



MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
NUKUS FILIALI



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

MAVZUSIDAGI HUDUDIY ILMIY-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

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

Informaciyalıq texnologiyalar hár-bir insanniń kúndelikli jumıslarına kirip barıp, búgingi kúnde oni hár-qıylı gadgetlersiz kóz aldımızǵa keltire almaymız. Kóplegen úylerde Internetke jalǵanǵan (óz ara sımsız tarmaq arqalı jalǵanǵan), ornatılǵan operacion sistemaǵa iye qurilmalar paydalanylmaqta. Adamalar barlıq orınlarda hár-qıylı terminallar, esaplaǵıshlar, datchikler h.t.b. menen islesiwine tuwrı kelmekte.

Intellektual texnologiyalardıń bunday tarqalıwı maǵlıwmatlar qáwipsizligi mashqalasın júzege keltirmekte. Biraq kriptografiyalıq quralları barlıq qurilmalarda birdey qollanıw imkaniyatı joq. Ápiwayı kriptografiyalıq algoritmlerdi júdá sheklengen resurslı qurilmalarda qollanıw imkaniyatı joq. Bunday qurilmalarǵa misal etip tómendegilerdi keltirse boladı:

RFID-esaplaǵıshlar (Radio Frequency Identification);

Smart-kartalar;

Sımsız sensorlar;

Indikatorlar, datchikler, kontrollerlar;

Internet zatlar hám basqalar.

Júdá kishi resurslı qurılmalarda paydalaniw ushın kriptografiyalıq algoritm jaratiw principleri hám jantasiwları ádettegi algoritmlerdi jaratiw kriteriyalarınan pariq qıladı. Bul ózine tán taraw kriptografiyanı «Kishi resurslı kriptorafiya» (Lightweight cryptography) dep atalıwshı tarawı esaplanadı.

Biz tómende jeńil bloklı shifrlardı qarastırıp, olardıń jaratiwda qollanılǵan jantasiwlар hám algoritmleri ózgesheliklerin analizlep shıǵamız.

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

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 jaratiw kriteriyaları onıń keń tarqalǵan kriptohújimlerge shıdamlılıǵın támiynleydi.

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

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

KATAN. Bul KATAN32, KATAN48 hám KATAN64 bloklı shifrlar semyası. Algoritmlerdiń atındıǵı sanlar algoritm blokinıń bitlerdegi ólshemi. Barlıq algoritmler 80 bitli giltten paydalanadı.

Bundaǵı eń kishi KATAN32 algoritmi 462GE (GE-Gate Equivalent, cifrlı elektron sxemalardıń quramalıǵın anıqlawshı ólshem birlik) kórsetkishli qurılmalarda qollanganda 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 uqságan low-end qurılmalardı keń qollanılmaqta.

KATAN shifrlaw algoritmi tómendegi faktorlar sebepli resurslarǵa talabı júdá kishkene:

- Apparat tärepten júdá jeńil qollanılatuǵın jılıjıwshı registrlardı paydalaniw;
- Kerekli sızıqlı emeslikti beriwshi ápiwayı keri baylanıs funkciyası;
- 32 den 64 bitke shekem bolǵan úlken bolmaǵan maǵlıwmatlar blogin qayta islew;

- Ishki halattıń ólsheminiń úlken bolmawı, onıń ólshemi blok ólshemi menen teń bolıwı.

Biz joqarıda kishi resurslı shifrlawǵa mısallar kórip, jánede olardıń islew tiykarların qarastırıp, kishi resurslı shifrlaw algoritmleriniń qollanıw tarawlarına toqtalıp óttik.

Paydalanylǵan 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 TASNIFFLASHDA 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 so‘zlar: tasniflash,informativ belgilar,dastlabgi ishlav berish , o‘quv tanlama.

Ma’ruzada ma’lumotlarni intellektual tahlil qılısh masalalarida belgilar fazosi o‘lchamini kamaytirish, ya’ni informativ belgilar majmuasiini tanlash masalasini yechish Bosh miya saratoni kasallılıgiga tadqiq etilgan. Bunda 4 ta sinf (X_1 –Bosh miya o‘ng peshona sohasi anaplatik astrositomasi; X_2 –Bosh miya xiazma selillyar-sohasi adenomasi; X_3 –Bosh miya o‘ng peshona sohasi gleoblastomasi; X_4 –Bosh miya o‘ng peshona sohasi meningiomasi) va 19 ta belgilardan iborat o‘quv 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.

Ma’lumotlarni intellektual tahlil qılısh masalalaridan biri tadqiqot obyektlarini optimal tavsiflovchi informativ belgilar majmuasi tanlash, ya’ni belgilar fazosi o‘lchovini kamaytirish deb atalib, bu yo‘nalishda juda ko‘plab ilmiy tadqiqotlar olib borilmoqda[1, 2, 3, 4, 5].

Mazkur ma’ruzada o‘quv tanlamadagi obyektlarni xarakterlovchi N o‘lchovli belgilar fazosidan $\ell \ll N$ bo‘lgan ℓ o‘lchovli belgilar fazosiga o‘tish masalasini yechish Bosh miya saratoni kasallılıgiga tadqiq etilgan.

Faraz qilaylik, boshlang‘ich ma’lumotlar asosida shakllantirilgan o‘quv tanlanma sinflarga ajratilgan va ular quyidagicha berilgan bo‘lsin: