KLASSIK SHIFRLASH ALGORITMLARI. BIGRAMM AKSLANTIRISH.

Karimov Abdukodir Abdisalomovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
karimovabduqodir041@gmail.com
Ergasheva Farida Yunus qizi *(TATU)*
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
afarida0630@gmail.com

Annotatsiya: Ma'lumotlarni maxfiyligini ta'minlashning bir necha usullari mavjud bo‘lsada, kriptografik usul o‘zining bardoshligi bilan ajralib turadi. Ma'lumotlarni kriptografik himoyalash qadimdan beri o‘rganilib kelingan bo‘lib ularni klassik shifrlash algoritmlari sinfiga bo‘lish mumkindir. Mavjud klassik shifrlash algoritmlarini ikki turga ajratish mumkin. Bular, o‘rniga qo‘yish va o‘rin almashtirish akslantirishlaridan iborat algoritmlardir. Klassik shifrlash algoritmlarini ishlab chiqish bilan bir qatorda ularni kriptotahlil usullariga bardoshliligini ham tekshirish muhim hisoblanadi. Hozirgi kunda klassik shifrlash algoritmlarining bardoshligi, matematik tahlil qilish va to‘liq tanlash hujumlari orqali sinaladi. Ushbu maqolada o‘rniga qo‘yish akslantirishiga asoslangan klassik shifrlash algoritmlari chastotalar tahlili usuli orqali baholangan hamda hujum oldini olish uchun bigram akslantirishidan foydalanish ko‘satilgan.

Kalit so‘zlar: kriptografiya, shifr (deshifr), transposition, substitution.

Kirish

Odatda klassik shifrlashda va rasshifrovkalashda ikki turdagi akslantirishlardan foydalaniladi. Ulardan biri o‘rniga qo‘yish (**substitution**) akslantirishi, ikkinchisi o‘rin almashtirish (**transposition**) akslantirishlaridir. O‘rniga qo‘yish usuli zamonaviy simmetrik kriptotizimlarning asosi hisoblanadi. O‘rniga qo‘yish kriptotizimlarida har bir belgi (yoki blok) ma‘lum bir qoidaga ko‘ra o‘zgartiriladi. Bu shifrlash usulida harf yoki raqamni boshqa harf yoki raqamga almashtirish orqali matnni yashiradi. Unga misol qilib esa eng birinchi klassik shifrlash algoritmlaridan biri hisoblangan Sezar shifrlash algoritmini misol qilib keltirish mumkin. Sodda matematik operatsiyalarini bajaradigan tizimga asoslangan bu algoritm har bir harfni belgilangan bir son bilan o‘zining alifbodagi joyidan *k* birlikka siljitish orqali shifrlaydi. *M*-ochiq matn belgisini alfavitdagi o‘rni hisoblanib, *m*-alfavit uzunligi bo’lsa, shifrlash jarayoni $C=(M+k) mod m$ formulasi orqali amalga oshiriladi. C shifr belgini alfavitdagi o‘rni. Masalan, ochiq matn sifatida M=DARSLIK so‘zini oladigan bo‘lsak, hamda uni kalit k=4 orqali shifrlash kerak bo‘lsa, shifr matn C=HEVWPMO ko‘rinishida bo‘ladi. Atbash shifrini ham eng qadimgi shifrlash algoritmlardan deyish mumkin. Atbash

shifri alifbodagi harflarni o‘zaro teskari tartibda almashtirishni o‘z ichiga oladi. Boshqacha qilib aytganda, har bir harfning o'rniga uning alifbodagi qarama-qarshi harfi qo'yiladi. Misol uchun shifrlashni ingliz alifbosida amalga oshirsak: Alifbodagi birinchi harf (A) oxirgi harf (Z) bilan o‘zgaradi.Ikkinchi harf (B) oxiridan bitta avvalgi harf (Y) bilan o‘zgaradi.

Kriptotahlil usullari.

Chastota tahlili usuli orqali shifrmatnni deshifrlash(sezar):

Shifrmatn: *OZYE QZCRPE EZ MCTYR ESP AZWTNP. ESP AWLY TD EZ NLENS ESP DFDAPNE LE ESP DELETZY. HP HTWW RTGP ESP DTRYLW HSPY TE TD DLQP EZ XZGP TY. LYJ OPWLJ NZFWO RTGP ESP DFDAPNE ETXP EZ PDNLAP. XLVP DFCP LWW XPXMPCD LCP CPLOJ LE ESP DAPNTQTPO ETXP*

Matnning shifrlangan qismida “ESP” va “RTGP” kabi qismlar takrorlanadi, bu o‘zgarishi mumkin bo‘lgan harflarni aniqlashga yordam beradi. Agar biz tahlilni boshlasak, eng ko‘p uchraydigan harfni topishimiz kerak, bu asosan “E” harfi bo‘lishi mumkin. ESP so‘zi bir necha marta takrorlangsni uchun bu so‘zni “the” ga moslashtirishni sinab ko‘rishimiz mumkin, chunki “the” so‘zi ingliz tilida keng tarqalgan. **E harfi -> T harfi** Ingliz alifbosida E harfi 5-chi o‘rinda turadi va T harfi 20-chi o‘rinda turadi. Shunday qilib, E harfidan T harfigacha bo‘lgan surish miqdorini topishimiz mumkin: T (20) - E (5) = 15 Demak, k = 15 bo‘ladi, ya'ni Sezar shifrlashida harflar 15 birlikka surilgan.

Ochiq matn: *THIS MESSAGE IS SECRET THE BROWNING. THE FINAL IS A CHANCE THE ADVENTURE OF THE CELEBRITY. TO TURN YOUR HEAD THE NARRATIVE FORM IS A LOOK AT WHAT IS HAPPENING. YOU SHOULD FIND OUT WHERE THE ADVENTURE MIGHT BE DANGEROUS*

Affin shifrlash algoritmi — bu klassik shifrlash usullaridan biri bo‘lib, harfning pozitsiyasi va qo‘shimcha bir doimiy qiymat orqali o‘zgartiriladigan algoritmga tayangan holda ishlaydi. Bu algoritm Sezar usuliga o‘xshash bo‘lsa-da, unda faqat bir xil raqamni qo‘llashdan ko‘ra, ikkita parametr orqali harflarni o'zgartirish qo‘llaniladi. Ya’ni bu algoritm sonlar juftligini shifrlashga asoslangan. a va b parametrlar mos ravishda ko’paytirish va qo‘shish parametrlari, m esa alfavitdagi belgilar soni va x belgini alifbodagi raqami bo’lsa shifr matn $C=(a\times x+b)modm$ formula orqali hosil qilinadi(a va m qiymatlar o’zaro tub bo‘ladi). Masalan, M (ochiq matn)=MUTLAQO ni affin algoritmi orqali shifrlash jarayoni quyidagicha kechadi:

a=3; b=7 deb tanlab olingan.

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
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

M harfi 12 raqamiga to‘g‘ri keladi. C_1=(3×12+7)mod26=43 mod26=17. 17-raqamda R belgisi turgani uchun M R ning o‘rnida turgani kelib chiqadi. Huddi shu holat barcha

harflar uchun takrorlanganda "RPMOHDX" shifr matn hosil bo'ladi. Rasshifrovkalash uchun x=a^{-1}(C-b)modm dan foydalaniladi.

Chastota tahlili usuli orqali shifrmatnni deshifrlash(affin):

Shifrmatn: *WKLV LV WHVW WR FDWFK YDU\A VKDUN. ZH KDYH WR PDNH VXUH WKDW DOO WKH QHA[DUH LQ SODFH. LI ZH PLVV DQ\WKLQJ, WKH VKDUN PLJKW HVFDSH. DQG WKLV JDPH, WLPH LV RI WKH HVVHQFH, DQG ZH PXVW DFW IDVW.*

Bu shifrmatndagi eng ko'p uchraydigan harflarni (**W, K, V, L, H)** ingliz alifbosidagi **E, T, A, O, I** kabi eng ko'p uchraydigan harflarga moslashtirish mumkin. Yoki ikki xonali so'z LV ni ingliz tilidagi IS so'ziga tenglashtirib ko'rish orqali ham natijaga erishish mumkin. Agar I L ning o'rnida turibdi deb hisoblansa, k=3 ekanligi oydinlashadi.

Ochiq matn: *THIS IS TEST TO CATCH VARA SHARK. WE HAVE TO MAKE SURE THAT ALL THE NEXT ARE IN PLACE. IF WE MISS ANYTHING, THE SHARK MIGHT ESCAPE. AND THIS GAME, TIME IS OF THE ESSENCE, AND WE MUST ACT FAST.*

O'rin almashtirishda ochiq matnda qanday belgilar berilgan bo'lsa shu harflarni o'zi bilan shifrlash amalga oshiriladi, ya'ni faqatgina ularning pozitsiyasi ma'lum qoida bo'yicha almashtiriladi. O'rin almashtirishga misol qilib Kolon shifrini keltirish mumkin. Bu metod matnni ustunlarga joylashtirish orqali amalga oshiriladi va bu usul matndagi harflarni o'rin almashtirishni ta'minlaydi. Bu metodda, matnni to'liq o'qishning o'zi orqali shifrlash ishlari amalga oshiriladi. Kolon shifrida, matnni ustunlarga joylashtirishdan avval, ustunlar sonini tanlash kerak bo'ladi. Ustunlar soni matnning uzunligiga mos bo'lishi kerak. Agar matnning uzunligi ustunlar soniga bo'linmasa, qolgan bo'sh joylar maxsus belgilar yoki tasodifiy harflar bilan to'ldiriladi. Matnni ustunlar bo'ylab vertikal yozish kerak bo'ladi. Masalan, agar matnni 5 ta ustunga joylashtirish kerak bo'lsa va ochiq matn M=ERGASHEVA FARIDA bo'lsa,

E	R	G	A	S
H	E	V	A	F
A	R	I	D	A

Shifrlangan matn C=EHARERGVIAADSFA bo'ladi.

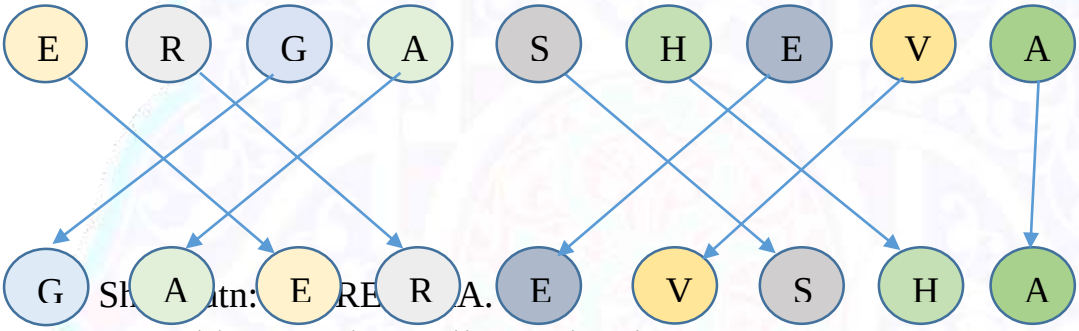
Kolon usulida shifrlangan matnni shifrlash qanday osonlik bilan kechsa, deshifrlash ham shunday oson bo'ladi. Deshifrlash uchun matnni qayta ustunlarga ko'chirish kifoya qiladi. Agar ustunlar soni ma'lum bo'lmasa Shifrlangan Matnning Uzunligini Tahlil Qilish, Chastotalar Tahlili yoki Shifrlangan Matnni Eksperimentally (Sinov orqali) Deshifrlash kabi usullardandan foydalanish mumkin. Agar ustunlar sonini tahmin qilib deshifrlamoqchi bo'lsak, Uzunlik=Ustunlar soni×Qatorlar soni dan foydalanish mumkin.

Yuqorida berilgan shifrmatn 15 ta belgidan iborat bo’lgani uchun ustunlar soni 3 va qatorlar soni 5 yoki ustunlar soni 5 va qatorlar soni 3 ta deb olindi:

E	H	A
R	E	R
G	V	I
A	A	D
S	F	A

Hosil bo’lgan matn: ERGASHEVAFARIDA.

Sodda o’rin almashtirishga misol: Ochiq matn:ERGASHEVA.



Shifrmatn: GAERAEVSHA.

Yuqorida sanab o‘tilgan barcha algoritmlar yordamida shifrlangan ma’lumotlarni harflar chastotasi yoki boshqa qo’shimcha usullar orqali osongina deshifrlash mumkinligi tekshirib ko’rildi. Agar shifrmatn ingliz alifbosi yordamida shifrlangan bo’lsa, qayd qilib o‘tish joizki, ingliz tilidagi so‘zlarda a, i va e harflarini boshqalariga nisbatan ko’p ishlatilishini sezish mukin. Demak, shifrlangan matnda eng ko‘p takrorlangan harflar a,i va e harflari o’rnida kelgan bo‘lishi mumkin. Bu kamchilikni oldini olish uchun Bigramm akslantirishdan foydalanish mumkin. Sezar algoritmida har bitta harf alohida shifrlangani uchun uni deshifrlash oson deyilgan edi. Bigrammning ustunlik tomoni esa deshifrlash jarayonini sekinlashtirish maqsadida harflar juftligi bir amalning o‘zida shifrlanadi. Shifrlashning bu usuli, ayniqsa, **chastota tahlili** kabi usullarni qo‘llab, tez buzilishi mumkin bo‘lgan klassik algoritmlardan samaraliroqdir. Bigramm usuli harflar juftliklarini bitta qilib shifrlagani uchun tabiiyki ochiq matn elementlari soni juft bo’lishi kerak. Agar ochiq matn elementlari toq bo‘lsa uning ohiriga belgi qo‘shish orqali juft qilinadi. Bu usulni Polybius kvadrati yordamida ishlatish mumkin. **Polybius kvadrati** – bu 5x5 o‘lchamdagi jadval bo‘lib, unda harflar va raqamlar mos ravishda joylashtiriladi. Har bir katakka bir harf yoki raqam berilgan, va shifrlash jarayonida matnni shifrlash uchun har bir harfning mos keladigan raqamlari ishlatiladi. Va harflarni (satr,ustun) ko’rinishida ifodalaymiz.

	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

Har bir bigramm uchun, masalan **BI**, “B” harfi **(1,2)** pozitsiyasida, “I” harfi esa **(2,4)** pozitsiyasida joylashgan. Shunday qilib, **BI** bigrammi **12 24** raqamlari bilan shifrlanadi. Masalan,

Ochiq matn= **BIGRAMM SHIFRLASH POLYBIUS KVADRATI YORDAMIDA HAM ISHLAYDI**

Belgilarni juftliklarga ajratib chiqamiz: **BI GR AM MS HI FR LA SH PO LY BI US KV AD RA TI YO RD AM ID AH AM IS HL AY DI**

- **BI**: B → (1, 2), I → (2, 4) → 12 24
- **GR**: G → (2, 2), R → (4, 2) → 22 42
- **AM**: A → (1, 1), M → (3, 2) → 11 32 va har bir juftliklar shifrlangan holatga kelganida, 12 24 22 42 11 32 32 43 23 24 21 42 31 11 43 23 35 34 31 54 12 24 45 43 25 51 11 14 42 11 44 24 54 34 42 14 11 32 24 14 11 23 11 32 24 43 23 31 11 54 14 24 shunday raqamlar kombinatsiyasi ko‘rinishida bo’ladi.

Shu tarzda, bigramm shifrlash Polybius kvadrati yordamida harflarni ikkilik (bigram) juftliklariga ajratib, ularni jadvaldagi raqamlar bilan almashtiradi. Bu usul **Sezar** yoki **Affin** kabi shifrlashlarga qaraganda yanada xavfsizroq va kuchliroq bo‘ladi.

Xulosa

Mazkur maqolada quyidagi natijalarga erishildi:

- Sezar, Affin va Kolon shifrlarining barcha variantlari, ayniqsa ularning ishlash prinsipi va tartibiga qarab, chastota tahlili usuliga nisbatan zaifliklarga ega ekanligi aniqlandi.

- Bigramm usuli yordamida yuqorida keltirilgan zaifliklarning oldini olish imkoniyatlari ko‘rsatib o‘tildi.

- Sezar, Affin va Kolon shifrlari chastota tahlili usuliga bardoshli emasligi keltirildi.

- Bigramm usulining qo‘llanilishi shifrlash metodlarini yanada xavfsizroq qilishga yordam berishi aniqlandi.

Foydalanilgan adabiyotlar ro‘yxati

1. Kiberxavfsizlik asoslari: o‘quv qo‘llanma / S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov; -T.: “Iqtisodiyot-Moliya”, 2021. - 228 b.

2. Classical Ciphers and Cryptanalysis Brian Carter and Tanja Magoc September 11, 2007

3. Kriptografiya 1: o‘quv qo‘llanma / Z.T.Xudoyqulov, Sh.Z.Islomov, U.R.Mardiyev;-T.: “Metodist nashriyoti” , 2024. -213 b.

Foydalanilgan elektron saytlar ro‘yxati

1. https://www.geeksforgeeks.org/implementation-affine-cipher/

2. https://github.com/AlexeyZatsepin/Cryptography-Athen-bigram-cipher

3. https://www.researchgate.net/publication/325049442_Bigram_cipher