'ni [CDAB 11 16 35].

Yuqoridagi (3\*) formula bo'yicha [CDAB 11 16 35] yozuvi quyidagi ko'rinishga ega bo'ladi:

$$c = d + ((c + H(d, a, b) + X[11] + T[35]) <<< 16) \quad (3^{**})$$

Bu yerdagи H(d, a, b) funksiya qiymatini F, G, H, I funksiyalari uchun haqiqiylik jadvaliga asoslanib hisoblaymiz:

Jarayon	Qiymat
d	<b>01010001110010001011001101100100</b>
a	<b>00011111010100001010100000111010</b>
b	<b>11101111110011011010101110001001</b>
H(d, a, b)	<b>10100001010101011011000011010111</b>

Yuqoridagi (3\*\*) formula bo'yicha hisoblashni jadval orqali amalga oshiramiz va qavsdan boshlaymiz:

Jarayon	Qiymat
c	10011000101110101101110011111110
H(d, a, b)	10100001010101011011000011010111
X[11]	000000000000000000000000000000000000
T[35]	01101101100111010110000100100010
c + H(d, a, b) + X[11] + T[35]	01010100011100100000110100001011
(c+H(d,a,b)+X[11]+T[35])<<<16	00001101000010110101010001110010
d	01010001110010001011001101100100
d+((c+H(d,a,b)+X[11]+T[35])<<<16)	0101110011000011110011100010110

**Izoh.** 1)  $T[35]=1839030562$  soni ikkilik sanoq tizimiga o'tkazilgan. 2) Qo'shish amali **Xor** orqali amalga oshiriladi.

Demak, **C = 01011100110000111110011100010110** ga teng bo'ladi.

Endi 4-raundda keltirilgan hisoblashlarni bajaramiz va faqatgina birinchi qatoriga to‘xtalamiz. Yuqorida e’tirof etilganidek, [abcd k s i] yozuvi quyidagini anglatadi:

$$a = b + ((a + I(b, c, d) + X[5] + T[52]) \lll s) \quad (4*)$$

Algoritmda mavjud 16 ta amaldan faqatgina bittasini bajaramiz, ya’ni [BCDA 5 21 52].

Yuqoridagi (4\*) formula bo‘yicha [BCDA 5 21 52] yozuvi quyidagi ko‘rinishga ega bo‘ladi:

$$b = c + ((b + I(c, d, a) + X[5] + T[52]) \lll 21) \quad (4**)$$

Bu yerdagi I(c, d, a) funksiya qiymatini F, G, H, I funksiyalari uchun haqiqiylik jadvaliga asoslanib hisoblaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
c	<b>01011100110000111110011100010110</b>
d	<b>01010001110010001011001101100100</b>
a	<b>0001111010100001010100000111010</b>
I(c, d, a)	<b>000000100011100101110001111101</b>

Yuqoridagi (4\*\*) formula bo‘yicha hisoblashni jadval orqali amalga oshiramiz va qavsdan boshlaymiz:

<b>Jarayon</b>	<b>Qiymat</b>
b	11101111100110110101110001001
I(c, d, a)	10101101001001110100010010110011
X[5]	000000000000000000000000000000000000
T[52]	1111110010010011101000000111001
b + I(c, d, a) + X[5] + T[52]	10111110011110010100111100000011
(b + I(c, d, a)+X[5]+ T[52])<<<21	11100000011101111100111100101001
c	01011100110000111110011100010110
c+((b+I(c,d,a)+X[5]+T[52])<<<21)	10111100101101000010100000111111

**Izoh.** 1) T[52]= 4237533241 soni ikkilik sanoq tizimiga o‘tkazilgan. 2) Qo‘shish amali **Xor** orqali amalga oshiriladi.

Demak, **B = 10111100101101000010100000111111** ga teng bo‘ladi.

Shunday qilib, quyidagilarni hisoblash qoldi:

$$A = AA + A$$

$$B = BB + B$$

$$C = CC + C$$

$$D = DD + D$$

Jarayonni jadval shaklida bajaramiz:

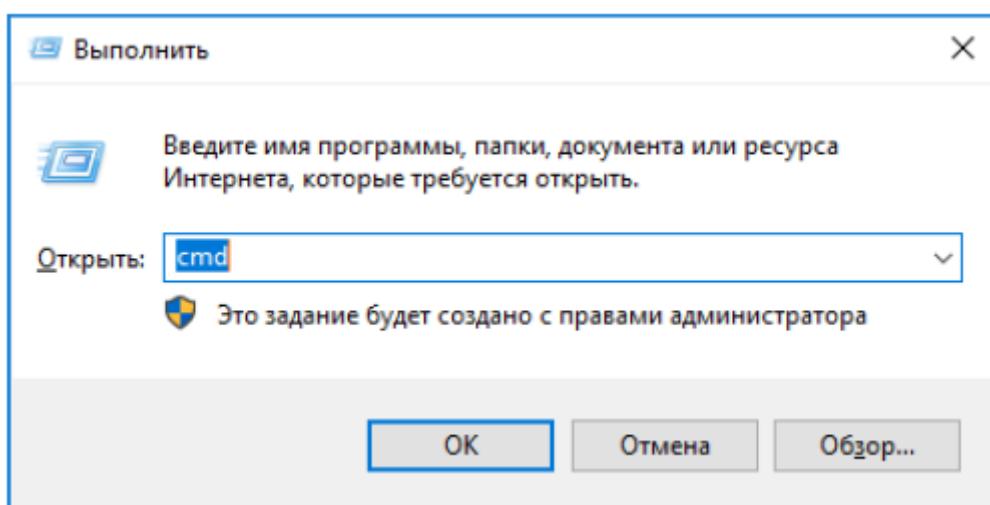
<b>Jarayon</b>	<b>Qiymat</b>	<b>a,b,c,d 16 lik tizimda</b>
AA	<b>01100111010001010010001100000001</b>	
A	<b>00011111010100001010100000111010</b>	
A=AA+A	<b>01111000000101011000101100111011</b>	78158B3B
BB	<b>11101111100110110101110001001</b>	
B	<b>10111100101101000010100000111111</b>	
B=BB+B	<b>0101001101110011000001110110110</b>	537983B6
CC	<b>100110001011101011011001111110</b>	
C	<b>01011100110000111110011100010110</b>	
C = CC + C	<b>11000100011110010011101111101000</b>	C4793BE8
DD	<b>00010000001100100101010001110110</b>	
D	<b>01010001110010001011001101100100</b>	
D = DD + D	<b>0100000111110101110011100010010</b>	41FAE712

Shunday qilib, natijaviy ABCD qiymatlarini teskari chiqarish orqali xesh-kod aniqlanadi: md5hash = DCBA = 41fae712c4793be8537983b678158b3b.

E'tibor bering, hisoblashlarda hattoki bitta bitda adashish barcha natijalarini chalkashtirib yuboradi.

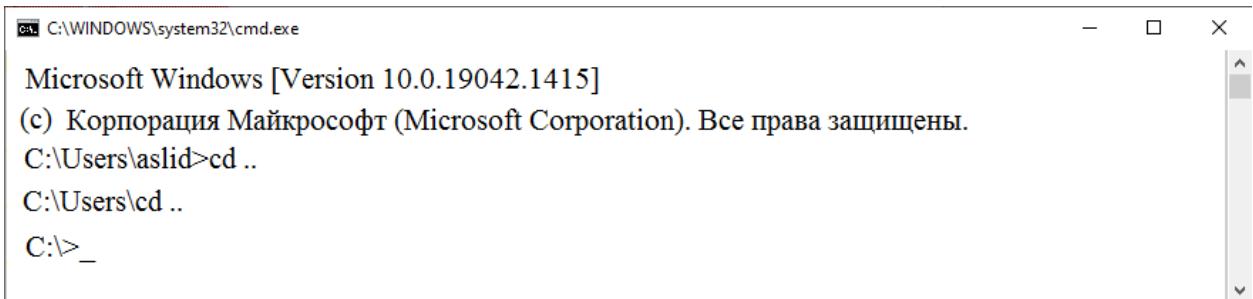
### 3.OpenSSL kutubxonasidan foydalanish

OpenSSL kutubxonasidan foydalanish uchun *cmd* buyrug'idan foydalaniladi



1-rasm. Cmd buyrug'ini ishga tushirilishi

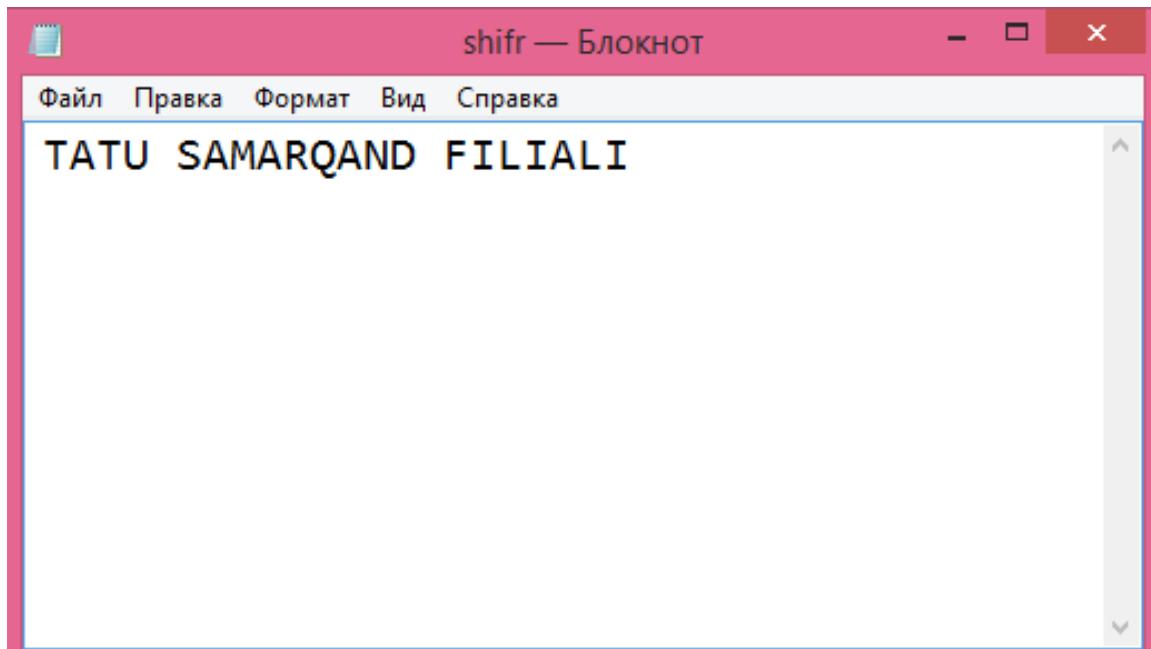
Cmd oynasidagi joriy papkasidan chiqish uchun *cd..* buyrug'idan foydalaniladi, masalan:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.1415]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\aslid>cd ..
C:\Users\cd ..
C:\>_
```

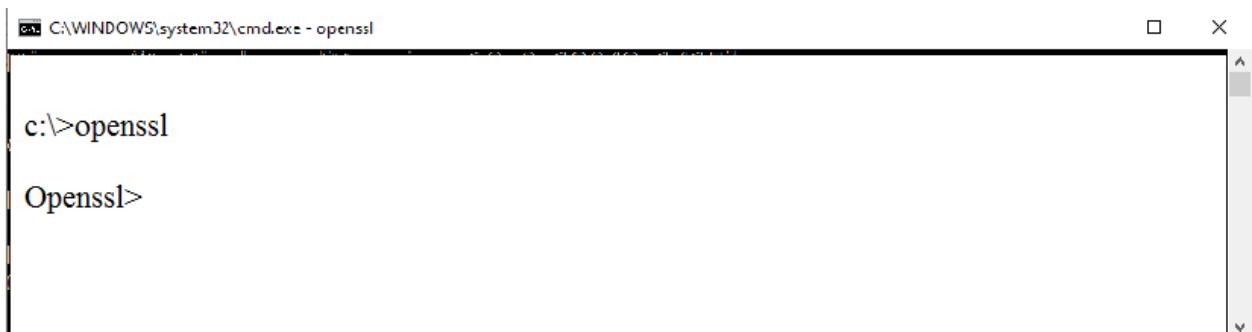
2-rasm. *cd..* buyrug‘idan foydalanish

OpenSSL kutubxonasi uchun foydalanadigan, masalan, *shifr\_md5* papkasiga *Блокном* dasturi orqali quyidagi ma’lumotni kiritib, faylda saqlaymiz:



3-rasm. Ochiq ma’lumot faylini yaratish

Openssl kutubxonasini faol holatga o’tkazish uchun quydagи *openssl* buyrug‘idan foydalaniladi:

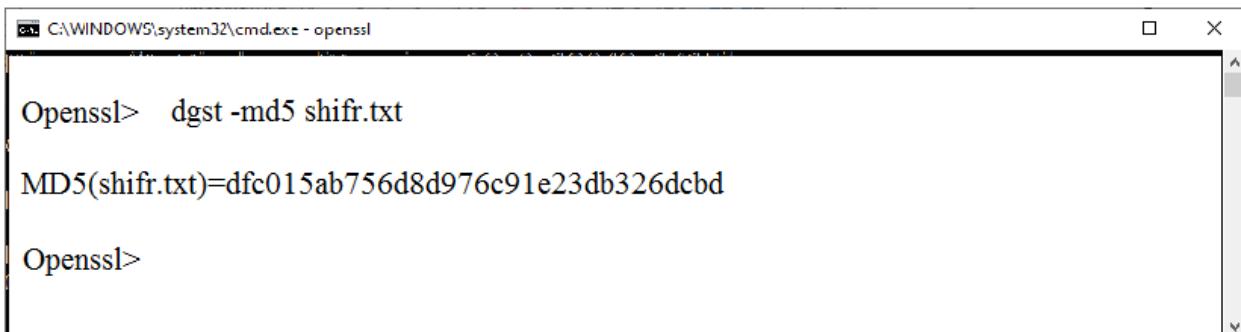


```
C:\WINDOWS\system32\cmd.exe - openssl
c:\>openssl
Openssl>
```

4-rasm. OpenSSL ni faollashtirish

Agar shu yerda *help* buyrug‘i kiritilsa, unda OpenSSL kutubxonasida mavjud funksiyalar ro‘yxati chiqariladi.

Ochiq ma'lumotni shifrlash uchun MD5 shifrlash algoritmidan foydalanish *dgst -md5 shifr.txt* buyrug'i orqali amalga oshiriladi. Natija esa quyidagicha bo'лади:



```
C:\WINDOWS\system32\cmd.exe - openssl
Openssl> dgst -md5 shifr.txt
MD5(shifr.txt)=dfc015ab756d8d976c91e23db326dcdb
Openssl>
```

5-rasm. OpenSSLda md5 ni qo'llash.

Shunday qilib, OpenSSL yordamida kiritilgan “TATU SAMARQAND FILIALI” qatorining xesh qiymati “dfc015ab756d8d976c91e23db326dcdb” aniqlanildi va olingan natija boshqa tizimlarda ham tekshirib ko'rildi.

### **Amaliy mashg'ulot**

**Mavzu: OpenSSL kutubxonasidan foydalangan holda ma'lumotlarni xesh qiymatini hisoblash.**

**Ishdan maqsad:** Xesh-funksiyalarni o'rganish orqali har xil shakldagi xesh-kodlarni tashkil qilish jarayonlarini o'rganish:

- 1) MD5 algoritmini o'rganish va qo'llaniladigan funksiyalarni tushunib olish;
- 2) Qisqartirilgan MD5 algoritmi bo'yicha hisob ishlarini bajarishni o'rganish;
- 3) SHA algoritmini tushunib olish;
- 4) Bajarilgan ishlar asosida hisobotni shakllantirishni o'rganish.
- 5) OpenSSL kutubxonasidan foydalangan holda MD5 algoritmini qo'llash buyruqlarini o'rganish.

### **Amaliy mashg'ulot ishini bajarish tartibi**

1. Nazariy ma'lumotlar bilan tarnishing.
2. Kompyuterni ishga tushiring.
3. Topshiriqlar ro'yxatidan variantni tanlang.
4. Eng oddiy xesh-funksiya bilan ishslash.
5. MD5 algoritmi bilan tanishing.

- 6.Qisqartirilgan MD5 algoritmi asosida hisoblarni amalga ohsiring.
- 7.Internetga kiring.
- 8.MD5 kalkulyatorlari bilan tarnishing.
- 9.Xesh-funksiyalarni amaliy dasturlarini tuzing.
- 10.Bajarilgan ishlar bo‘yicha hisobotlarni tayyorlang.
- 11.Hisobotni himoyaga tayyorlang.
- 12.Ishni tugating.

### **Hisobotni rasmiylashtirish tartibi**

- 1.Akademik jurnal bo‘yicha variant tanlansin.
- 2.Hisobotning matn qismi standart o‘lchamdagи varaqlarga (A4 hajmida 210-297 mm) 1,5 intervalda Times New Roman 14 shriftida yozilishi lozim. Fayl formati .doc yoki .docx va .pdf bo‘lsin.
- 3.Hisobotdagi jadvallar va rasmlar tartib bilan raqamlashtirilsin va nomlansin.
- 4.Matnda rasm va jadvalga izoh berilishi kerak.
- 5.Matn rasm va jadval bilan boshlanmasin.
- 6.Matn qismi titul varaqasi bilan boshlanadi va betlar ketma-ket sonlar bilan raqamlashtiriladi.
- 7.Hisobot o‘qituvchining elekton manziliga «Kriptografiya I –№-AX 1-lab» mavzusi bilan jo‘natilsin.
- 8.Hisobot yakuniy nazoratdan 5 kun oldin jo‘natilishi kerak.
- 9.O‘z vaqtida taqdim etilmagan hisobot baholanmaydi.

### **Amaliy mashg‘ulotlari uchun variantlar**

#### **1-topshiriq**

Eng oddiy xesh-funksiya orqali, ASCII jadvalidan foydalanib, berilgan belgilar qatorining 8 bitli xesh-kodini aniqlang.

#### **Variantlar**

<b>№</b>	<b>Qator</b>	<b>№</b>	<b>Qator</b>	<b>№</b>	<b>Qator</b>	<b>№</b>	<b>Qator</b>
1	DASTUR	11	XONA	21	BILIMLAR	31	AYIRMASI
2	SINF	12	TEST	22	DIREKTOR	32	BOSHQAR
3	QORA	13	SAHIFA	23	TIZIMLAR	33	MUHARRIR
4	VOSITA	14	TARMOQ	24	QIZIQCHI	34	TESTLASH
5	TAQINCHOQ	15	SAHIFA	25	RAQAMLAR	35	TARMOQLI

6	INSTITUT	16	ASKAR	26	SHAFTOLI	36	SAHIFASI
7	UNIVER	17	RAQAM	27	APPARAT	37	ASKARLAR
8	JAMLANMA	18	TIZIM	28	AYIRMA	38	BILIM
9	AXBOROT	19	STEGO	29	MATN	39	KODLAR
10	BUTUN	20	BETLAR	30	QATOR	40	KRIPTO

### 2-topshiriq

Oldingi 1-topshiriqda bajarilgan algoritm asosida eng oddiy xesh-funksiya dasturini tuzing va olingan natijalarni taqqoslang.

### 3-topshiriq

Qisqartirilgan MD5 algoritmidan foydalanib xesh-funksiya qiymatini aniqlang. Belgilarni kodlashda ASCII jadvalini qo'llang.

Variantlar

№	Qator	№	Qator	№	Qator	№	Qator
1	kompyuter	11	adobe	21	kitob	31	dasturlash
2	maxfiy	12	opera	22	jadval	32	python
3	shifrlash	13	internet	23	vektor	33	kitobxon
4	sinfosh	14	monitor	24	matriksa	34	pascal
5	axborotnama	15	printer	25	muammo	35	samarqand
6	virus	16	skaner	26	fizika	36	toshkent
7	antivirus	17	tarmoq	27	matematika	37	baxmal
8	windows	18	auditoriya	28	biologiya	38	buxoro
9	photoshop	19	sinfxona	29	adabiyot	39	guliston
10	microsoft	20	daftар	30	nashriyot	40	andijon

### 4-topshiriq

Oldingi 3-topshiriqda bajarilgan algoritm asosida qisqartirilgan MD5 algoritmi asosida tuzilgan dasturni o'rganing va natijalarni taqqoslang.

**Python tilidagi dastur kodi:**

```
import math
def decimalToBinary(n):
    return bin(n).replace("0b", "")
def wordToBinary(s):
    res = []
    for i in s:
        res.append(format(ord(i), '08b'))
    return ''.join(res)
def leftRotate(x, amount):
    x &= 0xFFFFFFFF
    return (x << amount | x >> (32-amount)) & 0xFFFFFFFF
def F(X, Y, Z):
    return ((X & Y) | ((~X) & Z))
```

```

def G(X, Y, Z):
    return ((X & Z) | (Y & (~Z)))
def H(X, Y, Z):
    return (X ^ Y ^ Z)
def I(X,Y,Z):
    return(Y ^ (X | (~Z)))
s = input()
string = wordToBinary(s)
length = len(string)
length_2 = decimalToBinary(length)
length_2_64_zeros = 64 - len(length_2)
for i in range(length_2_64_zeros):
    length_2 = "0" + length_2
length_minus_one = length_2[32:] + length_2[:32]
string = string + '1'
remaining_zeros = 512 - len(string) - len(length_minus_one)
for i in range(remaining_zeros):
    string = string + "0"
string = string + length_minus_one
X = []
for i in range(16):
    temp = string[32 * i : 32 * (i + 1)]
    X.append(temp)
T = []
for i in range(64):
    T.append(math.floor(4294967296 * abs(math.sin(i+1))))
for i in range(len(X)):
    X[i] = int(X[i], 2)
def md5_reduced(msg):
    A = 0x67452301
    B = 0xefcdab89
    C = 0x98badcfe
    D = 0x10325476
    a = A
    b = B
    c = C
    d = D
    a = b ^ leftRotate((a ^ F(b, c, d) ^ X[0] ^ T[0]), 7)
    d = a ^ leftRotate((d ^ G(a, b, c) ^ X[6] ^ T[17]), 9)
    c = d ^ leftRotate((c ^ H(d, a, b) ^ X[11] ^ T[34]), 16)
    b = c ^ leftRotate((b ^ I(c, d, a) ^ X[5] ^ T[51]), 21)
    A = A ^ a
    B = B ^ b
    C = C ^ c
    D = D ^ d

```

```
    result = "".join(str(hex(D))[2:] + str(hex(C))[2:] + str(hex(B))[2:] + str(hex(A))[2:])
    return result
print(md5_reduced(string))
```

## XULOSA

O‘zbekiston Respublikasi mustaqillik yillari axborotlashtirish sohasida inqilobiy o‘zgarishlar davrini boshdan kechirmoqda. Zamonaviy axborot-kommunikatsiya texnologiyalari qulayliklar yaratish bilan bir qatorda yangi muammolarni ham o‘rtaga qo‘ymoqda. Axborot bazalarida saqlanadigan va telekommunikatsiya tizimlarida aylanayotgan axborot xavfsizligiga tahdid keskin oshmoqda. Keyingi vaqtarda, ayniqsa, Internet paydo bo‘lgandan boshlab, axborot o‘g‘irlash, axborot mazmunini egasidan ruxsatsiz o‘zgartirib qo‘yish, tarmoq va serverlardan beruxsat foydalanish, tarmoqqa tajovuz qilish hollari dunyo miqyosida ko‘paydi.

Respublikamizda axborot texnologiyalarini rivojlantirishning aniq yo‘nalishlari belgilab berilib, bu soha mutaxassislariga faoliyat ko‘rsatish uchun shart-sharoitlar yaratilib berilmoqda. Ayniqsa, axborot xavfsizligini ta’minlash sohasida asosiy yo‘l bo‘lgan kriptografiya yo‘nalishini rivojlantirishga davlatimiz tomonidan ham katta ahamiyat berilmoqda. Xususan, 2007-yil 3-aprelda qabul qilgan “O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risidagi” PQ-614-sonli qaror shular jumlasidandir. Mazkur qarorning asosiy vazifalaridan biri axborotning kriptografik muhofazasi sohasida yuqori malakali kadrlarni tayyorlashdan iborat. Buning uchun kriptografiya yo‘nalishida milliy kadrlarni tayyorlashda o‘quv qo‘llanmalar, darsliklar va uslubiy qo‘llanmalar ishlab chiqish muhim ahamiyat kasb etadi.

Keyingi yillarda kriptografiya usullarining qo‘llanish sohalari faqatgina maxfiy sir hisoblangan ma’lumotlarga nisbatan emas, balkim Internet olamida mavjud barcha jarayonlarda o‘z aksini topmoqda. Shu bois, qo‘llanmada keltirilgan kriptografiya usullari bevosita misollarda ko‘rib chiqilgan. Ushbu sohaga mansub bo‘lgan manbalarda keltirilgan misollarni yoshlarimizga yetkazib berish uchun ular mantiqan bog‘liq mavzularga birlashtirildi. Qo‘llanmada keltirilgan masalalar sinchiklab o‘rganilgan bo‘lib, misollar bilan boyitilgan.

## Tayanch so‘zlar ko‘rsatkichi

Additiv .....	13	Gammalash .....	153
additiv usullar.....	127	gammalashtirish .....	127
al-Faraxidi.....	8	Gronsfeld usuli .....	99
Algoritmli generator.....	179	inversiya.....	47
al-Kindi .....	7	Jadvalli generator .....	179
Analitik .....	13	Kalkashandi .....	7
an-Nabati.....	7	Knapsack problem.....	122
Apparatli generator.....	179	kolliziya .....	210
aralash shifrlash.....	107	criptogramma .....	8
arifmetikaning asosiy teoremasi ....	33	Kriptomustahkamlik.....	9
ARX.....	161	kvadratik kongruent generator.....	185
bigramma .....	131	Mantiqiy qo‘shish.....	22
bir tomonlama funksiya.....	118	Mantiqiy inkor .....	24
birlik matritsa .....	57	Mantiqiy qo‘shishni inkor etish.....	22
Blokli shifrlash.....	161	matritsa .....	55
Bo‘linish xossalari.....	28	MD5.....	211
chiziqli bog‘langan.....	57	murakkab son .....	31
chiziqli bog‘lanmagan .....	57	nol matritsa .....	56
Chiziqli kongruent generator .....	182	Not amali .....	24
Chiziqsiz kongruent generator.....	186	NP-to‘liq .....	122
deshifrlash.....	11	o‘rin almashtirish .....	13,47,107
eng katta umumiyl bo‘luvchi .....	35	o‘rniga qo‘yish .....	13,48
eng kichik umumiyl bo‘linuvchi.....	36	o‘zaro tub sonlar.....	35
Eratosfen g‘alviri.....	31	Or amali .....	22
Fermaning kichik teoremasi .....	41	Psevdotasodify ketma-ketlik .....	178
Feystel tarmog‘i .....	161	Psevdotasodify sonlar generatori ..	177
Gamilton sikli.....	116	qo‘shimcha kod .....	20
gamma .....	127, 128	Qoldiqli bo‘lish haqidagi teorema ..	29

raund .....	161	Tasodifiy sonlar generatori .....	177
RLE.....	142	teskari kod.....	20
sanoq tizimi.....	14, 15	teskarilanuvchi .....	59
Sehrli kvadrat .....	115	Tetrada .....	19
shifr.....	9	transponirlangan matritsa .....	56
Shifr .....	9	transpozitsiya .....	48
Shifrlash.....	8	Triada .....	19
Shifrlash kaliti .....	9	tub son.....	31
Shifrllovchi jadval .....	109	umumiy karrali .....	36
shifrmatn .....	8	Vijiner jadvali .....	101
sikl .....	49	Vijiner tizimi .....	101
siklning uzunligi.....	50	Xaffman .....	143
Skrembler.....	155	xesh-funksiya .....	209
Skremblerlash .....	154	Xeshlash algoritmi .....	209
taqqoslama .....	40	Xill usuli .....	136
taqqoslanuvchi .....	39	Xor amali .....	22
Tasodifiy son.....	177	Yevklid algoritmi .....	35

## Foydalanilgan adabiyotlar ro‘yxati

1. Akbarov D.Y. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi.- Toshkent, «O‘zbekiston markasi» nashriyoti, 2009-432 bet.
2. Aripov A.N., Mirzaxidov X.M., Shermatov Sh.X., Saidxodjayev S.R., Hasanov P.F., Amirov D.M., Bakirov O.A. Axborot – kommunikatsiya texnologiyalari. Izohli lug‘at. Toshkent-2004.-499 bet.
3. Buyuk ajdodlarimiz / nashrga tayyorlovchi va mas’ul muharrirlar: M.Aminov, F.Hasanov. – T.: «O‘zbekiston milliy ensiklopediyasi» Davlat ilmiy nashriyoti, 2010. – 208 bet.
4. Axborot xavfsizligiga oid aatamalarning ruscha-o‘zbekcha izohli lug‘ati. 2-nashr. X.P.Xasanovning umumiy tahriri ostida. Toshkent, 2016. – 733 bet.
5. Kurosh A.G. Oliy algebra kursi. Ruschadan tarjima. – T.: ”O‘qituvchi“, 1976. – 461 bet.
6. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, 1. U. Xolimtayeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. T.: «Aloqachi», 2019, – 192 bet.
7. R.H.Ayupov, A.V.Kabulov. Kriptografiya va kriptovalyutalar. T.: M.Ulug‘bek nomidagi O‘zMU, 2018. – 144 bet.
8. Романьков В.А. Введение в криптографию . Курс лекций / В.А. Романьков. – 2 – е изд., испр. и доп. – М .: ФОРУМ : ИНФРА- М , 2019. – 240 с.
9. Бабаш А.В., Ларин Д. А. История защиты информации в зарубежных странах : учеб. пособие / А.Б. Бабаш, Д.А. Ларин. –М .: РИОР:ИНФРА - М, 2018. – 283 с.
- 10.Баранова Е.К.,Бабаш А.В. Информационная безопасность и защита информации: учеб.пособие / Е.К. Баранова, А.В.Бабаш. – 4-е изд., перераб. и доп. – М.: РИОР : ИНФРА –М ,2019. – 336 с.

- 11.Manturov O.V., Solnsev Yu.K., Sorkin Yu.I., Fedin N.G. Matematika termin-larining ruscha-o‘zbekcha izohli lug‘ati.Tarjima. /Prof. V.A.Ditkin tahriri ostida. O‘qituvchi, T.-1974-550 bet.
- 12.Nazarov R.N. va boshq. Algebra va sonlar nazariyasi: Ped.in-t va un-t fiz.-mat. fak. talabalari uchun o‘quv qo‘llanma/ R.N.Nazarov, B.T.Toshpo‘latov, A.D.Do‘sumbetov, 2 qismli. Q.I. – T.: O‘qituvchi, 1993 – 320 bet.
- 13.Ж.Хожиев, А.С.Файнлейб. Алгебра ва сонлар назарияси курси. Дарслик. – Тошкент: “Узбекистон”, 2001. – 304 bet.
- 14.Виноградов И.М. Основы\_теории\_чисел. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
- 15.Оре Ойстин. Приглашение в теорию чисел: Пер. с англ. Изд. 2-е, стереотипное. – М.: Едиториал УРСС, 2003. – 128 с.
- 16.Кочева А.А. Задачник-практикум по алгебре и теории\_чисел.Ч. III. – М.: Просвещение, 1984. – 41 с.
- 17.Нарзуллаев У. Алгебра и теория чисел. Сборник задач и упражнений: Часть1.–LAP LAMBERT Academic Publishing, GmbH & Co.KG.: Saarbrucken, 2012. – 217 с.
- 18.Бабенко,Л.К. Криптографическая защита информации: симметричное шифрование: учеб.пособие для вузов / Л.К.Бабенко,Е.А.Ищукова. – М.:Издательство Юрайт,2019.-220 с.
- 19.O‘zbek tilining izohli lug‘ati: 80000 dan ortiq so‘z va so‘z birikmasi. J. III. N-Tartibli / Tahrir hay’ati: T.Mirzayev (rahbar) va boshq.: O‘zR FA Til va adabiyot in-ti.- T.: “O‘zbekiston milliy ensiklopediyasi” Davlat ilmiy nashriyoti, 2006.-688 bet.
- 20.Rajabov F., Masharipov S., Madrahimov R. Oliy matematika. O‘quv qo‘llanma. Toshkent- “Turon-Iqbol”-2007.-400 bet.
- 21.N.R.Zaynalov, A.N.Muhamadiev, J.Kiyamov. Kriptografiya usullariga doir oddiy misollar// Fizika, matematika va informatika jurnali ,2019, № 2, 26-34 b.
- 22.Зайналов Н.Р., Давронов А.Э. Преподавание информатики в высшей школе: проблемы и решения/ InfoCOM.UZ ,2004, № 5, С.66-67.

- 23.Матвиевская Г. П., Розенфельд Б. А. Математики и астрономы мусульманского средневековья и их труды (VIII-XVII вв.). В 3 т. М.: Наука, 1983.
- 24.Р.Х.Алимов, Б.Ю.Ходиев, К.Алимов ва бошқ. /С.С.Гуломовнинг умумий таҳрири остида. Миллий иқтисодда ахборот тизимлари ва технологиялари: Олий ўқув юртлари талабалари учун ўқув қўлланма. Т.: «Шарқ»,2004. – 320 бет.
- 25.Кнут Д. Искусство программирования для ЭВМ. – Т.1. Основные алгоритмы. – М.: Мир, 1976. 735 с.
- 26.Шень А. Программирование: теоремы и задачи. 6-е изд., дополненное. М.: МЦНМО, 2017. – 320 с.
- 27.Окулов С.М. Программирование в алгоритмах. – М.: БИНОМ. Лаборатория знаний, 2002. – 341 с.
- 28.Тилборг ванн Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006, 471 с.
- 29.William Stallings.Cryptography and network security. Principles and practice. Fifth edition. Pearson Education. New York. 2011. 900 p.
- 30.<http://cryptowiki.net/>-Энциклопедия теоретической и прикладной криптографии.

## Amaliy dasturlar

### 3.2.1. Sezar usuli

```
{ PascalABC tili }
program Cesar;
const n=26; {lotin alifbosidagi harflar soni }
var
i, k: integer;
p: string;
fayl : text;
begin
    assign(fayl, 'input.txt');
    reset(fayl);
    readln (fayl , k);
    readln (fayl , p);
    {siljитish sonini va matnni o'qib oldik}
    close (fayl);
for i:=1 to length(p) do
if p[i] in ['A'..'Z'] then
begin
    p[i]:= chr((ord(p[i])-ord('A')+k) mod n+ord('A'));
    {bu yerda mod n bevosita harflar chegasidan o'tib ketmaslikni ta'minlaydi}
end;
    assign(fayl, 'output.txt');
    rewrite(fayl);
    writeln (fayl ,p);
    close (fayl);
end.
```

Bu yerda masaladagi ma'lumotlar quyidagicha kiritiladi va chiqariladi:

<i>input.txt</i>	<i>output.txt</i>
3 SAMARQAND	VDPDUTDQG

Bu yerda *input.txt* faylida birinchi qatorda *k* va ikkinchi qatorda shifrlanadigan matn kiritiladi va *output.txt* faylida shifrlangan matn chiqarilgan bo'ladi.

### 3.2.6. Pleyfer usuli

```
// Java kotlin tili
package tatu
import java.util.*
import kotlin.collections.ArrayList

fun main() {
    var sc = Scanner(System.`in`)
    var temp = true
    val englishAlphabet = arrayListOf<Char>('A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'K',
'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z')

    while (temp) {
        print("1> Pleyfer usulida shifrlash : 2> Chiqish\nEnter here - ")
        when (sc.nextInt()) {
            1 -> {
                sc = Scanner(System.`in`)
                print("Shifrlanadigan malumotni kiriting - ")
                var playfair = sc.nextLine()
                print("Kalit so'zni kiriting - ")
                val keyWord = sc.nextLine()

                //main value
                var noSameCharKeyWord =
removeSameCharsInWord(keyWord.toLowerCase())

                //printing keyword with no dublicated words
                //println("After removing duplicated chars in keyword -
${removeSameCharsInWord(keyWord.toLowerCase())}")

                var list = ArrayList<Char>()
                noSameCharKeyWord.forEach {
                    list.add(it)
                }
                englishAlphabet.forEach {
                    list.add(it.toLowerCase())
                }
                var beta = ""
                for (i in 0 until list.size) {
                    beta += list[i]
                }

                //main value
                val table = removeSameCharsInWord(beta)
```

```

//printing 5x5 alpgabet
//println("General position - ${table}")

val array1 = ArrayList<Char>()
val array2 = ArrayList<Char>()
val array3 = ArrayList<Char>()
val array4 = ArrayList<Char>()
val array5 = ArrayList<Char>()

val tableArray = table.toCharArray()
val tableMatrix = ArrayList<ArrayList<Char>>()
for (i in tableArray.indices) {
    if (i < 5)
        array1.add(tableArray[i])
    if (i in 5..9) {
        array2.add(tableArray[i])
    }
    if (i in 10..14) {
        array3.add(tableArray[i])
    }
    if (i in 15..19) {
        array4.add(tableArray[i])
    }
    if (i in 20..25) {
        array5.add(tableArray[i])
    }
}
tableMatrix.add(array1)
tableMatrix.add(array2)
tableMatrix.add(array3)
tableMatrix.add(array4)
tableMatrix.add(array5)

//printing matrix
for (i in 0 until tableMatrix.size) {
    for (j in 0 until tableMatrix[i].size) {
        print(tableMatrix[i][j] + " ")
    }
    println()
}

//generating and printing bigrams
var biggramm = generateBiggrams(playfair.toLowerCase())
//prints biggrams
//println(biggramm)

```

```

var listSize =biggramm.size

var encryptionKey = ""
for (i in 0 until listSize step 2){
    encryptionKey+=
mainProcess(biggramm[i],biggramm[i+1],tableMatrix)
    //mainProcess(biggramm[i],biggramm[i+1],tableMatrix)
}
println("Shifrlangan so'z - ${encryptionKey.toUpperCase()}")

}

2 -> {
    temp = false
}
}

}

fun removeSameCharsInWord(message:String):String{
//Romoving dublicates in words by hasan
val chars = message.toCharArray()
val charSet: MutableSet<Char> = LinkedHashSet()
for (c in chars) {
    charSet.add(c)
}

val sb = StringBuilder()
for (character in charSet) {
    sb.append(character)
}
return sb.toString()
}

fun generateBiggrams(word:String):List<Char>{
var list = ArrayList<Char>()
word.forEach {
    list.add(it)
}

for (i in 0 until list.size-1){
    if (list[i]==list[i+1]){
        list.add(i+1,'x')
    }else continue
}
}

```

```

if (list.size%2==1){
    list.add('x')
}

return list
}

fun mainProcess(a: Char, b: Char, tableMatrix:
ArrayList<ArrayList<Char>>):String{
    var encrypt = ""
//printin Biggramms
//    println(a)
//    println(b)

    var aUstun = 0
    var bUstun =0
    var aSatr= 0
    var bSatr =0

    for (i in 0 until tableMatrix.size){
        for (j in 0 until tableMatrix[i].size){
            if (a ==tableMatrix[i][j]){
                aSatr = i
                aUstun =j
            }
        }
    }

    for (i in 0 until tableMatrix.size){
        for (j in 0 until tableMatrix[i].size){
            if (b ==tableMatrix[i][j]){
                bSatr = i
                bUstun =j
            }
        }
    }

    //index of biggrams
//    print(aSatr)
//    println(aUstun)
//    print(bSatr)
//    println(bUstun)

    //Satrlar teng bulgan holda
    if (aSatr==bSatr){

```

```

//a uchun
if (aUstun==4){
    aUstun=0
}else{
    aUstun += 1
}
//b uchun
if (bUstun==4){
    bUstun=0
}else{
    bUstun += 1
}
//printing reindex of biggrams
//    print(aSatr)
//    println(aUstun)
//    print(bSatr)
//    println(bUstun)
    encrypt+= tableMatrix[aSatr][aUstun]
    encrypt+= tableMatrix[bSatr][bUstun]
}
//Ustunlar teng bulgan holda
if (aUstun==bUstun){
    //a uchun
    if (aSatr==4){
        aSatr=0
    }else{
        aSatr += 1
    }
    //b uchun
    if (bSatr==4){
        bSatr=0
    }else{
        bSatr += 1
    }
    //printing reindex of biggrams
    //    print(aSatr)
    //    println(aUstun)
    //    print(bSatr)
    //    println(bUstun)

    encrypt+= tableMatrix[aSatr][aUstun]
    encrypt+= tableMatrix[bSatr][bUstun]
}
//Satr!= Ustun hol uchun
if (aSatr!=bSatr&&bUstun!=aUstun){

```

```

    var temp = aUstun
    aUstun = bUstun
    bUstun = temp
    //printing reindex of biggrams
    //    print(aSatr)
    //    println(aUstun)
    //    print(bSatr)
    //    println(bUstun)

    encrypt+= tableMatrix[aSatr][aUstun]
    encrypt+= tableMatrix[bSatr][bUstun]
}
return encrypt
}

```

### **3.4.3. Matritsa usuli**

```

# Python tili
# kalit va shifrlanadigan so'zni kiritish
kalit = input()
shifr = ".join(input().split())

# jadvalni o'lchamini topish
col = len(kalit)
numberOfElements = len(shifr)
row = numberOfElements // col
if numberOfRowsElements % col != 0:
    row += 1

# jadval yaratish
table = [[ "*" for i in range(col)] for j in range(row)]

# jadval to'ldirish
k = 0
for j in range(col):
    for i in range(row):
        if k < len(shifr):
            table[i][j] = shifr[k]
        k += 1

# class yaratish
class po:
    def __init__(self, nomer, harf, vector):
        self.nomer = nomer
        self.harf = harf
        self.vector = vector

```

```

# kalitni alfavit tartibida saralash
temp = sorted(kalit)

# dictionaryga kalitning harflari tartibi va harflarni kiritish
dict = {}
for i in range(col):
    dict[temp[i]] = i + 1

# obyektlarni dictionary bo'yicha tartiblash
arr = []
for j in range(col):
    tempor = []
    for i in range(row):
        tempor.append(table[i][j])
    object1 = po(dict[kalit[j]], kalit[j], tempor)
    arr.append(object1)

# obyektlarni tartib bo'yicha saralash
arr.sort(key=lambda x: x.nomer)

# saralangan obyektlardan vectorlarni yangi tablega joylashtirish
res = [[ "*" for i in range(col)] for j in range(row)]
for i in range(col):
    obj = arr[i]
    k = 0
    for j in obj.vector:
        res[k][i] = j
        k += 1

# yangi tabledan harflarni yig'ib chiqish
ans = ""
for i in range(row):
    for j in range(col):
        ans += res[i][j]

# shifrlangan so'zni chiqarish
for i in range(len(ans)):
    if i % 4 == 3:
        print(ans[i], " ", end="")
    else:
        print(ans[i], end="")

```

## 4.2. Xaffman usuli

```
{ PascalABC tili }
program Xaffman;
const MaxK = 1000;
var k,a,b : array [1..MaxK] of longint;
bits : array [0..MaxK] of string[20];
sk : array [1..MaxK] of char;
free : array [1..MaxK] of boolean;
res : array [0..255] of string[20];
kj, m, kk1, kk2 : longint;
str : string;
fayl : text;
procedure InputData;
{boshlang‘ich qiyatlarni kirituvchi qism dastur}
var c:char;
j, ij, nj :integer;
s: array [0..255] of longint;
begin
    assign(fayl, 'input.txt');
    reset(fayl);
    for ij:=0 to 255 do s[ij]:=0;
    {s[] indeksi ij ASCII kodini bildiradi va uning chastotasi saqlanadi}
    readln(fayl, str);
{fayldan qatorni o'qib oldik}
    for nj:=1 to length(str) do
        begin
            c:=str[nj]; {bitta belgini tanladik}
            inc(s[ord(c)]);
            {c belgisiga mos keluvchi kod indeksini s[ord(c)] bittaga oshiramiz}
{natiyada s[] massivida har bir belgining chastotasi saqlanadi}
        end;
    j:=0;
    for ij:=0 to 255 do {0...255 bu ASCII kodlari}
        if s[ij]<>0 then begin inc(j); k[j]:=s[ij]; sk[j]:=chr(ij) end;
{k[j] massivida matnda mavjud belgi chastotasi saqlanadi}
{sk[ij] massivida matnda mavjud belgi saqlanadi}
kj:=j; {kj - bu kiritilgan qatordagi jami takrorlanmas belgilar soni}
Close (fayl);
end;
function MinK: longint;
{chastotalar ichidan eng kichigini aniqlaymiz va }
{uning o'rnini m o'zgaruvchida saqlaaymiz va}
{uni free[] ro'yxatda false deb belgilaymiz}
var min, ij : longint;
```

```

begin ij:=1;
    while (not free[ij]) do inc(ij);
min:=k[ij]; m:=ij;
for ij:=m+1 to kk2 do
    if free[ij] and (k[ij]<min) then begin min:=k[ij]; m:=ij end;
MinK:=min; free[m]:=false
End;

Procedure SumUp;
{ Yig‘indilarni hisoblaydigan qism-dastur}
Var s1, s2, m1, m2, ij,ii : longint;
Begin if kj=1 then begin
    assign(fayl, 'output.txt');
rewrite(fayl);
Writeln(fayl,8*length(str), ' ',length(str), ' ',8);
close(fayl);
Exit; {faylda bitta belgili qator bo'lsa unda ishni tugatamiz}
End;
For ij:=1 to kj do
    Begin free[ij]:=true; a[ij]:=0; b[ij]:=0 end;
kk1:=kj; kk2:=kj;
While kk1>2 do {iktadan elemetni olamiz, shu bois oxirida 1 ta yoki 2 ta element
qoladi}
    Begin s1:=MinK; m1:=m; s2:=MinK; m2:=m;
    {chastotasi kichik bo'lgan ikkita qiymat va}
    { ularming o'rni tanlanildi, takrorlanmas ro'yxatdan}
    Inc(kk2);
    K[kk2]:=s1+s2; a[kk2]:=m1; b[kk2]:=m2;
    {ikki minimal chastotani qo'shdik va }
    {ularming o'rmini alohida a[] va b[] massivida saqlab qo'ydik}
    Free[kk2]:=true;
    Dec(kk1)
    End;
end;
Procedure BuildBits;
{ Kiritilgan belgilarni ikkilik raqamlar bilan kodlaydigan qism-dastur}
var ij : integer;
Begin
    bits[kk2]:='1'; free[kk2]:=false;
    bits[a[kk2]]:=bits[kk2]+'0';
    bits[b[kk2]]:=bits[kk2]+'1';
    ij:=MinK;
    bits[m]:='0'; free[m]:=true;
    bits[a[m]]:=bits[m]+'0';
    bits[b[m]]:=bits[m]+'1';
    for ij:=kk2-1 downto 1 do

```

```

        if not free[ij] then begin
            bits[a[ij]]:= bits[ij]+'0';
            bits[b[ij]]:= bits[ij]+'1';
        end
    end;
procedure OutputData;
{ Matnni kodlaydigan va chiqarib beradigan qism-dastur}
var b8, bh, ij : longint;
begin
    assign(fayl, 'output.txt');
    rewrite(fayl);
    for ij:= 1 to kj do
        begin
            res[ord(sk[ij])]:=bits[ij];
            {bits[ij] massivda matndagi harflarning Xaffman kodlari saqlanadi}
            { writeln (fayl,sk[ij], ', ', k[ij], ', ',bits[ij] );}
            {agar barcha qiymatlarni chiqarish talab etilsa,unda ushbu operatorni qo'llang}
            end;
    b8:= 8*length(str);
    bh:=0;
    for ij:=1 to length(str) do
        begin
            inc(bh, length(res[ord(str[ij])]));
            write (fayl, res[ord(str[ij])]);
        end;
    writeln (fayl);
    writeln (fayl, b8, ' ', bh, ' ', b8/bh : 0:1);
    close (fayl);
end;
begin
    InputData;
    SumUp;
    {faylda bitta belgi bo'lsa unda ishni tugatamiz}
    If kj<>1then BuildBits;
    If kj<>1then OutputData;
end.

```

### 3.5.2. Xaltaga buyumlarni joylashtirish masalasi

```

# Python tili
yopiqKalit = [1, 2, 4, 10, 20, 40]
orig = yopiqKalit[:]
m = 110
n = 31
s = "100100111100101110"

```

```

for i in range(len(yopiqKalit)):
    yopiqKalit[i] = (yopiqKalit[i] * n) % m
shifrMatn = []
print(yopiqKalit)
for i in range(3):
    temp = 0
    for j in range(i * 6, 6 * i + 6):
        if s[j] == '1':
            temp += yopiqKalit[j % 6]
    shifrMatn.append(temp)
print(shifrMatn)
def ExtendedEuclidAlgo(a, b):
    if a == 0 :
        return b, 0, 1
    gcd, x1, y1 = ExtendedEuclidAlgo(b % a, a)
    x = y1 - (b // a) * x1
    y = x1
    return gcd, x, y
def linearCongruence(A, B, N):
    A = A % N
    B = B % N
    u = 0
    v = 0
    d, u, v = ExtendedEuclidAlgo(A, N)
    if (B % d != 0):
        print(-1)
        return
    x0 = (u * (B // d)) % N
    if (x0 < 0):
        x0 += N
    for i in range(d):
        return (x0 + i * (N // d)) % N
x=linearCongruence(31, 1, 110)
ochiqMatn = []
for i in range(3):
    temp = (shifrMatn[i] * x)%m
    ochiqMatn.append(temp)
    print(temp)
for i in range(3):
    ochiqMatn[i] = bin(ochiqMatn[i])[2:]
for i in range(3):
    for k in range(6 - len(ochiqMatn[i])):
        ochiqMatn[i] = '0' + ochiqMatn[i]
for i in range(3):
    print(ochiqMatn[i])

```

## Masalalar javoblari

### 2-bob. KRIPTOGRAFIYANING ARIFMETIK ASOSLARI

2.1. Bitlar ustida amallar bajarish

- 1.**  $20_{(16)}$  . **2.**  $213_{(8)}$  . **3.** 10 . **4.** 10010 . **5.**  $222222_{(3)}$  . **6.**  $1D3_{(16)}$  . **8.** 5 . **10.** 19 .  
**11.** 10110 . **12.**  $FF_{(16)}$  . **14.** 11101 . **15.** 11001 . **17.** Fibonachchi sonlari  
**18.** 5 . **19.**  $333_{(8)}$  . **21.** 6 . **22.** True . **23.** True . **25.** True . **26.** False . **27.** False .  
**29.** 5 . **31.** MIRZO . **32.** 3 . **33.** FOTIMA . **34.** 12 . **35.** ZAHRO . **36.** ALI .  
**37.** TATU . **38.** RASUL . **39.** 4 va 5 . **40.** A . **41.** 12 . **42.**  $171_{(8)}$  .  
**43.**  $11011010_{(2)}$  . **44.** 3 . **45.**  $11010_{(2)}$  . **46.**  $111_{(2)}$  . **47.**  $101_{(2)}$  . **48.**  $110_{(2)}$  . **49.** 9 .  
**50.**  $B1_{(16)}$  .

2.2. Butun sonlarning bo‘linishi

- 1.** 1 . **2.**  $b = 7$ ; 8 va  $r = 4$ ; 1; **3.**  $b = 8$ ; 9 va  $r = 2$ ; 6; **4.** 1 . **5.** 1 . **6.** 3 . **7.** 41 .  
**8.** 7 . **9.** 9 . **10.** 00 . **11.** 4356 . **12.** 5 . **13.** 128205 . **14.** 8281 .

2.3. Tub sonlar

- 1.** tub . **2.** murakkab . **3.** tub . **4.** murakkab . **5.** 2333, 2339, 2341, 2347 . **6.** 211 .  
**7.** 2543, 2549, 2551, 2557 . **8.** 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249 .  
**9.** 3, 5, 7, 11, 13, 19, 23, 29, 31, 37 . **10.** 12 .

2.4. Sonlarni ko‘paytuvchilarga yoyish

- 1.**  $7 \cdot 13 \cdot 73$ ; **2.**  $61 \cdot 29$ ; **3.**  $67 \cdot 53$ ; **4.**  $89 \cdot 73$ ; **5.**  $7 \cdot 11 \cdot 17$ ; **6.**  $3 \cdot 3 \cdot 7 \cdot 13$ ;  
**7.**  $3 \cdot 11 \cdot 37$ ; **8.**  $3 \cdot 3 \cdot 3 \cdot 7 \cdot 7$ ; **9.**  $2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \cdot 7$ ; **10.**  $11 \cdot 13 \cdot 17$ ;  
**11.**  $3 \cdot 13 \cdot 13$ ; **12.**  $2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7$ ; **13.**  $7 \cdot 11 \cdot 97$ ; **14.**  $2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$ ;  
**15.**  $2^2 \cdot 3 \cdot 5 \cdot 7 = 420$  . **16.**  $2 \cdot 3 \cdot 5 \cdot 7 = 210$  . **17.** 72; 84; 90; 96. **18.** 192 .

2.5. Eng katta umumiy bo‘luvchi

- 1.** 21 . **2.** 13 . **3.** 119 . **4.** 3 . **5.** 23 . **6.** 72 . **7.** 3 . **8.** 45 . **9.** 3276 . **10.** 1116 .  
**11.** 5382 . **12.**  $d = 29$ ,  $x = -6$ ,  $y = 11$  . **13.**  $d = 5$ ,  $x = 2$ ,  $y = -5$  . **14.**  $d = 17$ ,  $x = -10$ ,  
 $y = 23$  . **15.**  $d = 43$ ,  $x = -4$ ,  $y = 5$  . **16.**  $d = 47$ ,  $x = 2$ ,  $y = -5$  . **17.**  $x = 495$ ,  $y = 315$  .

**18.**  $x = 140$ ,  $y = 252$ .

### 2.6. Taqqoslama arifmetikasi

- 1.** 5 . **2.** 10 . **3.** 25 . **4.**  $x \equiv 81 \pmod{337}$  . **5.**  $256x \equiv 1630 \pmod{2413}$  .  
**6.**  $x \equiv 91 \pmod{120}$  . **7.**  $x \equiv 8479 \pmod{15015}$  .  
**8.**  $x \equiv 100 \pmod{143}$ ;  $y \equiv 111 \pmod{143}$ ; **9.**  $x \equiv 16 \pmod{27}$  .  
**10.**  $x \equiv 113 \pmod{125}$  . **11.**  $x \equiv 4 \pmod{11}$  . **12.**  $x \equiv 10 \pmod{11}$  .  
**13.**  $x \equiv -3 \pmod{24}$  . **14.**  $x \equiv 10 \pmod{53}$  . **15.**  $x \equiv 10 \pmod{35}$  .  
**16.**  $x \equiv 10 \pmod{25}$  . **17.**  $x \equiv 9 \pmod{16}$  . **18.**  $x \equiv 5 \pmod{23}$  .  
**19.**  $x \equiv 75 \pmod{106}$  . **20.**  $x \equiv -5 \pmod{13}$  . **21.**  $x \equiv -3 \pmod{8}$  .  
**22.**  $x \equiv 35 \pmod{37}$  . **23.**  $x \equiv 14 \pmod{15}$  . **24.**  $x \equiv 16 \pmod{25}$  .  
**25.**  $x \equiv 103 \pmod{123}$  . **26.**  $x \equiv 50 \pmod{58}$  . **27.**  $x \equiv 11 \pmod{169}$  .  
**28.**  $x \equiv 2 \pmod{8}$  . **29.**  $x \equiv 4 \pmod{13}$  . **30.**  $x \equiv 11 \pmod{30}$  .  
**31.**  $x \equiv 131 \pmod{187}$  . **32.**  $x \equiv 296 \pmod{575}$  . **33.**  $x \equiv 287 \pmod{340}$  .  
**34.**  $x \equiv 217 \pmod{240}$  . **35.**  $x \equiv 360 \pmod{667}$  . **36.**  $x \equiv -1 \pmod{28}$  .  
**37.**  $x \equiv 31 \pmod{1872}$  . **38.**  $x \equiv 19 \pmod{8736}$  . **39.**  $x \equiv 32 \pmod{75}$ .  
**40.**  $x \equiv 86 \pmod{231}$  . **41.**  $x \equiv 22 \pmod{120}$  .**42.**  $x \equiv 256 \pmod{1547}$  .  
**43.**  $x \equiv 93 \pmod{140}$ . **44.**  $x \equiv 18 \pmod{35}$  . **45.** 25 . **46.** 49 . **47.** 49 .

### 2.7. O‘rin almashtirishlar

- 1.** (10,8), (1,9), (2,5), (1,10), (7,10), (7,4), (2,3), (3,6), (4,6); **2.**  $i = 8$ ;  $k = 3$ .  
**3.** 12. **4.** 10 ta va juft . **5.** 15 ta va toq . **6.** 28 ta va juft . **7.** 6 ta va juft .  
**8.** 10 ta va juft . **9.** 3 ta va toq . **10.** 9 ta va toq . **11.** 16 ta va juft .  
**12.** 25 ta va toq . **13.** 3 ta va toq . **14.** 9 ta va toq . **15.** 18 ta va juft . **16.**  $k-1$ .  
**17.**  $n-k$  . . **18.** o‘rniga qo‘yish emas. **19.** o‘rniga qo‘yish. **20.** o‘rniga qo‘yish.  
**21.** o‘rniga qo‘yish. **22.** o‘rniga qo‘yish. **23.** o‘rniga qo‘yish emas.  
**24.** (1) (278) (345) (6), juft o‘rniga qo‘yish.  
**25.** (18) (27) (36) (45) (9), juft o‘rniga qo‘yish. **26.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 4 & 6 & 1 \end{pmatrix}$

**27.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 6 & 4 \end{pmatrix}$

**28.**  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

**29.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

**30.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$

**31.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

**32.**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 6 & 3 & 2 & 5 & 8 & 9 \end{pmatrix}$

## 2.8. Matritsalar

**1.** 0;

**2.**  $(-1)$ ;

**3.**

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

**4.**

$$\begin{pmatrix} 8 & -12 & 0 \\ 6 & -9 & 0 \\ 2 & -3 & 0 \end{pmatrix}$$

**5.** 50 .

**6.**  $\begin{pmatrix} 8 & 14 \\ 8 & 14 \end{pmatrix}$

**7.**

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

**8.** (1 1);

**9.** 0.

**10.**  $\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$

**11.** (0 3 2);

**12.**

$$\begin{pmatrix} 3 \\ 6 \\ 4 \\ 3 \end{pmatrix};$$

**13.**

$$\begin{pmatrix} 4 & 4 \\ 3 & 3 \end{pmatrix};$$

**14.** (6, 9, 12);

**15.**  $\begin{pmatrix} 4 \\ 3 \\ 1 \\ 2 \end{pmatrix};$

**16.**  $\begin{pmatrix} 2 & -6 & -5 \\ 2 & -6 & -5 \\ -2 & 6 & 5 \end{pmatrix}$

**17.**  $2^{n-1} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix};$

**18.**  $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix};$

**19.** 0 agar  $n > 1$  bo'lsa; **20.**  $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix};$  **21.**  $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix};$  **22.**  $\begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix};$  **23.** -1 .

**24.**  $\begin{pmatrix} 4 \\ -11 \\ -16 \end{pmatrix};$     **25.** 0 .    **26.**  $\sin(\alpha - \beta)$  .    **27.** 0 .    **28.** 16 .    **29.** 0 .    **30.** 0 .

**31.**  $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix};$     **32.**  $\begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix};$     **33.**  $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{3} \\ 0 & \frac{1}{2} & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix};$

**34.**  $\frac{1}{7} \begin{pmatrix} -5 & 2 & 2 & 2 \\ 2 & -5 & 2 & 2 \\ 2 & 2 & -5 & 2 \\ 2 & 2 & 2 & -5 \end{pmatrix};$     **35.**  $\begin{pmatrix} 0 & -1 & 1 & -1 \\ 1 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{pmatrix};$     **36.**  $\begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix};$

**37.**  $\begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix};$     **38.**  $\begin{pmatrix} -\frac{7}{3} & 2 & -\frac{1}{3} \\ \frac{5}{3} & -1 & -\frac{1}{3} \\ -2 & 1 & 1 \end{pmatrix};$     **39.**  $\frac{1}{9} \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix};$     **40.**  $\begin{pmatrix} 5 & -8 \\ 2 & -3 \end{pmatrix};$

## 3-bob. SIMMETRIK KALITLI SHIFRLASH TIZIMLARI

### 3.1. O‘rniga qo‘yish usul

<b>№</b>	<b>Shifrlangan so‘z (<math>T_m</math>)</b>	<b>№</b>	<b>Shifrlangan so‘z (<math>T_m</math>)</b>
1	BUJZTIWPD_UIL_XRWMWF	26	ZGMGCWOLIDFUHUMW
2	VWVMWLKIUYWFDZUCJWY	27	PTMBTOMUIDAWMLJW
3	ZGOPLIBUQDQUJRWHUJW	28	FUJUMNLHUDVWHLJW
4	BUJZTIWPDCIJWZUMUI	29	FTZTVNLHUDFWZLVW
5	ZU_WHXRL_MUIDHUINW	30	FLJQLHUCZMUIDTPW
6	PWMEWKWXRMUIDIUKW	31	_WOW_DQUZGQUZWFW
7	THWCGIJWZGZDVWHLJW	32	PUHKWDQTMUZKWXR
8	BUJZTIWPDAUQMUHQU	33	VUOWJDCUIWUHZMUI
9	UNVLILZDGJFWIWJRW	34	FUIHUPDJTIHUPXRW
10	UNVLILZDVTZTHMWKW	35	ZWMMUDZWJRXRUMUI
11	BUJZTIWPDQURJTMLZ	36	VWMWQMUIDLQVLIW
12	UNVLILZDUKGHZMWKW	37	UNVLILZDVWOHGJW
13	BUJZTIWPDWMLCUMUI	38	UNVLILZDVUMUHJW
14	QWMWZJWPUDWBLIUJW	39	BWIGFZLIDNLHUJW
15	_TMTEHUPDJRUIVUZW	40	UJFUIMUIDRUPPLZW
16	IU_UQMUIDUPWIQUJW	41	VTPIT_MUIDJUZIW
17	JRUYZLMWDJRUIVUZW	42	PUHKWDBUYZUIMUI
18	YLZLUUEUIUZD_WJQW	43	ZWJRDBLFZLIMUIW
19	PUHKWDZGNHMLKWP	44	UNVLILZDVLOLIW
20	VLJR UITCDNLHUJW	45	CU_ZDQUJRWHUJW
21	VUHFMIUIILDZWOWQ	46	VLJRDJURWYUXRW
22	VUHHGIDIGFMUQUJW	47	VTMMDUMKGVIUJW
23	BUJZTIHWDJLOMUJR	48	VUHPUHDZUIQL_
24	ZGMGYLHDZITVFUJW	49	VGZUDZGJZMUJR
25	_LCTIWMKUHDVUMW_	50	VLJRDQTRUIIWI

### 3.2. Monoalifboli o‘rniga qo‘yish usuli

<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>	<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>
1	_RRUX OOIOL ROFLX LOXOU	26	UCXC_ OLFOO URCRX O****
2	OUUXO FIORF OUOUR _ROF*	27	IXX_X LXROO ROXFR O****
3	UCLIF O_R_O _RRLO CRRO*	28	URRRX FFCRO UOCFR O****
4	_RRUX OOIO_ FROUR XRO**	29	UXUXU FFCRO UOUFU O****
5	URLOC XLFLX ROOCR OFO**	30	UFR_F CR_UX ROOXI O****
6	IOXIO IOXLX ROOOR CIO**	31	LOLOL O_RUC _RUOU R****
7	XCO_C OROUC UOUOC FRO**	32	IRCIO O_XLX RUIOX L****
8	_RRUX OOIOR R_XRC _R***	33	URLOR O_ROO RCUXR O****
9	RFUFO FUOCR UOOOR LO***	34	UROCR IORXO CRIXL O****
10	RFUFO FUOUX UXCXO IO***	35	UOXXR OUORL XLRXR O****
11	_RRUX OOIO_ RLRXX FU***	36	UOXO_XROOF_UFOO
12	RFUFO FUORI CCUXO IO***	37	RFUFO FUOUO LCCRO
13	_RRUX OOIOO XF_RX RO***	38	RFUFO FUOUR XRCRO
14	_OXOU ROIRO O_FOR RO***	39	_OOCU UFOOF FCRRO
15	LXXXI CRIOR LROUR UO***	40	RRURO XROOL RIFUO
16	ORLR_XROOR IOO_R RO***	41	UXIOX LXROO RRUOO
17	RLRFU FXOOR LROUR UO***	42	IRCIO O_RFU ROXRO
18	FFUFR IIROR UOLOR _O***	43	UORLO_FUUUF OXROO
19	IRCIO OUCFC FXFIO IR***	44	RFUFO FUOUF LFOO*
20	UFRLLO ROX_O FFCRR O****	45	_RLUO_RRLO CRRO*
21	URCUX ROROF OUOLO _****	46	UFRLO RRLOF RXLO*
22	URCCC OOOUCU XR_RR O****	47	UXXXO RXICU ORRO*
23	_RRUX OCOOR FLXRR L****	48	URCIR COUR_O_FL**
24	UCXCF FCOUO XUURR O****	49	UCURO UCRUX RRL**
25	LF_XO OXIRC OURXO L****	50	UFRLO_XLRO OOO**

### 3.2.1. Sezar usuli

<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>	<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>
1	C_RSTQHXZP_QNPBGHKHJ	26	UFMFWJ_PSALBOBMJ
2	_G_JGMEPZDGIYRZTQGD	27	XTKCTYK_QZIHKNRH
3	QBWVLOAYJXJYPEFKYPF	28	IZQZJVMLZY_GLMQG
4	_XOPQNEUWRKOEPXHXN	29	HRQRZULKYXHFQLZF
5	OWLDIYCJLGWMVIWMSD	30	GKOIKJXRPHXNWQUE
6	SCFJCACXBFLULVHAC	31	LDUDLVHWO_HWODFW
7	NGBOYKLBMYMTVBGHLB	32	SVHACUGOTFVNACXB
8	WTKLMJAQS TEDTFET	33	VUSBLTOUKBUGMEUK
9	SOTFIFKRWJB_I_JZ_	34	CTJFTQSKMJFTQV_A
10	RNSEHEJQSKJKDBZXZ	35	K_CCSRK_JZUZSCSI
11	TQHIJGYNPBQXHJADI	36	SZBZCBRHQECSEHZ
12	PLQCFCHOPVTBH_XVX	37	QMRDGDIPRYOCUHY
13	ROFGHEWLWZBIOZOE	38	PLQCFCHOQP_PBGX
14	ZVYVFEVKNMVQADNEV	39	RWESYGBENKBAOFW
15	BFXFAZMJLDTMCNMEU	40	NEXNDYNDMUNKAFV
16	BLALXWLBKLITBXLCT	41	NFJCFBXMCLDMECU
17	BRKPCYVSJBRKALKCS	42	ILYRTKOLQDLBWLB
18	OXBXJYYJ_JBIZRAVR	43	CSBRJNYUCYAVKAS
19	FIVOQHAMEVWTWOQFI	44	JFKX_XBIKXHX_R
20	IVZOXHYABGDVUHZP	45	CIYAHUI_PQVI_Q
21	HGTQRGXGXUFZOEOS	46	IVZOGZHOPMHJOP
22	GFSSJWEWJPQFRFXN	47	H_RRFGRMKHXGYO
23	HEWXYVRMDWSCPPEWL	48	GFSCFSEYFWRTV
24	WHOHIRQCWUXENDVL	49	FIXEDXIWXPEWL
25	SQXWTKNICPBDCNKS	50	ERVKCPXKDUULU

### 3.2.2. Affin tizimidagi Sezar usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	NFUZNTCJEJX	26	EJYJMZXW
2	KFKOFXZGHWFL	27	HZUEZWULG
3	OVGDZISJT	28	LZFZUYVMZ
4	CTNPSBEBI	29	UGXGRHEVI
5	HCYAPIXSYJCB	30	LRXBRWJISGJC
6	NZAKHZXQAF	31	BXMHBXMRJX
7	SVMZXEMLKL	32	RPEOHMZFC
8	KDTEPINH	33	TQLGQDPZQL
9	FYQDKDG	34	VNYANB
10	ILELOAFT	35	MLQQP
11	JFQLDABU	36	MNGNVGXS
12	BRDOEAFT	37	DUGTCTI
13	QFUDCF CJ	38	UFOFSP
14	CNUDE	39	WXERNUTE
15	LWXICPJ	40	DJP DAYDA
16	HIEISPIH	41	SHRGHXEJG
17	VSJIABMX	42	VUNJURPUR
18	VGPGMNNMBMP	43	CZTAZKORKD
19	SNCQZYFXLD	44	NUCPIPMAPLN
20	SFXGBHMTE	45	PFHADSFHD
21	UJWPAJO	46	TPSLGPBSL
22	WJVKBZBLR	47	DENBWODHZ
23	WGLHCWR	48	URGXLZ
24	ULKLWRG	49	SLVSQXVC
25	IYHCNUJKGT	50	PZMNSSXS

### 3.2.3. Tayanch so‘zli Sezar usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	ANBOAQVWHWZ	26	IVBVKZODG
2	LWLZWSTAKRWY	27	NHTUHPTQE
3	FUMLRCSNK	28	EPFPMLARP
4	IAFZGPUPD	29	AHGHRKBVQ
5	ELBXONWPBSLC	30	YHBEHSNFCZNA
6	KWSAWUWPVSMC	31	VNGTVNGYDN
7	FUXGQCDXEQE	32	AHNROGWZQX
8	URGHJFIP	33	IOEYOMGAOE
9	TPUDIDL	34	AUHDUQ
10	TKHKBMJS	35	LSDDV
11	ORZGITCH	36	STGTAGRF
12	RYWAGNPI	37	TNUEHEJ
13	DTBJOTOF	38	VUBUDK
14	OYFJV	39	VBGWSJDG
15	DHMHCAPL	40	RGYRFORF
16	HRGRCIRH	41	SJPJFMRG
17	GLTYHCNI	42	SPUGPEZPE
18	TIFIOYYOBOF	43	PYUEYCZMCW
19	DSIWEPEUXJL	44	LHNMBMDSMAL
20	SBGZDQFIJ	45	MSHZEASHE
21	TSCYOSH	46	GQZNXQUZN
22	DVSHQIQFZ	47	PNXVRDPEZ
23	KETBUKI	48	NUKCGJ
24	IXOXYDC	49	KXJKTRJA
25	CAHGDYIWOP	50	AJZSGGFG

### 3.2.4. Polibiy kvadrati

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	PTRUDZYKW	21	IFXYZWQTAHNOQFW
2	IFWFCYXORTS	22	OSYKMWFYXODF
3	YKCSTQTMODFQFW	23	FQMTWOYRQFW
4	FCGTWTYQFXNYOWOXN	24	RFYKRFYOPF
5	PWOUYTMWFLODF	25	OSLTWRFYOPF
6	XYKMFSTMWFLODF	26	FSYOAOOWZX

7	PQFAOFYZWF	27	OSYKWAFQ
8	XNOLWQFSMFS	28	OSYKMWFQ
9	YFWFVVODTY	29	UTBKWUTOSY
10	OSSTAFYXODF	30	UNTYTXNTU
11	WOATOQFSOXN	31	AOSHNKXYKW
12	DZPXFQOXN	32	MKTRKYWODF
13	YKQKAOETW	33	UXKAITYFXTILOD
14	RTSOYTWOSM	34	YKSMQFRFQFW
15	RTIZQDFYTW	35	TUYORFQQFXNYOWOXN
16	YWFSXQDFYTW	36	XTIIFQFXNYOWOXN
17	PTRUOQDFYTW	37	PTRGOSFYTWOPF
18	OSYKWUWKYFYTW	38	CFALXOEQOP
19	OSYKQQKHY	39	VOXVFWYRF
20	MKSKWFTYTW	40	IFATRFY

### 3.2.5. Atbash usuli

№	Shifrlangan so‘z	№	Shifrlangan so‘z
1	GVOVPLNNFMRPZGHRBZ	26	GVCMLPIZGRBZ
2	FMREVIHRGVGOZIRNRA	27	PIRKGLMZORA
3	ZEGLNZGOZHSGRIRHS	28	RMHGIFPGHRBZ
4	NZJYFOOZHSGRIRHS	29	RMULINZGHRBZ
5	ILYLGOZHSGRIRHS	30	PLMUVIVMHRBZ
6	GIZMHULINZGHRBZ	31	RMHGIFNVMGZO
7	QZWZOOZHSGRIRHS	32	PLNYRMZGHRBZ
8	HSGZMTVMGHRIPFO	33	RMGVOOVPGFZO
9	PLMURTFIZGHRBZ	34	PRYVIMVGRPZ
10	HGVTZMLTIZURBZ	35	GVCMLOLTRBZ
11	RMUIZHGIIFGFIZ	36	NFSZMWRHORP
12	NLWVIMRAZGHRBZ	37	WRZTMLHGRPZ
13	UFMPGHRLMZOORP	38	CZEUHRAORP
14	GIZMHPIRKGHRBZ	39	KILGHVWFIZ
15	KVIKVMWRPFOBZI	40	GVOVULMRBZ
16	IRELQOZMGRIRHS	41	POZERZGFIZ
17	VPHKOFGZGHRBZ	42	NRPILHCVNZ
18	HRERORAZGHRBZ	43	KILGHVHHLI
19	PLMHGRGFGHRBZ	44	PLMHGZMGZ
20	PLNKROBZGHRBZ	45	KOZGULINZ
21	NZHSRMZH LAORP	46	IVPFIHRBZ
22	PLMHGIFPGHRBZ	47	NVMVQNVMG
23	GZIRURPZGHRBZ	48	ZMGRERIFH
24	RMGVTIZGHRBZ	49	NRXILHPLK
25	PIRKGLOLTRBZ	50	GVCMLTV

### 3.2.6. Pleyfer usuli

<b>№</b>	<b>Shifrlangan so‘z</b>						
1	HIIRLQ	13	GHATHC	25	EGGNOR	37	TLKFCW
2	DBVAMU	14	LFSQRC	26	VDHOVE	38	TFKPTK
3	NBIEUR	15	USAYIU	27	LVNODR	39	FCXIGN
4	MLVGCN	16	LBUGUT	28	UAUSYT	40	ISKECS
5	DMXFSD	17	CLDEUP	29	CSAICT	41	EKYAZF
6	LREKDX	18	EMDUTV	30	CKORKT	42	CESRIRXY
7	HKEADL	19	XEPCUP	31	APMADZ	43	NFZLDG
8	OZIKMH	20	GKSBDI	32	DSDLFU	44	GEQUDP
9	DBKHPO	21	KDHROH	33	BPBFQO	45	ZAICCM
10	HBKSSF	22	OFXLPS	34	AHGQCD	46	TPEHMQ
11	ENTLLK	23	QSVTLD	35	TIHNNI	47	QRDIMO
12	UMITDV	24	ZKNCVE	36	TUXHFZ	48	EBWUSN

### 3.2.7. Omofon usuli

<b>№</b>	<b>Shifrlangan so‘z</b>
1	92 26 86 69 41 61 40 40 13 89 73 41 77 92 56 73 55 31
2	13 88 73 22 48 04 06 68 78 75 78 95 31 39 02 40 03 47
3	63 22 38 91 52 31 60 81 07 57 70 23 68 71 53 34 20
4	40 31 15 11 14 86 86 31 90 19 60 53 04 53 57 87
5	39 96 64 91 37 42 77 90 19 05 53 04 53 90 19
6	92 24 07 88 56 09 91 39 52 31 35 59 03 55 77
7	18 50 10 07 95 42 77 06 54 92 29 58 02 56 87
8	56 54 37 84 88 83 32 43 35 59 03 99 41 36 81
9	41 16 88 09 68 44 36 71 66 37 06 02 55 66
10	90 92 67 44 84 89 91 44 39 31 09 73 93 84
11	68 88 09 58 07 59 37 71 13 41 92 13 58 63
12	52 16 76 72 58 00 03 47 84 74 90 73 55 07
13	08 36 43 41 92 34 73 91 00 77 86 42 53 41
14	78 04 50 80 90 41 71 29 62 74 34 03 93 50
15	62 82 71 01 72 43 51 53 41 14 42 55 66 24
16	99 02 22 65 18 95 66 89 37 29 99 02 34 54
17	85 41 34 62 81 14 84 23 07 38 56 03 93 50
18	57 73 22 53 81 53 47 66 78 59 53 55 77
19	41 65 43 06 60 02 23 14 92 06 29 93 07

20	41 94 40 01 02 81 55 31 35 56 73 55 66
21	40 07 90 70 53 80 77 34 16 47 95 73 41
22	41 96 89 34 23 71 36 41 60 06 03 55 84
23	78 77 04 68 08 68 41 84 60 59 68 55 07
24	53 43 74 79 83 71 50 92 59 68 55 84
25	41 71 53 01 60 61 42 61 83 03 93 84
26	92 67 12 43 65 41 04 50 05 03 93 77
27	41 04 03 01 78 96 07 00 77 95 73 47
28	29 88 90 37 58 36 41 35 57 68 93 63
29	68 00 09 65 71 52 84 05 06 68 93 63
30	41 16 80 08 28 58 26 00 57 02 93 77
31	29 88 59 35 04 14 40 72 43 74 50 86
32	41 61 52 64 29 80 07 38 06 68 55 31
33	03 88 60 67 42 95 26 41 05 36 63 81
34	41 29 11 72 71 88 25 92 68 41 63
35	35 82 12 88 91 42 61 83 68 55 84
36	40 14 87 31 80 76 02 34 81 02 41
37	27 53 07 44 43 94 56 74 29 41 63
38	12 31 22 08 06 29 47 86 02 41
39	01 04 30 92 59 72 10 13 99 50
40	37 48 86 48 08 91 80 73 93 50
41	41 86 50 22 03 66 60 13 71 63
42	52 68 41 99 61 56 12 32 52 31
43	01 58 65 23 34 82 59 34 96 39
44	41 91 00 59 78 50 88 74 77
45	01 42 77 38 08 91 58 40 63
46	04 82 41 13 24 56 73 55 31
47	40 48 43 79 18 40 28 80 05
48	66 43 05 73 22 02 58 14 06
49	52 02 17 58 91 57 41 16 01
50	60 85 12 80 94 44 28 88

### 3.2.8. Vernam usuli

<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>	<b>№</b>	<b>Shifrlangan so‘z (T<sub>m</sub>)</b>
1	MIK@*RHQE?LRBY#JDLHC	26	BE#KU#Z**@YA_OK#
2	N_TDYOKFSNYKQHS@CIJ	27	S_YNVTDT*@DAYATC
3	*QL*#!PU?!YK?T#KUYE	28	ZE?I#EKBINSMBGD!
4	KPLIIX#FHMAAOAWAKGZ	29	FUY#UYOGOJFIYAUH
5	DNS?UDIV_YOAI?AGAD	30	O*?MEJRZTBEAQUISM
6	BTQCNPV@QBA_O?A!XF	31	TMMGB*IV@VPEGG!D
7	VJ#SM!TMBD!WAM*j#C	32	AU_GCEYFZBYHXII*
8	AOZYUALWXCA@IOGHA	33	QALED_HMAISBCLS@
9	HXLEV*U_OYOZWIYNM	34	YTFGSLIZGCZLKRTD
10	KZTC*_ZSTY@GHF#KG	35	*I#ZM_C#?HTVMLRD
11	TILYUAYQFHAWC_SFT	36	TPF*?MOGOJCW_WG
12	G*SOAOVUTGVNVD!GZ	37	QXT*BOBNRIL_US#
13	KADY_!BYNDDE_A#LZ	38	L*E@#GWPKIOTG#N
14	?ANACAA?IN#LIZRAA	39	QIGXTZCPXZ?TS*
15	HA#YB#UJQ_QUANOE_	40	G#FSXDPD#PPKI!H
16	QOJO@KOISRZGICRTG	41	LQUR?UHA!Y?AZVE
17	ZPML?FDES*MI@PNYA	42	WLBGGXPALYMRFL@
18	IK*GSCLMZS?Y_AABM	43	@Z_MSSAB@**AOAG
19	WTGGZ_APX_AYFGZWT	44	M*ZO@GL_NGBO@A
20	TACJ!S*E!XFA@OZ#	45	HOSUOCCVVGPHAG
21	CA_SFDRRJA*TZBGP	46	ROTWMSBWYFBTXI
22	FSKFOVOWMAPSLIYM	47	OAAEILESPOF@_
23	FIZTYXFD_?IRAA?B	48	EIJ@IGZ!LUEFV
24	_EAXLBNXA!*BBT@I	49	MK?NS?J_?GO*K
25	?_Z#_GZKOASTMFF?	50	SGZUUHHPLCZDC

### 3.3.1. Gronsfeld usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>kalit (k)</b>	<b>№</b>	<b>Shifrlangan so‘z</b>	<b>kalit (k)</b>
1	FDWYWUMDSDVTSFLNNLO	2345	17	RLERRPFCFPFCJNF	1359
2	EMGRLSLXDJNQWEAYLJ	3456	18	CKOMNNNDVPOESSK	1234
3	OZZBFCUUEKGFPN	4567	19	CAFTTRXGKCRJUL	2345
4	IGZBZXPGAUZQYGSIW	5678	20	DBGVUSYIDPFUVM	3457
5	JHACAYVRYVHUGZP	6789	21	FZEZYVRIVXGBVN	4568

6	AMUFMWWUYCKLHAR	7891	22	DGUPNJHOYGYUFX	5679
7	CWJXMATKBNUDQWPUQ	8912	23	ECIXVTAKSEVAM	4579
8	MBUWDSKBSBOOJOOD	9123	24	AHZXRHBLNUJWN	5794
9	CBHWTSZMUOOZKWNQ	2468	25	GUALXGPMKGKLN	5684
10	EDJQVUBDYZCPPOOK	4682	26	HCPQGTKJHZEXO	6845
11	JIUXAZKCSIJWATQX	6824	27	VFXIQQHZEDPZQFZQ	4578
12	IZFUZQXGOGRZTKKO	8246	28	DHVPNAMGSVTXLPGJ	5789
13	GFZCXWPHLQVEDQHA	3579	29	IWBIXIAVCFXOHAR	7891
14	GLCBYLBQHBI	5791	30	JJPOTJTEZXVMHRO	8924
15	VYFUHCTLVWULGRN	7913	31	BGLZUKODJFVIC	9248
16	KVBWDRTFCPUN	9135	32	IEUVCPIBJYADNM	2489

### 3.3.2. Vijiner jadvali

№	Shifrlangan so‘z	kalit	№	Shifrlangan so‘z	kalit
1	nutdosssrklpawisfju	kub	17	elzuepafspafwna	odam
2	bymlyzghlfyvtqgsyq	aql	18	ziyoujaeuuzoeo	yangi
3	fckotswluxvgcc	virus	19	vxrhmojudzdxni	vaqt
4	dnlbuebgvblqtnear	anti	20	oabhfrtuooaggl	odat
5	kajybrenzoqqhsy	harf	21	jmjfgylfeikcw	islom
6	wmdoiwfductudaa	disk	22	falubkadhtylyf	hayot
7	zymnlwdmllymmfvxt	flesh	23	mxsqdoktazfju	mars
8	eifhvzvmkizzbvzo	bino	24	jqyfaqatwdiew	oqim
9	fxzzworpxkgcnsft	fayl	25	cckotozpgouoj	bosh
10	iipjrwepptcyzdq	ilova	26	uorxaeaknrtmo	tugma
11	talhlhirarxsnzfj	qator	27	koatavtfkrwbfoecb	tok
12	kfnmfybmexbxgus	kimyo	28	mlzgweqxbzxoutka	olma
13	dvdhxrdjwooplzdr	avlod	29	bbgyqnflvkceafw	anor
14	eygyhhmgjovb	dunyo	30	roieyqfvlbjwucz	qovun
15	npqznssuwasilqz	zamin	31	pyydzfemmrouk	xurmo
16	aukfhpqmhbqi	zamon	32	wuetqfszxokbbc	qush

### 3.3.3. ADFGX usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Kalit</b>
1	AGXG AGFD GGFA FXFA DDXG FDDD ADFF	kabinet
2	DGGA AGFG FFAD FAGG ADDF FFFX FDFD	dasturi
3	DFDD GAAD AXXG FADG DXXG AFFF XDAF	yuklash
4	FXAD AGXG ADXD GGGD FDGD AGGG DDXD	yeterli
5	AGFAGFDX XAGG XAFD GGXD ADAF XGAD	xavfsiz
6	AGXX ADAD XGXA FFFX XDXD FAXA ADGF	kabinet
7	DAFG FDDG GXFD GGGF GFFD DAXG AGAD	dasturi
8	FDFGADDG AGAG FXFF GGGF AGXF DDXF	yuklash
9	GXDA FFGA GFAD XFGG DFFF FFDA Xdff	yeterli
10	FXDX XDGG AADG AFDG GDGA AFDG DDGD	xavfsiz
11	AGXD AGAF GGFX FXAX DDXG FDDD ADDD	kabinet
12	AFDG DDFD AFAX XDDF FXAX AAGG GDGF	joylash
13	FFXD GFXD FAFG GADG DADG AFAD DGAX	formula
14	XFFA AGDF FDFA FDDA GDGD FDDF FGXF	kabinet
15	DAFG FFAD DXAD DAFG DFXD FADD AXAG	dasturi
16	FAAD DDAD XGAD FGFX XGGX DAXX AFXF	yuklash
17	FADA DDAF FFAD XDXX GGXF XFGG AXGF	yeterli
18	AGFF FXXG GXXG FDXD AGFG DDXG AAGD	xavfsiz
19	ADFX GFDX XDAF FAFF AAGF AXDF DGXX	joylash
20	XDGF DADD AGGA FFFA XGXX DGAX XXFF	formula
21	AFGD GAXG GAFG DXAG FDGG DDFG GGDG	kabinet
22	DXDD XFGF ADDG AGDD AAGD FADD FGDD	dasturi

### 3.4. O‘rin almashtirish

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Qadam</b>	<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Qadam</b>
1	OORXBU	3	11	AIFHSA	4
2	RTUSDA	4	12	ZGINDE	4
3	RLANSO	2	13	SANLBA	3
4	RLADKO	5	14	IFLVXA	3
5	QMORTA	4	15	AITSVO	4
6	OFBIAL	3	16	RTOKDO	5
7	RTAFDA	2	17	YLIAAM	5
8	QRUYBU	3	18	YNARKA	4
9	NFILDE	4	19	LLIHTA	3
10	ZDULYU	5	20	MDARYO	5

### 3.4.1. Shifrlangan so‘z jadval

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>k</b>
1	KYRN GLBE OUTO IAIS MTEL YRZD PEXO AINA	4x8
2	MOIA OLAT NXNI ‘LGT M*LA DSO* URAI D*MN RME*	6x6
3	MOIA OLAT NXNI ‘LGT M*LA DSO* URAI D*MN RME*	8x4
4	AEYI XXAZ BNLI OOAM RLRL OOOA TGAR TITI	7x5
5	ALI’ GXAS RIBS HIQO HTSO RTOI NOI’ DUTR GAN	5x7
6	KOIN EKLR GYGM AAIR AMAS RPAN ATOI TFIT ISO*	6x7
7	MOIN IASA TSOY SH’L TGAH *LAE RDI* URGA AR*M NAFYI*	5x6
8	KATL IVLT UANS AUGR GIVR MITF IAAN AI	6x5
9	SAAE LHNT SAIG NHSF ANIH RNIF *LMD R*	4x8
10	OETA QTOI ‘KOR IOND ZINA YSAA BSTQ OTS*	7x5
11	RTGD AAEI ATQX YISA NANI MOLN YLLA OAIO RV*	5x8
12	TMVN AEOL ANOI PXGA ‘IJS ENIR LRLH DOY* IIAD TLA*	7x4
13	OSSA ‘TAV ZOLR BNII EYSD KUHA IKD*	4x8
14	TVRN MUSI EILI AND* LZAN VTI* EORG JAF*	3x9
15	MIRG ROMM IOTI JANA U*NO NAYI ZN*	5x6
16	SLII MYIL USOA GAZH DTNR ADUO ANTA LR	5x5
17	TLRI RRYV NLAA AGAN TUTR SONU I	7x4
18	KAGM OTAA MOSZ PROM INSU LIIN YNYI	5x7
19	IPTD RALN ROAL MLTE RSAI AETL TRSR RAIU GO*	4x8
20	SITK NVAH UYET GONI NILN RJI* ‘NEI ILS*	7x5

### 3.4.2. Tayanch so‘zli shifrllovchi jadval

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Kalit (k)</b>	<b>Tayanch so‘z</b>
1	*qdn noi* kagf ct*a laoh d*la nyia	4x7	texnika
2	ilui likl atdi kaas ee*a sshn n*sh ivtt *iuy aii* ysaa ff*a u	7x7	magistr
3	Skik tuhi zoes *rim ri*i mpvn *tgy ii*i aurt	6x6	kotiba
4	rhan hyli a*gq amnq *lus ati* arhs id*s iii	5x7	tamoyil
5	ukoia iaun toyn rrli emah uias rpli svrh vyam lad*	5x8	dasturiy
6	xsal hiah xiam vubg qofs oiiy surd dail oaall zith *a	7x6	mantiq
7	gspm hioh giad ruph *ain aa*t tclq *u	5x6	mantiq
8	iisi aymy praa mtil smo* ioet *kst i*rl rz*	7x5	haker
9	sols aghh nlos arim ashm ufar iuit rrid slil s*au ta	6x7	tezlash
10	nhia ilai gatn fask alma rrou ngil liss so*i	6x8	mustaqil

	aglu hr*t saal		
11	uark hlaa troo iala emtm mmax ronp oisb tqiy ydho	5x8	mahsulot
12	airi auoa xhoy rnys bita ikah omnl *slf	4x8	agentlik
13	aild pdsf yaaa hros rm*l rhoi	4x6	piyoda
14	rama tida susa smsh nogh *rfa i	5x5	idora
15	uhrs dlni iiaa cmht tsho aauh ayql sv*a iaho	6x6	enigma
16	tasu hrsi liih mlfk umar sser 1	5x5	nashr
17	riyr yimv lnxi agaj agas sixu rmbh hnfd naa* iiil	5x8	shaftoli
18	oesy hnkj riat ools yseg mata inrp nesr dayi giie fusa *vni t	7x7	teskari
19	lkag brsu aora ikut tmin rape ipsd amer lyha s*rl	5x8	tezlamoq
20	olkl yoab irie sjak idth ar*p aald d*tr ria	5x7	sozlash
21	ayyn sass olgh yhnn iojt ivig daaf anid rrrq i*ia il	6x7	tasodif
22	anrs ahcv dlii hlih odaq sdam isas ahar oqin hs*n iyati	5x9	marketing
23	lins lyas mhaa rhai nrn* tfga i*nr at	5x6	turizm
24	letc coax ilog rnno miio gupy *ltd ua	5x6	moliya
25	metr mllr azie oqoi kna*	4x5	dinar
26	amgl slra teae hald nnnl irav jtme fina	4x8	logarifm
27	auie iang smzd ftiu iaaf isld rniz	4x7	tumaris
28	uari dsss uhae uhva azlt crla iihf mr	5x6	tarmoq
29	slla atmн hsal dmat ixrg ille redo *agg imar *rar laai *ioa	6x8	integral
30	uror ohqt tiqg moia ehli pzdr raak yiam	4x8	xorazmiy
31	ektd ptll uaio irez d*cl okaa *han	4x7	avtobus
32	rlsl nmui eigg sgzn khui aiai	4x6	mansub

### 3.4.3. Matritsa usuli

№	Shifrlangan so‘z
1	dtmliuosvaeparrykuroaioioyhonolmosoonha
2	aitaartuykyfejsanaiionlitoinlgoialairohn
3	tfedso’idaaiinaintiykomnoaoghosaoiodonsiq
4	tisarrramuanhliaiylqoooiooooooofoooisoo
5	netyhannoaitteailrimvooaoooihooooosoorsoo
6	‘zvvoaiatbla farmsxoxooooooooooooootooooouoo
7	gnssrlvaaaoishaaimlsoatoahiodoqmoooliroi
8	dtblhhoxrsanoaisrafiotiomoorrioipolotkaz
9	taiaillhgnosfmnirsghohsodoiuoioauaoalnoq
10	tainiilhanisfanlrsghoasooooluoooruooolkoi

11	rhrnyaqaoaimiayotsmoosooooioooohoooootoo
12	htbaisoxyhdnolmaraoiolhooorsohoaioofaos
13	hkkzoiikinasiiqmlitaoodooooiooooaoqqoqoo
14	anlaagoerqtoeslmftiroshoooisooohiooruoo
15	snrqmireaihiviolesyholsaaaaoioaioootvor

### 3.4.4. Sehrli kvadrat

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	kriu p’os lmet yrvu	16	maa’ bxar xafri y’li
2	tya’ aute ifkn iais	17	sty’ reaf ogga n’ia
3	iik’ dfa’ eisa ntiy	18	sue’ ppyu omer k’tre
4	yal’ qsur inhm raii	19	krhk rido bapl oist
5	hiai nmis laos arhy	20	shl’ hius asfi l’ur
6	xao’ xvbo zaft i’rs	21	his’ smit vooi a’ay
7	ald’ hgaq tmoa i’ir	22	sha’ gian anft lnmr
8	krsi ziim tipo osat	23	cln’ pout omug c’id
9	gali umsu onia trll	24	rasi mqzo iiau llum
10	anl’ uasu ikla trli	25	jat’ edme elvi l’na
11	tas’ mroy himi q’ao	26	iknr ukbs ltil iaol
12	axa’ ibmo thos oiy	27	alsi rmis tiao hnhs
13	sho’ hipa asfl lirr	28	inar stxe alel ramg
14	rai’ sshi tums ahrg	29	hour ozmp ikit geyr
15	hii’ imha chod aaqy	30	elt’ peoc onka r’ht

### 3.4.5. Gamilton usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	YKMP OUET UIIR VS*R	16	IMXF AYAX A*RB AR*L
2	NATE UTFI IAAI KY*S	17	ASEG TNGO YSFR AAII
3	TIEN DIIF Y*SK AA*I	18	RSPE UKMO E*UP YR*T
4	IYSH ARNI LARQ UM*I	19	TKIP ROAB HIOR DLKS
5	YHMO IAAL ARSN ISIH	20	RSIF HLSA L*SH UI*U
6	SXVF AIAZ O*OX BT*R	21	YHMO IAOV LRTS IAIA
7	RAGO LIMT D*QH AA*I	22	RSIF HLNA ANNG AT*M
8	TKIP ROIT SSMZ IOIA	23	DCOU LCMO N*TP UG*I
9	LGMI ATNO LRUU SAIL	24	MRQA ALII SLOM ZUIU
10	IAAL NTKI LRUU SA*L	25	AJDV ALLE T*EE MI*N
11	OTRM AQIH S*YM OI*A	26	LIKI KITK NASU BLRO
12	RABO XOHT AIOI MS*Y	27	SAMA LHIT SNSR IOIH
13	RSIF HLSA OIAH PL*R	28	GITE NRLA AAES XLRM

14	GRSM AAUT IHIS HS*R	29	RHZI OKKI UEPO MTRY
15	YHMO IAHC IAAI HD*Q	30	TEEK LRNO T*CP OA*H

### 3.5.1. Matritsalarni ko‘paytirish usuli

<b>№</b>	<b>Shifrmatn, <math>T_1</math></b>	<b>№</b>	<b>Shifrmatn, <math>T_1</math></b>
1	<78, 36, 64, 90, 104, 88>	2	<82, 72, 121, 66, 72, 72, 49, 56, 40>
3	<111, 82, 134, 108, 68, 87, 177, 126, 196>	4	<61, 91, 102, 94, 145, 161, 83, 104, 124>
5	<39, 114, 185, 76, 164, 186, 130, 215, 239>	6	<71, 30, 139, 156, 121, 188>
7	<45, 91, 8, 151, 314, 187>	8	<92, 92, 118, 60, 47, 75, 100, 128, 122>
9	<119, 162, 104, 78, 118, 89, 139, 206, 94>	10	<78, 57, 38, 122, 151, 93, 109, 59, 37>
11	<55, 72, 118, 52, 115, 29>	12	<65, 122, 125, 68, 184, 150>

### 3.5.2. Xaltaga buyumlarni joylashtirish masalasi

<b>№</b>	<b>Shifrlangan matn</b>	<b>№</b>	<b>Shifrlangan matn</b>
1	170, 177, 232	13	148, 236, 95
2	151, 125, 47	14	47, 141, 108
3	36, 89, 128	15	108, 128, 105
4	151, 171, 177	16	177, 140, 128
5	152, 117, 162	17	59, 201, 156
6	212, 229, 190	18	274, 323, 306
7	117, 103, 34	19	60, 108, 126
8	121, 254, 198	20	185, 169, 121
9	258, 250, 209	21	86, 115, 250
10	171, 119, 128	22	117, 154, 171
11	162, 266, 242	23	182, 236, 260
12	141, 187, 124	24	59, 122, 71

### 3.6.1. Gammalashtirish usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Gamma</b>	<b>№</b>	<b>Shifrlangan so‘z</b>	<b>Gamma</b>
1	cionyek	kabinet	12	jlzzrga	joylash
2	dvlhgrb	dasturi	13	awigmyi	formula
3	kucsifh	yuklash	14	hawnfms	kabinet

4	kekkrdq	yeterli	15	dphtblr	dasturi
5	paowdiq	xavfsiz	16	ryhyich	yuklash
6	uiuwoht	kabinet	17	zegkclz	yeterli
7	aoftfrz	dasturi	18	jeidmah	xavfsiz
8	ymydlsy	yuklash	19	csjpfgu	joylash
9	qeuaaswq	yeterli	20	yixyuwi	formula
10	euezevh	xavfsiz	21	wawhhrb	kabinet
11	loaweht	kabinet	22	uaitgcq	dasturi

### 3.6.2. Uitstonning “ikki kvadrat” usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	IW EN AF BZ WD FY BX .O	17	GH DN UO SH OS JG GY
2	AU BZ L' VU LX UO MO	18	'R __ MU _L J. QA G.
3	VW MP Z' QA JX ZA G.	19	'K LQ JF T' IT BY OP
4	G. XA FY .U IZ C. NV MO	20	JY .Y UB OS RD BA J_ FU
5	CH A_ G. GS ZZ XA LX C.	21	XA VU JG LX KN 'K NS
6	SH YG ZA SI Z_ OR BR	22	CH A_ G. IG ZA OI GS C.
7	GO AL C. C' JH ZB S.	23	XA VU JG MU SK CZ LY MB
8	JY .Y UB Z' ZI GH 'L ZA	24	JB UK XD T' IE Z' YB
9	SK NH BE EK BX OO GS C.	25	J. FI G_ QX NN UK 'K NS
10	MU GO PY FU BX OO GS HG	26	S' 'D GO O_ TC MP Z'
11	OI CD BL CH A_ G. ZA	27	FU CX NS WY TO 'L GB GY
12	'U UQ KG EI QW UR LX .O	28	GO GH XA Z' C. XA 'L ZZ
13	XA VU LX EC GY FR .O	29	.U BZ OK GO 'A TC GO GY
14	SI A_ YM BA J_ GY	30	'K WD OP IW EN AF BZ HG
15	J. Z' SK UZ XA FY PX .C	31	O_ ON O' EK IQ HI OI
16	CH A_ G. HI .X LO VW MO	32	BZ MH FR _L UO GO GY

### 3.6.3. To‘rt kvadrat usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	RXVV_SYOJ.FYNU	17	Z_LVFOO_XQTG.'
2	XIYOBANKWUYIIIZM_Q	18	MIN_IBNF_GU' Q
3	FWI_OWU'_OZM_Q	19	ZIAQ_JHKFQIX.P
4	_QC'FYWQUI_DCESB.'	20	JYEWLXXQJDNK_UY
5	_V'H_QZQO'C'NZ_D	21	C'KWTGNZ_HZIZC
6	O_KDZMOBQH.RIA	22	_V'H_QK.ZMOOZQ_D
7	SB'A_DYU__UMOG	23	C'KWTGIBZFYKII'

8	JYEWLXOWOMZ_‘IZM	24	TBXABJHKUSOWL
9	ZFZVMSZFNUSOZQ_D	25	_GUBV_UWMNXAZIZC
10	IBSBWXUYNUSO	26	_FG.SBS_HNI_OW
11	OOPLI‘_V‘H_QZM	27	UY_WZC’XSX‘IQF.’
12	.ZNSR.YYAU.FI_V	28	SBZ_C’OW_DC’‘IO‘
13	C’KWTGNZTV.’SF	29	WOYODRSBDZHNSB.’
14	OB‘HG‘NKT_.	30	CBJ..PRXVV_SYOTG.’
15	_GCZZFOXC’FY	31	S_XPGYIFKSP’OO
16	_V‘H_QP’EO._UMOG	32	YOB_SFNFOSB.’

### 3.6.4. Xill usuli

<b>№</b>	<b>Shifrlangan so‘z</b>	<b>№</b>	<b>Shifrlangan so‘z</b>
1	KARWEQZZG	16	YGJKO
2	HKCYGBWV	17	PSAYNAUQIPIVWM
3	ZCVCKPIVWSIIWM	18	SAQHMRMMYLTGHI
4	OMGBGRHKZG	19	TYJUCLCHRNEIVHUF
5	MJOOWMWXYZFA	20	OOQVHKFSSP
6	UFFFIIFDUG	21	IIIYNGBWMUL
7	KWYGIPUL	22	FAFSPZNAMQHXUG
8	TYJUCLKPWFQZG	23	YGLJVAKW
9	MQWSBVPQ	24	QVGBIYNGBWM
10	NAHKVAUG	25	UJULHKFSSP
11	MDSHYS	26	BYSUWKZG
12	RCSPYXTN	27	HKYGFAKPGBFA
13	FAFSPZCOVHZG	28	DEYJLWHK
14	CLYVFA	29	WCTBHIYZSJ
15	MJOOWMZSXOZG	30	PMMELJPU

5-bob. AMALIY MASHG‘ULOTLAR UCHUN KO‘RSATMALAR

5.5. OpenSSL kutubxonasidan foydalangan holda ma’lumotlarni xesh qiyimatini hisoblash

3-topshiriq

1	48cc9b01c95e434bd83ffd937593f339
2	5ad63412ff44f9484c6546867299782a
3	4f5ea81cf6cd7446e58e5a9a7611f825
4	4add281df34ff147c02c4fab76927825

5	46523c85efd1e1d65f90cc9a7e147cac
6	dec2249f6250e9d4d163f6bbf69c71a7
7	59593f95f0caf6c6e28b79a8751f7fac
8	4add2d1ff74ff445646c4aa976927927
9	cb4da01d73de785740adf68af612f124
10	4fcbbe12ea59625879785c247694f22a
11	4d5dba15e4ce624ff7af4c937012fa2c
12	4748be02e2cb664873cbc147a17f22b
13	59513191f8c2f8caeb8377a4751f79a8
14	49d43392ec46eac1fe47752d75927faa
15	c256ad0d7ad5715feba65c83fb11fc24
16	4ed2ac1df740704f64234f137795fc25
17	dada289e6648e5cdd55b7aa3f29c7da6
18	44d13f84ed53e6d7fd12dbbb78977fac
19	4add281df34ff147c02c4fab76927825
20	cec93416625bed5cd16a7331f296712e
21	5ad93491fb4bfdc2c92a42ac769f7ca9
22	cec839116e5ae05b5d2bfe17f2977029
23	c9cfa41f755d7855c66ee6a8f090f127
24	5ec03e12fb52f75848734816729f722a
25	41d3b182e4516dd17451d0ad7895fdAA
26	dede3a97724cf7c4c07de82af6987faf
27	5ed13592fb43fcc9684243a7729f79aa
28	cbd5bc15634764475136fbff692fd2d
29	495aba15e0c9664ff3a848137015fa2c
30	dbdbb2137f497e41cd78e13ff29cff2b
31	dbc3b4167751785cc460e723f29cf12e
32	d2d82e0c6a5ae75e5b297a10fe9f7f24
33	5ad93491fb4bfdc2c92a42ac769f7ca9
34	dbd2ab9c634067c7701378b9f29cfAA4
35	4fddab9df64f73c6e52c4d3a7293fba5
36	dcdbaa1e6049664cd37a5932f59cff26
37	dadf3c95724df1c6c03cee28f2997dad
38	d0df3d85785df0d6c82ced38f8997cad
39	44d53b87e957e2d4f9765f3878937faf
40	49513f95e0c2e6c6f28369aa75177fac