2-AMALIY MASHG`ULOT

Simmetrik (mahfiy) kalitli shifrlash tizimlari

Almashtirish usullarining mohiyati – bir alfavitda yozilgan information simvollarni boshqa alfavit simvollari bilan ma'lum bit qoida bo'yicha almashtirishdan iboratdir. Bu guruhga mansub eng sodda usul sifatida **to'g'ridan-to'g'ri almashtirish usulini** ko'rsatish mumkin. Dastlabki informatsiya yoziluvchi A_0 alfavitning s_{0i} simvollariga shifrlovchi alfavitning s_{1i} simvoli mos qo'yiladi. Oddiy xolda ikkala alfavit ham bir xil simvollar to'plamiga ega bo'lishi mumkin. Ikkala alvavitdagi simvollar o'rtasidagi moslik ma'lum bir algoritm bo'yicha **K** simvollar uzunligiga ega bo'lgan dastlabki matn T_0 simvollarining raqamli ekvivalentlarini o'zgartirish orqali amalga oshiriladi.

Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko'rinishida ifodalanishi mumkin:

1-qadam: **[1xR]** o'lchamli dastlabki A_0 alfavitdagi har bir simvol $s_0 \in T(i=1, K)$ ni A_0 alfavitdagi s_{0i} simvol tartib raqamiga mos keluvchi $h_{0i}(s_{0i})$ soniga almashtirish yo'li bilan raqamlar ketma ketligi L_{0h} ni shakllantirish.

2-qadam: L_{0h} ketma-ketligining har bir sonini $h_{1i} = (k_1 x \ h_{0i}(s_{0i}) + k_2) \ (mod \ R)$ formula orqali hisoblanuvchi L_{1h} ketma ketligining mos soni h_{1i} ga almashtirish yo'libilan L_{1h} sonlar ketma ketligini shakllantirish, bu yerda k_1 o'nlik koeffitsient, k_2 esa siljitish koeffitsienti. Tanlangan k_1 va k_2 koeffitsientlar h_{0i} va h_{1i} sonlarining bir ma'noli mosligini ta'minlashi lozim. $h_{1i} = 0$ deb olinganida $h_{1i} = R$ almashinuvi bajarilishi kerak.

3-qadam: L_{1h} ketma ketligining har bir soni $h_{1i}(s_{1i})$ ni **[1xR]** o'lchamli shrifrlash alfavitining mos $s_{1i} \in T_1(i=1, K)$ simvoli bilan almashtirish orqali T_1 shifr matnini hosil qilish.

4-qadam: Olingan shifr matni o'zgarmas **b** uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to'liq bo'lmasa, blok orqasiga mahsus simvol-to'ldirgichlar joylashtirish (masalan, * simvolini).

Misol: *Shifrlash uchun dastlabki ma'lumotlar*:

T_0 = <ҲИМОЯ_ХИЗМАТИ>

A_0= <АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ>

A_1= <ОРЁЬЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЪШБУЮ ҚГН>

R=36 k_1=3 k_2=15 b=4

Algoritmning qadamba-qadam bajarilishi quyidagi natijalarga olib keladi:

1-qadam: L_{0h} = <35,10,14,16,31,36,23,10,9,14,1,20,10>

2-qadam: L_{1h} = <12,9,21,17,36,14,12,9,6,21,18,3,9>

3-qadam: T_1 = <ХЖЕФНВҲЖТЕҚЁЖ>

4-qadam: T_1 = <ХЖЕФ НВҲЖ ТЕҚЁЖ***>

Rasshifrovka qilishda bloklar birlashtirilib, **K** simvolli shifromatn T_1 hosil qilinadi. Rasshifrovka qilish quyidagi butun sonli tenglamani (tselochislennoe uravnenie) yechish kerak bo'ladi:

$$k_1 h_{01} + k_2 = n R + h_{1i}$$

Ushbu tenglamadagi k_1 , h_{11} , k_2 va **R** butun sonlar ma'lum bo'lganda h_{0i} kattaligi **n** ni saralash orqali hisoblanadi. Bu muolajani shifromatnning barcha simvollariga tadbiq qilish uning rasshifrovka qilinishiga olib keladi. Almashtirish usulining kamchiligi sifatida dastlabki va berilgan matnlar statistik ko'rsatgichlarining bir xilligini ko'rsatish mumkin. Dastlabki matn qaysi tilda yozilganini bilgan xolda, kriptoanalitik axborotlarni statistik qayta ishlab, ikkala alfavitdagi simvollar orasidagi mos kelishliklarni aniqlashi va matnni rasshifrovka qilishi mumkin

Polialfavitli almashtirish usullari

Bu usullar yetarlicha yuqori darajadagi kriptoturg'unlikka ega va bunda dastlabki matn simvollarini almashtirish uchun bir necha alfavitlardan foydalanadilar. Rasman polialfavitli almashtirishni quyidagihca tasavvur qilish mumkin. **N** – alfavitli almashtirishda dastlabki A_0 alfavitdagi s_{01} simvoli A_1 alfavitdagi s_{11} simvoli bilan almashtiriladi va hakozo. s_{0N} simvolini s_{NN} simvoli bilan almashtirgandan so'ng $s_{0(N+1)}$ simvolining o'rnini A_1 alfavitdagi $s_{1(N+1)}$ simvoli oladi va xakozo.

Polialfavitli almashtirish algoritmlari ichida **Viginer jadvali (matritsasi)** $T_в$ ni ishlatuvchi algoritm eng keng miqyosda tarqalgan. **Viginer jadvali [RxR]** o'lchamli kvadrat matritsadan iborat bo'lib (**R** - *ishlatilayotgan alfavitdagi simvollar soni*), birinchi qatorda simvollar alfavit tartibida joylashtiriladi. Ikkinchi qatordan boshlab, simvollar chapga bitta o'ringa siljitilgan xolda yoziladi. Siqib chiqarilgan simvollar o'ng tarafdagi bo'shagan o'rinni to'ldiradi (tsiklik siljitish). Agar bu jarayonda kirill alfavitidagi o'zbek alfaviti ishlatilsa, **Viginer martitsasi** quyida keltirilganidek, (**36x36**) o'lchamga ega bo'ladi:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_
БВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_А
ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБ
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБВ
ДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБВГ
ЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБВГД
ЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБВГДЕ

.....

.....

.....

_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ

Shirflash takrorlanmaydigan **M** simvoldan iborat kalit yordamida amalga oshiriladi. Vijinerning to'liq matritsasidan **| (M+1), R |** o'lchamli shifrlash matritsasi $T_ш$ ajratiladi. Bu matritsaning birinchi qatori va birinchi elementlari kalit simvollariga mos keluvchi qatorlardan iborat bo'ladi. Agar kalit sifatida **<ҒЎЗА>** so'zi tanlangan bo'lsa, shifrlash matritsasi $T_ш$ quyidagi beshta qatordan iborat bo'ladi:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_
ҒҲ_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚ
ЎҚҒҲ_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯ
ЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ_АБВГДЕЁЖ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ

Viginer jadvali yordamida shifrlash algoritmi quyidagi qadamlar ketma ketligidan iborat:

1-qadam: Uzunligi **M** simvolli **K** kalitni tanlash.

2-qadam: Tanlangan **K** kalit uchun **| (M+1), R |** o'lchamli shifrlash matritsasi $\mathbf{T_m = (b_{ij})}$ ni qurish.

3-qadam: Dastlabki matnning har bir simvoli $\mathbf{s_{0R}}$ tagiga kalit simvoli $\mathbf{k_m}$ joylashtiriladi. Kalit keraklicha miqdorda takrorlanadi.

4-qadam: Dastlabki matn simvollari shifrlash matritsasi $\mathbf{T_m}$ dan quyidagi qoida bo'yicha tanlangan simvollar bilan quyidagicha tartibda ketma ket almashtiriladi:

1. **K** kalitning almashtiriluvchi $\mathbf{s_{0R}}$ simvoliga mos $\mathbf{k_m}$ simvoli aniqlanadi.
2. Shifrlash matritsasi $\mathbf{T_m}$ dagi $\mathbf{k_m = b_{ij}}$ shart bajariluvchi **i** qator topiladi.
3. $\mathbf{s_{0R} = b_{ij}}$ shart bajariluvchi **j** ustun aniqlanadi.
4. $\mathbf{s_{0R}}$ simvoli $\mathbf{b_{ij}}$ simvoli bilan almashtiriladi.

5-qadam: Shifrlangan ketma-ketlik ma'lum uzunlikdagi (*masalan, 4 simvolli*) bloklarga ajratiladi.

Matnni rasshifrovka qilish esa quyidagicha ketma ketlikda amalga oshiriladi:

1-qadam: Shifrlash algoritmining uchinchi qadamidagidek, shifroformat tagiga kalit simvollari ketma ketligi yoziladi.

2-qadam: Shifromatndan $\mathbf{s_{1R}}$ simvollari va mos kalit simvollari $\mathbf{k_m}$ ketma ket tanlanadi. Shifrlash matritsasi $\mathbf{T_m}$ dagi $\mathbf{k_m = b_{ij}}$ shartni qanoatlantiruvchi **i** qator aniqlanadi. **i** qatorda $\mathbf{b_{ij} = s_{1R}}$ element aniqlanadi. Rasshifrovka qilingan matnda **r** –o'rniga $\mathbf{b_{ij}}$ simvoli joylashtiriladi.

3-qadam: Rashsifrovka qilingan matn ajratilmasdan yoziladi. Xizmatchi simvollar esa olib tashlanadi.

Мисол:

K = <ГЎЗА> kaliti yordamida **T = <ПАХТА ГАРАМИ>** dastlabki matnni shifrlash va so'ngra rasshifrovka qilish talab etilsin. Shirflash va rasshifrovka qilish natijalari quyida keltirilgan:

Dastlabki matn: **ПАХТА_ГАРАМИ**

Kalit: **ҒЎЗАҒЎЗАҒЎЗА**

Almashtirilgan so'nggi matn: **МЎЯТҒЯЕАНЎФИ**

Shifromatn: **МЎЯТ ҒЯЕА НЎФИ**

Kalit: **ҒЎЗА ҒЎЗА ҒЎЗА**

Rasshifrovka qilingan matn: **ПАХТА _ҒАРАМИ**

Dastlabki matn: **ПАХТА _ҒАРАМИ**

Polialfavitli almashtirish usullarining kriptoturg'unligi oddiy almashtirish usullariga nisbatan sezilarli darajada yuqori, chunki ularda dastlabki ketma ketlikning bir simvollari turli simvollar bilan almashtirilishi mumkin. Ammo shifrning statistik usullarga bardoshliligi kalit uzunligiga bog'liq.