



MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
NUKUS FILIALI



«XALQ XO'JALIGI SOHASIDA ILG'OR TEXNOLOGIYALAR TADBIQI MUAMMOLARI»

MAVZUSIDAGI HUDUDIIY ILMIIY-TEXNIK KONFERENSIYASI

MA'RUZALAR TO'PLAMI



Chorvachilikda ilg'or texnologiyalar
va innovatsion yechimlar



Dasturlash, kiber xavfsizlik va qishloq
xo'jaligi fan sohalari integratsiyasi



Ta'lim va ishlab chiqarishda innovatsiyalar,
tahlil va prognozlash vositalari



27-dekabr 2023 yil

Konferensiya IL-392103072-
"Chorvachilik komplekslarini
elektron boshqarishning mobil
ilovasini yaratish" innovatsion
loyiha doirasida olib borilgan
ilmiy-amaliy tadqiqotlar
natijalariga bagishlangan



Nukus sh. A.Dosnazarov k. 74 uy



(61) 222-49-10



www.uzplf.uz



www.tatunf.uz

<i>B.Y.Geldibayev</i> Chorva komplekslarida sut mahsuldorligi haqidagi tahliliy hisobatlarni shakllantirishda kdd tahlil jarayonidan foydalanish	87
<i>G.G'.Artikova, M.Sh.Qazaqov</i> Xorazm viloyatida online chorva bozori qurish uchun mo'ljallangan mobil ilova tahlili.	91
<i>J.I.Dauletnazarov</i> Aqlli dehqonchilikda foydalaniladigan texnologiyalar	94
<i>B.Y.Geldibayev</i> IoT qurilmalaridan ma'lumotlarni olish jarayoni tashkil etishda «Edge Computing»dan foydalanishning afzalliklari	98
<i>J.I.Dauletnazarov</i> IoTning qishloq xo'jaligida qo'llanilishi	100
<i>A.A.Temirov</i> IoT asosidagi aqlli qishloq xo'jaligi uchun energiya tejamkor Edge-Fog-Cloud arxitekturasi	105
<i>D.A.Ernazarov</i> Qoramollarda oqsoqliklarni va tuyoq kasalliklarini erta aniqlash	109
<i>Э.С.Бабаджанов, Н.И.Калимбетов</i> Қорамол касалликларини С4.5 алгоритми орқали таснифлаш	113
II SHO'BA. DASTURLASH, KIBER XAVFSIZLIK VA QISHLOQ XO'JALIGI FAN SOHALAR INTEGRATSIYASI	117
<i>A.X.Nishanov, B.C.Samandarov</i> Real vaqt rejimida dinamik ma'lumotlar oqimini samarali boshqarish masalasi	117
<i>A.X.Nishanov, X.B.Kenjaev</i> Matnlarni kalit so'zlar asosida umumlashtiruvchi tizimni yaratish vazifalari	121
<i>N.U.Uteuliev, G.M.Djaykov, D.Sh.Yuldoshev</i> Numerical method for solving the problem of integral geometry on a family of semicircles	123
<i>X.N.Zaynidinov, X.Sh.Quzibayev</i> Sun'iy neyron tarmoq yordamida quyi amudaryo hududidagi suv sifatini bashoratlash	127
<i>B.B.Akbaraliyev, R.X.Xoliqnazarov</i> Tashkilotlarga ichki elektron hujjat aylanuv tizimini joriy etish	131
<i>Sh.R.G'ulomov</i> Uzfirwall-Next Generation Firewall apparat-dasturiy vositasining funksional strukturasi	136
<i>T.T.Berdimbetov, S.K.Nietullayeva, G.Q.Baytileuova, D.O.Madetov, M.J.Eshbayev</i> GIS ilovalarining rivojlanish tendensiyalari	140
<i>T.T.Berdimbetov, S.K.Nietullayeva, G.Q.Baytileuova, D.O.Madetov, M.J.Eshbayev</i> GISta fazoviy mal'umotlar tahlili	143
<i>F.K.Achilova</i> "Hand Tools" mobil ilovasini ishlab chiqish va tadbiq etishning afzalliklari	146
<i>M.E.Shukurova</i> Neft qatlamlari g'ovak muhitida filtratsiya jarayoni chegaraviy masalalarini yechishni avtomatlashtirish	150
<i>D.Kenjaboeva</i> Ta'lim berishda o'qituvchi deontologisi va kompetentligi	154
<i>A.M.Risnazarov</i> Kishi resursli kriptografiya	157
<i>S.X.Saparov, U.B.Allayarov, H.B.Qudratov</i> Bosh miya saratoni kasalligini erta tasniflashda informativ belgilar majmuasini tanlash algoritmi	159
<i>S.X.Saparov, U.B.Allayarov, H.B.Qudratov</i> Bosh miya saratonini erta tasniflashda obyektlar muhimligini aniqlash algoritmi	164

qarash qobiliyatini, shuningdek o'z vazifasini topa olish qobiliyatini nazarda tutadi. Yuqorida qayd etilgan deontologiya, kompetensiya va kompetentlikka oid nazariy fikrlardan bugungi kun o'qituvchisi shaxsiga nisbatan qo'yiladigan talablar mazmunini anglatadi.

Foydalanilgan adabiyotlar

1. Dilafroz Kenjabayeva. Innovative technology of deontological competence formation in future foreign language teachers. Yeuropen Scholar Journal (YeSJ). Spain. Vol. 3 No.10, October 2022. PP.-19-22.
2. Kenjaboyeva D.A. Innovatsion yondashuv asosida xorijiy til o'qituvchilarida deontologik kompetentlikni rivojlantirish texnologiyasi. // Xalq ta'limi ilmiy-metodik jurnal. –Toshkent., -2022, -5-son, B.91-95. (13.00.00. №17).
3. Kenjaboev A.E. Pedagogik deontologiya va o'qituvchining kasbiy kompetentligi. Zamonaviy ta'lim jurnali 2021 yil №4. 10-bet
4. Arapov G. N. Interpretation of the light industry lexicon in modern linguistics //ISJ Theoretical & Applied Science. – 2023. – T. 7. – №. 123. – C. 2023.
5. Namozovich A. G. Expression of Ethnocultural Realia in the Lexicon of Light Industry in English, Uzbek and Russian //Web of Semantic: Universal Journal on Innovative Education. – 2023. – T. 2. – №. 3. – C. 102-105

KISHI RESURSLI KRIPTOGRAFIYA

A.M.Risnazarov (TITU Nókis filiali)

Informatsiyaliq texnologiyalar hár-bir insannín kúndelikli jumislarina kirip barip, búgingi kúnde oní hár-qiyli gadjetlersiz kóz aldımızga keltire almaymiz. Kóplegen úylerde Internetke jalangan (óz ara simsiz tarmaq arqali jalangan), o'natilgan operacion sistemağa iye qurilmalar paydalanilmaqta. Adamalar barliq orinlarda hár-qiyli terminallar, esaplagishlar, datchikler h.t.b. menen islesiwine tuwri kelmekte.

Intellektual texnologiyalardín bunday tarqalwı maqlıwmatlar qawipsizligi mashqalasın júzege keltirmekte. Biraq kriptografiyalıq qurallardı barliq qurilmalarda birdey qollanıw imkaniyatı joq. Ápiwayı kriptografiyalıq algoritmlerdi júdá sheklengen resurslı qurilmalarda qollanıw imkaniyatı joq. Bunday qurilmalarga misal etip tómendegilerdi keltirse boladı:

RFID-esaplagishlar (Radio Frequency Identification);

Smart-kartalar;

Simsiz sensorlar;

Indikatorlar, datchikler, kontrollerlar;

Internet zatlar hám basqalar.

Júdá kishi resurslı qurılmalarda paydalanıw ushın kriptografiyalıq algoritm jaratıw principleri hám jantasıwları ádettegi algoritmlerdi jaratıw kriteriyalarınan parıq qıladı. Bul ózine tán taraw kriptografiyanıń «Kishi resurslı kriptorafiya» (Lightweight cryptography) dep atalıwshı tarawı esaplanadı.

Biz tómende jeńil bloklı shifrlardı qarastırıp, olardıń jaratıwda qollanılğan jantasıwlar hám algoritmleri ózgesheliklerin analizlep shıǵamız.

DESL hám DESXL. DESL (DES Lightweight) hám DESXL (DES-Xor Lightweight) shifrları RFID-esaplaǵıshlarında qollanıw ushın jaratılğan bolsada, óziniń ápiwayılıǵı sebepli temperatura datchikleri, geolokaciyalıq qurılmalar qosımshalarında keń qollanıwmaqta.

DESL 64 bit ólshemli bloklardan ibarat DES (Data Encryption Standard) algoritmine tiykarlanǵan. DES algoritmi ózine n bit qabıllap anıq algoritm tiykarında túrlendirip m bit shıǵarıp beriwshi segiz blok tiykarında qurılǵan. DESL algoritminde tekte bir S-blok isletilip, jalǵız S-blok jaratıw kriteriyaları onıń keń tarqalǵan kriptohújimlerde shıdamlılıǵın támiynleydi.

DESXL – bul DESX (DES- Xor) algoritminiń jeńillestirilgen forması bolıp, bunda da bir S-blok isletiledi. Bunda ózgeshelik sonnan ibarat, kiriwshi hám shıǵıwshı maǵlıwmatlar «ishki giltler» paydalanıp, tiykarında XOR operaciyası menen túrlendiredi.

DESL hám DESXL algoritmleriniń artıqmashılıǵı turaqlı saqlawshı qurılmada tablıcalardı saqlaw ushın talaptı 8 ese kemeytiliwi bolıp, passiv RFID-esaplaǵısh uqsalǵan sheklengen resurslı qurılmalarda paydalanıwǵa boladı.

KATAN. Bul KATAN32, KATAN48 hám KATAN64 bloklı shifrlar semyası. Algoritmnerdiń atındaǵı sanlar algoritm blokınıń bitlerdegi ólshemi. Barlıq algoritmler 80 bitli giltten paydalanadı.

Bundaǵı eń kishi KATAN32 algoritmi 462GE (GE-Gate Equivalent, cıfrlı elektron sxemalardıń quramalıǵın anıqlawshı ólshem birlik) kórsetkishli qurılmalarda qollanǵanda 12,5 Kbit/s (100 kGc) tezlikte isley aladı. KATAN48 versiyası 588GE qurılmalarǵa arnalıp, RFID-metkalar ushın usınıladı. KATAN64 bular arasında eń úlken hám eń iykemli shifr bolıp, 1054GE kórsetkishli qurılmalar ushın 25,1 Kbit/s (100kGc) ótkiziw imkaniyatına iye. Bul shifr geolokaciya datchikleri hám meteodatchik uqsalǵan low-end qurılmalardı keń qollanıwmaqta.

KATAN shifrlaw algoritmi tómendegi faktorlar sebepli resurslarǵa talabı júdá kishkene:

- Apparat tárepten júdá jeńil qollanılatuǵın jıljıwshı registrardı paydalanıw;
- Kerekli sıızıqlı emeslikti beriwshi ápiwayı kerı baylanıs funkciyası;
- 32 den 64 bitke shekem bolǵan úlken bolmaǵan maǵlıwmatlar blogin qayta islew;

- Ishki halattin olshemini ulken bolmawı, onin olshemi blok olshemi menen teń bolıwı.

Biz joqarıda kishi resurslı shifrlawğa mısallar kórip, jánede olardin islew tiykarların qarastırıp, kishi resurslı shifrlaw algoritmlerinin qollanıw tarawlarına toqtalıp óttik.

Paydalanılğan ádebiyatlar

1. G. Leander, C. Paar, A. Poschmann, and K. Schramm. New Lightweight DES Variants. Springer, 2007.
2. C. De Cannière, O. Dunkelman, M. Knežević. KATAN & KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers. Springer, 2009

BOSH MIYA SARATONI KASALLIGINI ERTA TASNIFLASHDA INFORMATIV BELGILAR MAJMUASINI TANLASH ALGORITMI

S.X.Saparov (TATU doktoranti),

U.B.Allayarov (Toshkent tibbiyot Akademiyasi Termez filiali),

H.B.Qudratov (RIO va RIATM Surxondaryo filiali)

Kalit soʻzlar: tasniflash, informativ belgilar, dastlabgi ishlav berish, oʻquv tanlama.

Maʼruzada maʼlumotlarni intellektual tahlil qilish masalalarida belgilar fazosi oʻlchamini kamaytirish, yaʼni informativ belgilar majmuasiini tanlash masalasini yechish Bosh miya saratoni kasallikligiga tadqiq etilgan. Bunda 4 ta sinf (X_1 – Bosh miya oʻng peshona sohasi anaplatik astrositomasi; X_2 – Bosh miya xiazma selillyar–sohasi adenomasi; X_3 – Bosh miya oʻng peshona sohasi gleoblastomasi; X_4 – Bosh miya oʻng peshona sohasi meningiomasi) va 19 ta belgilardan iborat oʻquv tanlamadan foydalanilgan holda informativ belgilar majmuasini tanlash masalasini yechish asnosida 19 ta belgilardan 4 ta sinflarni har birini kamida 65% ga ajratib beradigan 6 ta belgilar majmuasi tanlangan.

Maʼlumotlarni intellektual tahlil qilish masalalaridan biri tadqiqot obyektlarini optimal tavsiflovchi informativ belgilar majmuasi tanlash, yaʼni belgilar fazosi oʻlchovini kamaytirish deb atalib, bu yoʻnalishda juda koʻplab ilmiy tadqiqotlar olib borilmoqda [1, 2, 3, 4, 5].

Mazkur maʼruzada oʻquv tanlamadagi obyektlarni xarakterlovchi N oʻlchovli belgilar fazosidan $\ell \ll N$ boʻlgan ℓ oʻlchovli belgilar fazosiga oʻtish masalasini yechish Bosh miya saratoni kasallikligiga tadqiq etilgan.

Faraz qilaylik, boshlangʻich maʼlumotlar asosida shakllantirilgan oʻquv tanlanma sinflarga ajratilgan va ular quyidagicha berilgan boʻlsin: