

MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI
FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

“AL-FARG‘ONIIY 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



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'oniyl avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») 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

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2024 YIL

TAHRIR HAY'ATI

Maxkamov Baxtiyor Shuxratovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

Muxtarov Farrux Muhammadovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

Arjannikov Andrey Vasilevich,

Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

Satibayev Abdugani Djunosovich,

Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

Rasulov Akbarali Maxamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

Yakubov Maksadxon Sultaniyazovich,

Muhammad al-Xorazmiy nomidagi TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

G'ulomov Sherzod Rajaboyevich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

G'aniyev Abduxalil Abdjalioviich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

Zaynidinov Hakimjon Nasritdinovich,

Muhammad al-Xorazmiy nomidagi TATU Kompyuter injiniringi fakulteti, Sun'iy intellekt kafedrasida texnika fanlari doktori, professor

Abdullayev Abdujabbor,

Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

Qo'ldashev Obbozjon Hakimovich,

O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

Ergashev Sirojiddin Fayazovich,

Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

Polvonov Baxtiyor Zaylobiddinovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

Zulunov Ravshanbek Mamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Dasturiy injiniring kafedrasida dotsenti, fizika-matematika fanlari nomzodi

Abdullaev Temurbek Marufovich,

Muhammad al-Xorazmiy nomidagi TATU Axborot texnologiyalari kafedra mudiri, texnika fanlar bo'yicha falsafa doktori

Zokirov Sanjar Ikromjon o'g'li,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, To‘xtasinov Azamat G‘ofurovich, NOYOB MIS METALL KLASTERLARINING GEOMETRIK TUZILISHINI KOMPYUTER EKSPERIMENTI ORQALI TADQIQ ETISH	7-11
Далиев Бахтиёр Сирожидинович, Решение уравнения Абеля методом оптимальных квадратурных формул	12-15
Saidov Mansurjon Inomjonovich, Tartiblangan statistikalarda baholarni topish usullari	16-21
Kayumov Ahror Muminjonovich, TRIKOTAJ TO‘QIMASI TARKIBIDAGI IP XUSUSIYATLARI VA DEFORMATSIYAGA TA’SIRI	22-27
Muradov Farrux Abdukaxarovich, Kucharov Olimjon Ruzimurotovich, Narzullayeva Nigora Ulugbekovna, Eshboyeva Nodira Faxriddinovna, GAZLI ARALASHMALAR VA ZARARLI MODDALARNING ATMOSFERADA TARQALISHI MASALASINI YUQORI TARTIBLI APPROKSIMATSIYANI QO‘LLAGAN HOLDA UNI SONLI YECHISH ALGORITMI	28-37
Maniyozov Oybek Azatboyevich, NAVIER-STOKES TENGLAMASINI KLASSIK HAMDA KLASSIK BO‘LMAGAN YECHIMLARINI VA UNING O‘ZIGA XOSLIGI	38-44
Tillavoldiyev Azizbek Otobek o‘g‘li, Tibbiy tasvirlarda reprezentativ psevdoobyektlarni segmentatsiyalash algoritmi	45-51
Fayziev Shavkat Ismatovich, Karimov Sherzod Sobirjonovich, Muxtarov Alisher Muxtorovich, DDoS hujumlarni aniqlashda neyron tarmoqlarga asoslangan gibrid modellarni ishlab chiqish	52-58
Rasulmuxamedov Maxamadaziz Maxamadaminovich, Shukurova Shohsanam Bahridin qizi, Mirzaeva Zamira Maxamadazizovna, MURAKKAB SHAKLLI, HAJMLI JISMLARNING ELASTOPLASTIK DEFORMATSIYASINING MATEMATIK MODELLARINI QURISH	59-63
Uzakov B.M., Melikuziyev M.R., TARELKALI TURDAGI REKTIFIKATSIYA KOLONNANING HARORAT KO‘RSATKICHLARINI MOSLASHUVCHAN BOSHQARISH	64-72
Порубай Оксана Витальевна, Эволюционные алгоритмы в задачах оптимизации режимов работы региональных энергосистем	73-77
Musayev Xurshid Sharifjonovich, TRIKOTAJ TO‘QIMA TASVIRLARINI ANIQLASH VA RAQAMLI ISHLOV BERISH USULLARI	78-81
Нурдинова Разияхон Абдихаликовна, ПОЛУПРОВОДНИКИ КАК МАТЕРИАЛЫ ДЛЯ ИЗГОТОВЛЕНИЯ ТЕРМОГЕНЕРАТОРОВ В МЕДИЦИНЕ	82-85
Мовлонов Пахловон Ибрагимович, ДЕГРАДАЦИЯ СЭ ПОД ДЕЙСТВИЕМ ИЗЛУЧЕНИЯ ВИДИМОЙ ОБЛАСТИ СПЕКТРА И ИОНИЗИРУЮЩЕЙ РАДИАЦИИ	86-90
Севинов Жасур Усманович, Темербекова Барнохон Маратовна, Мамазаров Улугбек Бахтиёр угли, Бекимбетов Баходир Маратович, Синтез методов цифровой регистрации в системах сбора и обработки измерительной информации для обеспечения достоверности в информационно-управляющих системах	91-96
O.S.Rayimdjonova, ISSIQLIK VA OPTOELEKTRON O‘ZGARTIRGICHLARNING ASOSIY TAVSIFLARI VA UMUMIY MASALALARI	97-100
Muradov Farrux Abdukaxarovich, Narzullayeva Nigora Ulugbekovna, Kucharov Olimjon Ruzimurotovich, Eshboyeva Nodira Faxriddinovna, ATMOSFERANING CHEGARAVIY QATLAMIDA GAZLI ARALASHMALAR VA ZARARLI MODDALARNING TARQALISHI MASALASINI O‘ZGARUVCHILARNI ALMASHTIRISH USULI YORDAMIDA IFODALASH VA UNING SONLI YECHISH ALGORITMI	101-107
Акбаров Давлатали Егиталиевич, Акбаров Умматали Йигиталиевич, Кучкоров Мавзуржон Хурсанбоевич, Умаров Шухратжон Азизжонович, РАЗРАБОТКА АЛГОРИТМА СИММЕТРИЧНОГО БЛОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ СЕТИ ФЕЙСТЕЛЯ ПО КРИПТОСТОЙКИМИ БАЗОВЫМИ ТАБЛИЧНЫМ ПРЕОБРАЗОВАНИЯМИ	108-113
Xolmatov Abrorjon Alisher o‘g‘li, Xoshimov Baxodirjon Muminjonovich, MAZUTNI REKTIFIKATSIYALASH QURILMALARINING VAKUUM YARATISH TIZIMINI TAKOMILLASHTIRISH	114-125
Goipova Xumora Qobiljon qizi, Dasturiy ta‘minotdagi xatolarni avtomatik topish va tuzatish uchun o‘qitiladigan algoritmlar	126-129
Xudoykulov Z.T., Xudoynazarov U.U., YETARLI GOMOMORFIK SHIFRLASH ALGORITMLARI YORDAMIDA AXBOROTNI KRIPTOGRAFIK HIMOYALASH	130-135
Калашников Виталий Алексеевич, ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОЗДАНИЯ СПЕЦИАЛЬНОГО АГРЕГАТА ДЛЯ ПОСЕВА СЕМЯН ПШЕНИЦЫ В МЕЖДУРЯДЬЯ ХЛОПЧАТНИКА И ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ПАРАМЕТРОВ ШАРНИРНО-ПОЛОЗОВИДНОГО СОШНИКА	136-143
Ermatova Zarina Qaxramonovna, To‘qimachilik sanoatida Linter qurilmalarining ahamiyatini o‘rganish va kuzatish	144-146
Tolipov Nodirjon Isaqovich, Madibragimova Iroda Mukhamedovna, ON A NON-CORRECT PROBLEM FOR A BIHARMONIC EQUATION IN A SEMICIRCLE	147-151
Xudoykulov Zarif Turakulovich, Qozoqova To‘xtajon Qaxramon qizi, PRESENT YENGIL VAZNLI KRIPTOGRAFIK ALGORITMINING TAHLILI	152-157
D.S.Yaxshibayev, A.H.Usmonov, Yer osti sizot suvlari sathi o‘zgarishini matematik modellashtirish va sonli tadbiq qilish	158-162

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Tojimatov Dostonbek Xomidjon o'g'li, KIBERRAZVEDKA AMALIYOTIDA IOC, LOG VA DARK WEB MONITORING MA'LUMOTLARINING INTELLEKTUAL INTEGRATSIYASIGA ASOSLANGAN KIBERTAHDIDLARNI ERTA ANIQLASH MODELI	163-167
Mirzayev Jamshid Boymurodovich, MATNLI MA'LUMOTLARNI YASHIRIN UZATISHDA STEGANOGRAFIK USULLARDAN FOYDALANISH	168-172
Kabildjanov Aleksandr Sabitovich, Pulatov G'iyos Gofurjonovich, Pulatova Gulxayo Azamjon qizi, LSTM MODELI ASOSIDA OB-HAVO SHAROITLARINING YURAK-QON BOSIMI KASALLIKLARIGA TA'SIRINI BASHORATLASH	173-177
Erejevov Keulimjay Kaymatdinovich, SHAXSNI OVOZI ORQALI IDENTIFIKATSIYALASH ALGORITMLARI	178-183
Muxtarov Ya., Obilov H., OPERATOR USULI YORDAMIDA O'ZGARMAS KOEFFITSIENTLI CHIZIQLI DIFFERENSIAL TENGLAMALAR SISTEMASINI INTEGRALLASH	184-188
Tillaboev Muxiddinjon, PILLANI NAMLIGINI O'LCHISHNING OPTOELEKTRON QURILMASI	189-192
Atajonova Saidakhon Boratalievna, Khasanova Makhinur Yuldashbayevna, INTEGRATION OF HYBRID SYSTEM ANALYSIS METHODS TO IMPROVE DECISION-MAKING EFFICIENCY	193-196
Зулунув Равшанбек Мамагович, ТЕХНОЛОГИИ ROBOTIC PROCESS AUTOMATION В МЕДИЦИНЕ	197-200
Aliyev Ibratjon Xatamovich, Bilolov Inomjon Uktamovich, CREATING A MODEL OF THE FALL OF SOLAR ENERGY IN CERTAIN COORDINATES	201-204
Akbarov Xatam Ulmasaliyevich, Ergashev Dilshodbek Mamasidiqovich, RDB TOKARLIK DASTGOHIDA ISHLOV BERISH JARAYONINING MATEMATIK MODELINI YARATISH	205-209
Абдуллаев Темурбек Маруфжонович, Козлов Александр Павлович, Разработка интеллектуальной системы управления освещением на основе IoT - технологий	210-219
O'rinboevyev Johongir Kalbay o'g'li, Nugmanova Mavluda Avaz qizi, KLASSTERLASH USULLARI YORDAMIDA NUTQNI AVTOMATIK SEGMENTATSIYALASH	220-225
Dalibekov Lochinbek Rustambekovich, 5G TARMOQLARIDA MASSIVE MIMO TEXNOLOGIYASINI JORIY ETISHNING TAHLILI	226-232
Bozarov Baxromjon Ilxomovich, Fure almashtirishlarini taqribiy hisoblash uchun optimal kvadratur formulalar	233-235
Xusanova Moxira Qurbonaliyevna, TARMOQ QURILMALARIDA DEMILITARIZATSIYALANGAN ZONA (DMZ) NI SOZLASH ORQALI XAVFSIZLIKNI TA'MINLASH	236-239
Ravshan Indiaminov, Sulton Khakberdiyev, INTERACTION BETWEEN MAGNETIC FIELDS AND THIN SHELLS	240-244
Muradov Muhammad Murod o'g'li, Mobil aloqa tayanch stansiyalarini qayta tiklanuvchan energiya ta'minot manbalaridan foydalangan holda energiya bilan ta'minlash xususiyatlari	245-250
Kabildjanov Aleksandr Sabitovich, Pulatov G'iyos Gofurjonovich, Pulatova Gulxayo Azamjon qizi, OB-HAVO SHAROITLARINING YURAK QON BOSIMI KASALLIKLARIGA TA'SIRINI MLP MODELIDA OPTIMALLASHTIRISH	251-255
Okhunov Dilshod Mamatjonovich, Okhunov Mamatjon Xamidovich, Azizov IskandarAbdusalim ugli, Ismoilzhonov Abdullokh Farrukhbk ugli, THE USE OF BIG DATA IN THE DIGITAL ECONOMY	256-260
Abduraimov Dostonbek Egamnazar o'g'li, ELASTIKLIK NAZARIYASI MASALASIGA LIBMAN TIPIDAGI ITERATSION USULNI QO'LLASHNING MATEMATIK MODELI	261-266
Мамадалиев Фозилжон Абдуллаевич, Новый подход составления математической модели для определения параметров торможения автомобиля в экстремальных условиях эксплуатации	267-269
Nasriddinov Otadavlat Usubjonovich, FIZIK MASALALARNI MATEMATIK PAKETLAR YORDAMIDA MODELLASHTIRISH	270-272
Jo'rayev Mansurbek Mirkomilovich, Ro'zaliyev Abdumalikjon Vahobjon o'g'li, AVTOMATLASHTIRILGAN MONITORING TIZIMI SIMSIZ SENSOR TARMOG'IDA MA'LUMOTLARNI UZATISH	273-278
Shamsiyeva Xabiba Gafurovna, VIDEO MA'LUMOTLARGA ISHLOV BERISH VA KOMPYUTERLI KO'RISH ALGORITMLARINING APPARAT DASTURIY MAJMUI	279-284
Atajonov Muhiddin Odiljonovich, AVTONOM FOTOELEKTRIK MODULNI MODELLASHTIRISH	285-288
J.M. Kurbanov, S.S.Sabirov, J.J.Kurbonov, NANOKATALIZATOR OLIISH TEXNOLOGIYASIDA "NAVBAHOR" BENTONITINI QURITISH VA KUYDIRISH JARAYONLARINING TERMOGRAVIMETRIK TAHLILI	289-293
Umarov Shukhratjon, Rakhmonov Ozodbek, ASSESSMENT OF THE LEVEL OF SECURITY AVAILABLE IN 4G AND 5G MOBILE COMMUNICATION NETWORKS	294-297
Soliyev Bahromjon Nabijonovich, Elektron tijorat savdolarini dasturiy yondashuvi tahlilida metodlar, matematik model va amaliy ko'rsatkichlar	298-302
Asrayev Muhammadmullo Abdullajon o'g'li, SINFLAR ORASIDAGI MASOFA, QAROR QABUL QILISH QOIDASI VA AJRATISH FUNKSIYASI	303-305

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Polvonov Baxtiyor Zaylobidinovich, Khudoyberdieva Muxayyoxon Zoirjon qizi, Abdubannabov Mo'ydinjon Iqboljon o'g'li, Ergasheva Gulruksor Qobiljon qizi, Tohirjonova Zahro Shovkatjon qizi, Mamasodiqov Shohjahon, CHARACTERIZATION OF PHOTOLUMINESCENCE SPECTRUM OF CHALCOGENIDE CADMIUM-BASED SEMICONDUCTOR POLYCRYSTALLINE FILMS	306-315
Sharibayev Nosirjon Yusupjanovich, Musayev Xurshid Sharifjonovich, TRIKOTAJ TO'QIMALARINI REAL VAQT REJIMIDA ANIQLANGAN NUQSONLARNI TAHLIL QILISH	316-320
Эргашев Отабек Мирзапулатович, Асомиддинов Бекзод, СОЗДАНИЕ ПРОГРАММНЫХ МОДУЛЕЙ ДЛЯ РЕШЕНИЯ ФУНКЦИОНАЛЬНЫХ ЗАДАЧ ИНФОРМАЦИОННЫХ СИСТЕМ	321-326
Djurayev Sherzod Sobirjonovich, Ermatova Zarina Qaxramonovna, YANGI KONSTRUKSIYADAGI MULTISIKLON QURILMASINING ENERGIYA SAMARADORLIGINI TAHLIL QILISH	327-331
J.M. Kurbanov, S.S.Sabirov, J.J.Kurbonov, "NAVBAHOR" BENTONITINING MODIFIKATSIYALANGAN NAMUNASINI O'YUCH EMMda QIZDIRISH HARORATIGA QARAB TEKSTURA XUSUSIYATLARINING O'ZGARISHI	332-337
Sharibayev Nosirjon Yusubjanovich, Kayumov Ahror Muminjonovich, SINOV YORDAMIDA TRIKOTAJ MAXSULOTLARINI SHAKL SAQLASH VA DEFORMATSIYALANISH JARAYONLARINI MONITORINGI	338-343
Muminov Kamolkhon Ziyodjon o'g'li, Artificial Intelligence in Cybersecurity, Revolutionizing Threat Detection and Response Systems	344-347
Тажибаев Илхом Бахтиёрович, ОБРАБОТКА МНОГОКАНАЛЬНЫХ СИГНАЛОВ В РАДИОЧАСТОТНЫХ И ОПТИЧЕСКИХ СИСТЕМАХ	348-351
Karimov Sardor Ilhom ugli, Sotvoldiyeva Dildora Botirjon qizi, Karimova Barnokhon Ibrahimjon qizi, COMPARISON OF MULTISERVICE REMOTE SENSING DATA FOR VEGETATION INDEX ANALYSIS	352-354
Abdurasulova Dilnoza Botirali kizi, PNEUMATIC AND HYDRAULIC TECHNICAL TOOLS OF AUTOMATION	355-359
Абдукадиров Бахтиёр Абдувахитович, СПОСОБЫ НАСТРОЙКИ ВЕСОВ ДЛЯ СНИЖЕНИЯ ПОТЕРЬ ПРИ ОБУЧЕНИИ ДАННЫХ В НЕЙРОННЫХ СЕТЯХ	360-365
Turakulov Otabek Xolmirzayevich, Mamaraufov Odil Abdixamitovich, IJTIMOYI TARMOQLARDA ELEKTRON MATNLI MA'LUMOTLARNI TASNIFLASHNING NEYRON-NORAVSHAN ALGORITMI	366-370
Asrayev Muhammadmullo Abdullajon og'li, Muxtoriddinov Muhammadyusuf Temirxon o'g'li, REGIONS APPLICATIONS SYSTEMS RECOGNITION	371-373
Raximov Baxtiyor Nematovich, Yo'ldosheva Dilfuza Shokir qizi, Majmuaviy markazlashtirilgan tizimlarning arxitekturasi va funksiyalari	374-378
Нурилло Мамадалиев Азизиллоевич, Моделирование конфликтных ситуаций телевизионных изображений в процессе обработки видеoinформации	379-381
A.A. Otaxonov, ОБНАРУЖЕНИЕ И ОЦЕНКА ФИШИНГОВЫХ URL-АДРЕСОВ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ	382-390
Akbarov Xatam Ulmasaliyevich, Ergashev Dilshodbek Mamasidiqovich, X12M MARKALI PO'LAT UCHUN TERMOSIKLLI ISHLOV BERISHNI AMALGA OSHIRISH PARAMETRLARI	391-396
Abdukodirov Abduvaxit Gapirovich, Abdukadirov Baxtiyor Abduvaxitovich, YUZ TASVIRLARINI GEOMETRIK NORMALLASHTIRISH ALGORITMINI ISHLAB CHIQISH	397-401
D.B.Abdurasulova, T.U.Abduhafizov, RAQAMLI IQTISODIYOTNING O'SISHI VA UNING TADBIRKORLIK FAOLIYATIGA TA'SIRI	402-405
Ibragimov Navro'zbek Kimsanbayevich, Hududiy oliy ta'lim muassasalarida raqobat ustunligini ta'minlashning diagnostik tahlil qilish uchun dasturiy ta'minot	406-413
Melikuziyev Azimjon Latifjon ugli, USING COMPUTER-SIMULATOR PROGRAMS IN TEACHING PARALINGUISTIC UNITS	414-417
Soliyev B.N., Ismoilova M.R., ELEKTRON TIJORATDA QAYTARILISHLARNI OPTIMALLASHTIRISH VA ULARNING NATIJALARI	418-421
Ergashev Otabek Mirzapulatovich, FUZZY RULE BASE DESIGN FOR NUMERICAL DATA ANALYSIS	422-428
Abdukadirova Gulbahor Xomidjon qizi, Abduqodirova Mohizoda Ilxomidin qizi, YUZ TASVIRLARIGA DASTLABKI ISHLOV BERISHDA NEYRON TARMOQ ALGORITMLARINI QO'LLASH SAMARADORLIGI	429-436
Садикова Мунира Алишеровна, ТРАНСФОРМАЦИЯ УПРАВЛЕНИЯ В ЦИФРОВУЮ ЭПОХУ	437-444
Pulaton Sherzod Utkurovich, Djumaniyazov Otabek Baxtiyarovich, THE ROLE OF IoT TECHNOLOGIES IN MONITORING THE ENVIRONMENTAL IMPACT OF INDUSTRIAL ENTERPRISES IN THE KHOREZM REGION	445-448
Mukhammadyunus Norinov, RESEARCH ON INCREASING THE BRIGHTNESS OF TELEVISION IMAGES	449-455
Arabboyev Alisher Avazbek o'g'li, DIFFIE-HELLMAN ALGORITMI VA XAVFSIZ KALIT ALMASHISH PROTOKOLLARI	456-458
Raximov Baxtiyor Nematovich, G'oiyova Xumora Qobiljon qizi, Ovoz tovushlari intellektual taxlili asosida videokuzatuz tizimini boshqarish	459-462

DIFFIE-HELLMAN ALGORITMI VA XAVFSIZ KALIT ALMASHISH PROTOKOLLARI

Arabboyev Alisher Avazbek o'g'li,

TATU Farg'ona filiali
"Axborot xavfsizligi" kafedrası 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 haqiqiylikini 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 algoritmidan 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 xabarlarini 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.

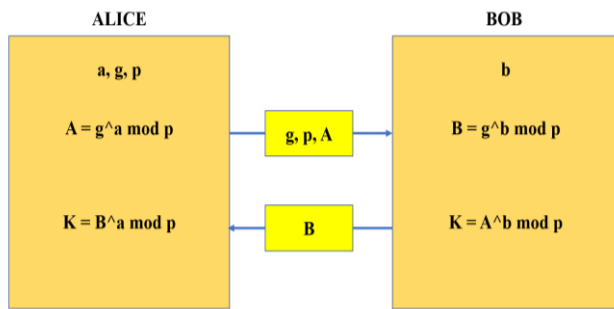
Ko'pgina kalit almashish protokollari bir juft kalitdan foydalanadi bular: ochiq kalit va egasi tomonidan maxfiy saqlanadigan yopiq kalit. Ushbu kalitlarning xavfsizligi protokol uchun asos hisoblanadi.

Ushbu protokollar kalit almashinuvi 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:

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

bunga qo'shimcha ravishda g ning har bir darajasi $g^1, g^2, g^3, g^4, g^5, \dots, g^{(p-1)}$ 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 $g^a \bmod p$ ni hisoblab, Bobga yuboradi;
- Bob $(g^a)^b \bmod p = g^{ab} \bmod p$ hisoblaydi va natijani Carolga yuboradi;
- Carol $(g^{ab})^c \bmod p = g^{abc} \bmod p$ hisoblab, umumiy maxfiy kalitni oladi;
- Bob $g^b \bmod p$ ni hisoblab, Carolga yuboradi;
- Carol $(g^b)^c \bmod p = g^{bc} \bmod p$ hisoblaydi va natijani Alicega yuboradi;
- Alice $(g^{bc})^a \bmod p = g^{bca} \bmod p$ ni hisoblab, umumiy maxfiy kalitni oladi;
- Carol $g^c \bmod p$ ni hisoblab, Alicega yuboradi;
- Alice $(g^c)^a \bmod p = g^{ca} \bmod p$ hisoblaydi va natijani Bobga yuboradi;
- Bob $(g^{ca})^b \bmod p = g^{cab} \bmod p$ ni hisoblab, umumiy maxfiy kalitga ega bo'ladi.

Natijada Alice, Bob va Carol $g^{abc} \bmod p = g^{bca} \bmod p = g^{cab} \bmod p$ 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. Diffie-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	$A \rightarrow B \rightarrow C$	$A^b \bmod p = (g^a \bmod p)^b \bmod p$ $23^4 \bmod 29 = 20$	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 : $(BC)^a \bmod p = (g^{bc} \bmod p)^a \bmod p$ $23^{12} \bmod 29 = 25$	$B \rightarrow C \rightarrow A$	$B^c \bmod p = (g^b \bmod p)^c \bmod p$ $25^{17} \bmod 29 = 23$
5	$C^a \bmod p = (g^c \bmod p)^a \bmod p$ $3^{12} \bmod 29 = 16$	Umumiy kalit K_b : $(CA)^b \bmod p = (g^{ca} \bmod p)^b \bmod p$ $16^4 \bmod 29 = 25$	$B \leftarrow A \leftarrow C$

$K_a = K_b = K_c = 25$ 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, algoritmlarni 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

