MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(8)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №4
Vol.1, Iss.4, 2024 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2024 YIL

Jurnal quyidagi bazalarda indekslanadi:

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

DIFFIE-HELLMAN ALGORITMI VA XAVFSIZ KALIT ALMASHISH PROTOKOLLARI

Arabboyev Alisher Avazbek o‘g‘li,
TATU Farg‘ona filiali
“Axborot xavfsizligi” kafedrasi assistenti
E-mail: alisher_arabboev@mail.ru

Annotatsiya: Ushbu maqolada kalitlarni xavfsiz almashishda foydalanuvchi protokollarning turlari va ularga bo‘ladigan tahdidlar hamda Diffie-Hellman kalitlarni almashish algoritmi to‘g‘risida ma’lumot berilgan.

Kalit so‘zlar: kriptografik protokollar, xavfsiz kalit, xavfsiz aloqa, autentifikatsiya, kibertahdidlar

Kirish

Kriptografik protokollarni tarmoq orqali ikki yoki undan ortiq tomonlar o‘rtasida xavfsiz aloqa va ma’lumot almashishni tartibga soluvchi qoidalar va protseduralar to‘plami sifatida tushunish mumkin. Ushbu protokollar ma’lumotlarning maxfiyligi, yaxlitligi va haqiqiyligini ta’minlash uchun kriptografik algoritmlardan foydalanadi.

Diffie-Hellman kalit almashinuvi sxemasi xavfsiz bo‘lmagan aloqa kanali orqali muloqot qilishda umumiy maxfiy kalitni olishning birinchi amaliy usuli edi. 1976-yilda Uitfild Diffi va Martin Xelman tomonidan ixtiro qilingan. Keyingi yillarda birinchi assimetrik shifrlash algoritmi RSA ixtiro qilindi, u xavfsiz bo‘lmagan kanal orqali aloqa muammosini tubdan hal qildi, endi har bir tomon bir xil maxfiy kalitning nusxasiga ega bo‘lishini talab qilmaydi.

Diffie-Hellman algoritmida nazariy jihatdan ishtirokchilar soni cheklanmagan. Har bir ishtirokchi o‘ziga xos xususiyatlarga ega bo‘lgan kalitlarni yaratadi va ulardan umumiy maxfiy kalitni yaratish uchun foydalanadi. Ushbu maqolada ishtirokchilar soni uchta bo‘lganda Diffie-Hellman algoritmi yordamida qanday qilib maxfiy kalit yaratish mumkinligi ko‘rib chiqilgan.

Tadqiqot usuli

Kriptografik kalitlarni almashish protokollari xavfsiz bo‘lmagan aloqa kanali orqali tomonlar o‘rtasida kriptografik kalitlarni xavfsiz almashish uchun ishlatiladigan usullar to‘plami hisoblanadi. Kriptografik kalit almashish protokollari zamonaviy kriptografiyada muhim rol o‘ynaydi, turli ilovalarda xavfsiz aloqani osonlashtiradi, shu jumladan xavfsiz elektron pochta, onlayn banking va virtual xususiy tarmoqlar (VPN). Asosan, ushbu protokollar ikki yoki undan ortiq tomonlarga xabarlarni shifrlash va shifrini ochish uchun ishlatilishi mumkin bo‘lgan umumiy kriptografik kalitni yaratishga imkon beradi, bu esa potensial buzilgan tarmoqlarda ham xavfsiz aloqani ta’minlaydi.

Kriptografik kalit almashish protokollari ularni xavfsiz aloqada ajralmas holga keltiradigan bir qator afzalliklarni taqdim etadi [1]:

Maxfiylik - ushbu protokollar, agar aloqa ruxsatsiz shaxs tomonidan ushlangan bo‘lsa ham, umumiy kalit sir bo‘lib qolishini ta’minlaydi;

Butunlik - ular almashtirilgan kalitning yaxlitligini saqlashga yordam beradi va yomon niyatli shaxslar tomonidan o‘zgartirilishining oldini oladi;

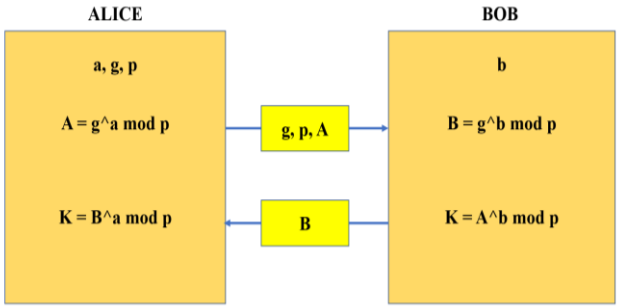
Autentifikatsiya – ko‘pgina kalit almashish protokollari autentifikatsiya mexanizmlarini o‘z ichiga oladi, bu kalit qonuniy tomon bilan almashtirilishini ta’minlaydi.

Ko‘pgina kalit almashish protokollari bir juft kalitdan foydalanadi bular: ochiq kalit va egasi tomonidan maxfiy saqlanadigan yopiq kalit. Ushbu kalitlarning xavfsizligi protokol uchun asos hisoblanadi.

Ushbu protokollar kalit almashinuvini osonlashtirish uchun RSA yoki ECC (elliptik egri chiziqlar kriptografiyasi) kabi turli xil shifrlash algoritmlariga tayanadi. Algoritmni tanlash protokolning xavfsizligi, tezligi va samaradorligiga ta’sir qilishi mumkin. Kriptografik kalit almashinuvi

ko‘pincha xavfsizlikni ta’minlash uchun katta tub sonlarni (RSA) faktorizatsiyalash yoki diskret logarifmlarni (Diffie-Hellman) yechish qiyinligi kabi murakkab matematik muammolarni qo‘llaydi [2].

Diffie-Hellman kalit almashinuvi (DH) - bu ikki tomonga sirni bevosita uzatmasdan xavfsiz bo‘lmagan kanal orqali umumiy sir yaratish imkonini beradi. Diffie-Hellmanning xavfsizligi diskret logarifm muammosini hal qilish qiyinligiga asoslanadi[3].



1-rasm. **Diffie-Hellman algoritmi**

Algoritmdan foydalanish uchun har bir tomon:

- Tasodifiy natural son a – shaxsiy kalit hosil qiladi;
- Masofaviy tomon bilan birgalikda *p* va *g* umumiy parametrlarini o‘rnatadi (odatda p va g qiymatlari bir tomonda hosil qilinadi va boshqa tomonga o‘tkaziladi), bu yerda [4]:

p – tasodifiy tub son ((p-1)/2 tasodifiy tub son bo‘lishi kerak);

g – mod p bo‘yicha ibtidoiy ildiz bo‘lishi kerak (shuningdek tub son);

Demak, g soni p sonining ibtidoiy ildizi bo‘lishi uchun quyidagi (1) formulada berilgan shart bajarilishi kerak:

$$g^{(p-1)} \bmod p = 1 \qquad (1)$$

bunga qo‘shimcha ravishda g ning har bir darajasi $g^1, g^2, g^3, g^4, g^5, \ldots g^{(p-1)}$ modul p ga nisbatan barcha qoldiqlarni 1 dan (p-1) gacha hosil qilishi kerak bo‘ladi. Bu protokolni xavfsiz qiladi, chunki agar g ibtidoiy ildiz bo‘lsa, tomonni maxfiy kalitni hisoblashda keng imkoniyatlar yaratadi.

Natijalar

Diffie-Hellman algoritmidan foydalanish faqat ikkita ishtirokchi bilan cheklanmaydi. U cheksiz miqdordagi foydalanuvchilarga qo‘llanilishi mumkin. Ishtirokchilar soni uch ta bo‘lganida, harakatlar ketma-ketligi quyidagicha bo‘ladi.

- Tomonlar **p** va **g** parametrlarni tanlash bo‘yicha kelishib oladi;
- Tomonlar Alice, Bob va Carol o‘z kalitlarini ishlab chiqadilar. Mos ravishda a, b, c;
- Alice $\mathbf{g^a \bmod p}$ ni hisoblab, Bobga yuboradi;
- Bob $\mathbf{(g^a)^b \bmod p = g^{ab} \bmod p}$ hisoblaydi va natijani Carolga yuboradi;
- Carol $\mathbf{(g^{ab})^c \bmod p = g^{abc} \bmod p}$ hisoblab, umumiy maxfiy kalitni oladi;
- Bob $\mathbf{g^b \bmod p}$ ni hisoblab, Carolga yuboradi;
- Carol $\mathbf{(g^b)^c \bmod p = g^{bc} \bmod p}$ hisoblaydi va natijani Alicega yuboradi;
- Alice$\mathbf{(g^{bc})^a \bmod p = g^{bca} \bmod p}$ ni hisoblab, umumiy maxfiy kalitni oladi;
- Carol $\mathbf{g^c \bmod p}$ ni hisoblab, Alicega yuboradi;
- Alice $\mathbf{(g^c)^a \bmod p = g^{ca} \bmod p}$ hisoblaydi va natijani Bobga yuboradi;
- Bob $\mathbf{(g^{ca})^b \bmod p = g^{cab} \bmod p}$ ni hisoblab, umumiy maxfiy kalitga ega bo‘ladi.

Natijada Alice, Bob va Carol $\mathbf{g^{abc} \bmod p = g^{bca} \bmod p = g^{cab} \bmod p}$ umumiy kalitga ega bo‘lishadi.

Ishtirokchilar soni uch ta bo‘lganida g = 11, p = 29 parametrlarini tanlab olamiz va har bir ishtirokchi uchun umumiy kalitni hosil qilish qarayonini quyidagi jadval orqali ko‘rib chiqamiz:

2-jadval. **Diffi-Hellman algoritmi yordamida umumiy kalitni hosil qilish**

№	Alice	Bob	Carol
1	a=12 yopiq kalit	b=4 yopiq kalit	c=17 yopiq kalit
2	Ochiq kalit: $A = g^a \bmod p$ $A = 11^{12} \bmod 29 = 23$	Ochiq kalit: $B = g^b \bmod p$ $B = 11^4 \bmod 29 = 25$	Ochiq kalit: $C = g^c \bmod p$ $C = 11^{17} \bmod 29 = 3$
3	A ⟹ B ⟹ C	$A^b \bmod p = (g^a \bmod p)^b \bmod p$ $23^4 \bmod 29 = 20$	Umumiy kalit K_c $(AB)^c \bmod p = (g^{ab} \bmod p)^c \bmod p$ $20^{17} \bmod 29 = 25$
4	Umumiy kalit K_a $(BC)^a \bmod p = (g^{bc} \bmod p)^a \bmod p$ $23^{12} \bmod 29 = 25$	B ⟹ C ⟹ A	$B^c \bmod p = (g^b \bmod p)^c \bmod p$ $25^{17} \bmod 29 = 23$
5	$C^a \bmod p = (g^c \bmod p)^a \bmod p$ $3^{12} \bmod 29 = 16$	Umumiy kalit K_b $(CA)^b \bmod p = (g^{ca} \bmod p)^b \bmod p$ $16^4 \bmod 29 = 25$	B ⟸ A ⟸ C

$\mathbf{K_a = K_b = K_c = 25}$ ekanligi kelib chiqdi. Bu jarayonda har bir ishtirokchi o‘zining ochiq kalitini

ikkinchi ishtirokchiga uzatdi. Ikkinchi ishtirokchi birinchi ishtirokchining ochiq kaliti va o‘zining yopiq kalitidan foydalanib kalit hosil qiladi va natijani uchinchi ishtirokchiga umumiy kalit hosil qilish uchun yuboradi.

Muhokama

Kalit almashinuvi protokollarini to‘g‘ri amalga oshirish turli omillarni, jumladan, kalitlarni boshqarish, algoritm tanlash va yon kanal hujumlariga qarshilikni diqqat bilan ko‘rib chiqishni talab qiladi. Kalitlarni hosil qilish jarayonida tomonlar to‘g‘ri autentifikatsiya qilinmasa, kalit almashish protokollari o‘rtadagi odam hujumlariga nisbatan zaif bo‘lishi mumkin, bunda tajovuzkor tomonlar o‘rtasidagi aloqani to‘xtatib, o‘zgartiradi [5].

Kvant hisoblashning paydo bo‘lishi ko‘plab mavjud kalit almashinuv protokollariga, xususan, RSA va Diffie-Hellmanga asoslangan protokollarga potentsial xavf tug‘diradi. Kvantdan keyingi kriptografiya kvant hujumlariga chidamli yangi protokollarni ishlab chiqishga intilayotgan rivojlanayotgan sohadir.

Xulosa

Kriptografik protokollarni loyihalash, yaratish, takomillashtirish va yangilashning murakkab jarayoni davom etmoqda. Bu yangi qo‘llash sohalarining paydo bo‘lishi, mumkin bo‘lgan amaliy vaziyatlarning xilma-xilligi va protokollarga yangi talablarni ishlab chiqish, shuningdek, ularning xavfsizligini tahlil qilish bo‘yicha doimiy harakatlar bilan bog‘liq, buning natijasida tobora ko‘proq yangi zaifliklar va hujumlar aniqlanmoqda.

Foydalanilgan adabiyotlar

1. A.O.Po‘latovna, X.P.Hasanov, M.H.Nazarova, I.U.Xolimtayeva, O.D.Nuritdinov. Axborot xavfsizligi protokollari / o‘quv qo‘llanma - Toshkent, -2019. – 168b.

2. M.Aripov, A.S. Matyakubov Axborotlarni himoyalash usullari, 2014.

3. Manoj Ranjan Mishra, Jayaprakash Kar, “A STUDY ON DIFFIE-HELLMAN KEY EXCHANGE PROTOCOLS” // International Journal of Pure and Applied Mathematics, -Volume 114, - No. 2, - 2017, - 179-189

4. W. Diffie, P. van Oorschot and M. Wiener, “Authentication and Authenticated Key Exchange”, Designs, Codes and Cryptography, 2, - 1992, - pp.107-125.

5. C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. // In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, - volume 175, - page 8. - New York, - 1984