



QR-kod
maqolaning DOI
sahifasini
ochadi

Arzieva Jamila Tileubaevna, Yuldasheva
Ravshanoy Allambergenovna. Ashiq
giltli kriptografiyalıq algoritmler hám
elektron sanlı qol // «O'zbekiston
olima ayollarining mamlakat
taraqqiyotiga qo'shayotgan hissasi»
mavzusidagi xalqaro ilmiy-amaliy
konferensiya materiallari (Nukus, 2026-
yil 9–10-oktyabr). – Nukus, 2026. –
B. 330–334. – DOI: <https://doi.org/10.66073/ReFocus-Conf/0910062>

ASHÍQ GILTİ KRIPTOGRAFIYALÍQ ALGORITMLER HÁM ELEKTRON SANLÍ QOL

Arzieva Jamila Tileubaevna

t.i.f.d.

Yuldasheva Ravshanoy Allambergenovna

Berdaq atındağı Qaraqalpaq mámleketlik universiteti

e-mail: a_jamila@karsu.uz

Annotaciya: Kriptografiyada keń qollanılıwshı shifrlaw usıllarınan biri *ashıq giltli* dep (yamasa eki giltli dep te ataladı) atalıwshı usıllardan qollanıw maǵlıwmattı shifrlaw hám rasshifrovkalaw. Ashıq giltli shifrlaw algoritmi járdeminde payda bolǵan eki tárep ortasındaǵı baylanıs kanalınıń ulıwma kórinisin jaratıw. Ashıq giltli kriptografiyalıq algoritmlerdi elektron sanlı qolda qollanıw.

Gilt sózler: Kriptografiya, Ashıq gilt, shifrlaw algoritmleri, rasshifrovkalaw algoritmleri, hújim, kriptosistemalar.

Kriptografiyada keń qollanılıwshı shifrlaw usıllarınan jáne biri *ashıq giltli* dep (yamasa eki giltli dep te ataladı) atalıp, maǵlıwmattı shifrlawda hám rasshifrovkalawda túrli gıltlerden paydalanadı.

Meyli, gilt maydanında Shifrlaw funkciyası hám ǵa sáykes rasshifrovkalaw funkciyası bolsın. Sonıń menen birge, barlıq shifrlaw/rasshifrovkalaw funkciyaları jubı () ushın berilgen shifrtexst ushın funkciya járdeminde ashıq tekst ni (shártti qánaatlandırıwshı) esaplawdıń múmkinshiligi bar bolmasın. Bul ózgeshelik, berilgen shifrlaw gılti den paydalanıp, rasshifrovkalaw gılti nı tabıwdıń imkansız ekenligin ko'rsetedi. Bunda, – qapqanlı bir tárepleme funkciya esaplanıp, onıń kerisin tabıw ushın tek parametri talap etiledi. Sol sebepli, ashıq giltli shifrlaw algoritmleri shifrlaw hám rasshifrovkalaw gıltleri birdey bolǵan, simmetrik shifrtexstlerden o'zgeshe boladı.

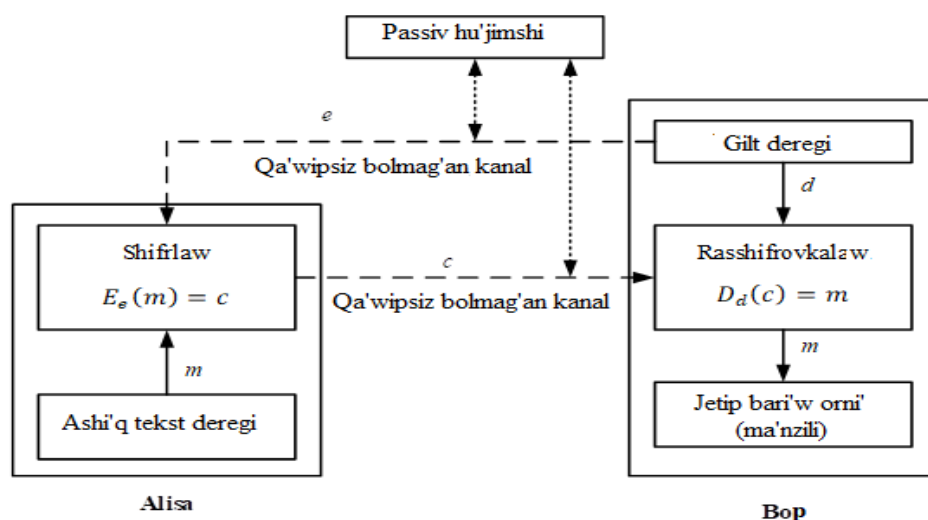
Ashıq giltli shifrlaw algoritmi járdeminde payda bolǵan eki tárep ortasındaǵı baylanıs kanalınıń ulıwma kórinisi 1-súwrette keltirilgen. Buǵan bola Bop gilt jubın tańlaydı. Shifrlaw gılti (*ashıq gilt* dep ataladı) ni Alisaǵa ashıq tarmaq arqalı jiberiledi hám rasshifrovkalaw gılti (*jeke gilt* dep ataladı) nı ózinde jasırın saqlaydı. Sonnan keyin, Alisa ashıq tekst nı Boptıń ashıq gılti járdeminde shifrlaydı: hám onı ashıq tarmaq arqalı jiberedi. Bop bolsa qabıl etilgen shifrtexst nı gilt penen funkciya járdeminde rasshifrovkalaydı.



Olimo

«O'zbekiston olim ayollarining
mamlakat taraqqiyotiga
qo'shayotgan hissasi»

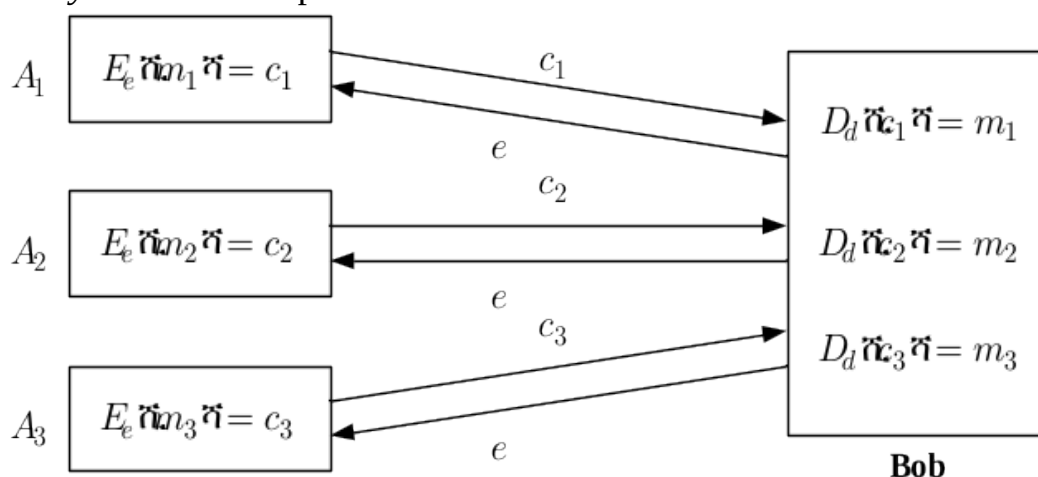
XALQARO ILMIY-AMALIY
KONFERENSIYA
NUKUS, 9–10-OKTYABR 2026



1-súwret. Ashiq giltli shifrlaw usulı járdeminde shifrlaw

Ashiq giltli shifrlaw algoritmleri járdeminde shifrlaw processı shifrlaw giltin ashıq uzatıwı menen simmetrik giltli shifrlardan parıqlanadı. Bunnan basqa, *ashıq giltli shifrlaw algoritmleri* járdeminde maǵlıwmat uzatıwda simmetrik kriptosistemalar sıyaqlı hár bir maǵlıwmattı uzatıwshı hám qabıl etiwshi arasında bólek – bólek giltten paydalanıwdı talap etpeydi. Boptıń ashıq gilti ni bilgen hár bir qatnasıwshı maǵlıwmattı shifrlap oǵan uzatıwı múmkin. Shifrlanǵan maǵlıwmattı rasshifrovkalaw bolsa tek ǵana giltti bilgen Bob ushın tiyisli boladı. Usı jaǵday 2-súwrette keltirilgen. Bul jerde, hám túrli tárepler bolıp, Boptıń birden bir gilti bolıp menen, hám maǵlıwmatlardı shifrlaw múmkin boladı. Payda bolǵan barlıq shifrtexstlerdi bolsa Bob birden-bir jeke gilt menen rasshifrovkalaw múmkin boladı.

Ashiq giltli shifrlaw algoritmleri shifrlaw giltin uzatıw ushın qawipsiz kanaldı talap etpewi menen ajralıp tursa da, bunda tolıq qawipsizlikti támiyinlew ushın jetkilikli esaplanbaydı. 3-súwrette buzıwǵa qaratılǵan tárepinen ashıq giltli shifrlaw algoritmın buzbastan maǵlıwmattı qolǵa kirgiziw processı keltirilgen. Bunday jaǵday *abroysızlandırıw* dep ataladı.



2-súwret. Ashiq giltli shifrlawdan paydalanıw sxeması

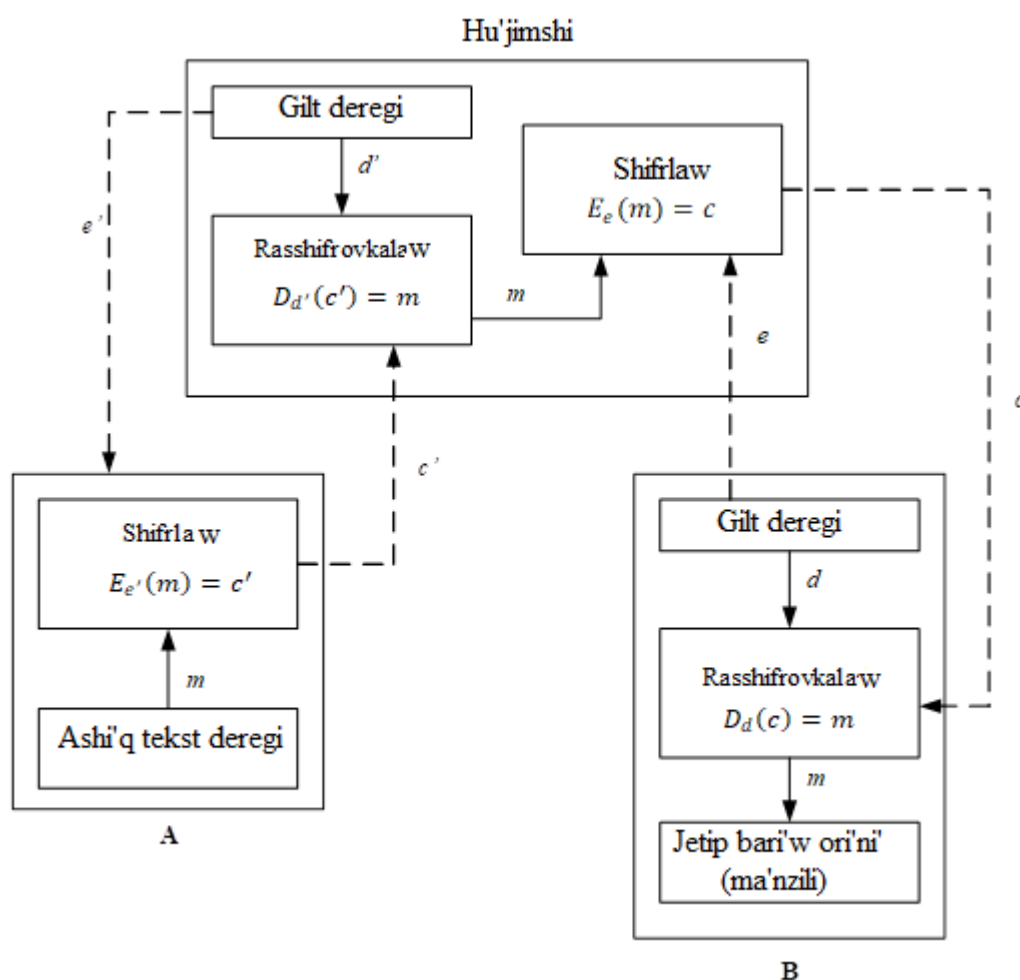
Joqarıdaǵı ssenariyde, abroysızlandırıw jaǵdayı hújimshi giltti táreptiń ashıq gilti dep tárepti isendiriw nátiyjesinde júzege kelmekte. Bunda, hújimshi dan tárepke uzatılǵan shifrtexstti o'ziniń jeke gilti menen rasshifrovkalaydı hámde táreptiń ashıq

gilti menen qayta shifrlap o'gan uzatadi. Bul ja'gdayda mashqala ta'rep ashıq gıltı ta'repke tiyisli ekenligin tekserı almaslıgı na'tıyjesinde ju'zege kelmekte.

Ámelde ashıq gıltli shifrlaw algoritmlerinen *elektron sanlı qol* dep atalıwshı sistemanı qurıw ushın paydalanıladı. *Elektron sanlı qol* algoritmleri ashıq gıltli kriptosistemalardıń bir túri esaplanadı. Meyli, ashıq tekst maydanı nen shifrtıktı maydanı ға sáwlelendiriwshı shifrlaw funkciyası hám bunda bolsın. Eger ge sáykes bolğan rasshifrovkalaw funkciyası bolsa, onda hám lar ushın orın almasırw múmkin:

ler ushın, .

Ashıq gıltli shifrlawdıń bul kórinisi *qaytarılatsuđın* dep ataladı. Bunda, tek ushın orınlı bolıwın esapqa alıw kerek. Basqa ja'gdaylarda bolsa (), sáwlelendiriw mániske iye bolmaydı.



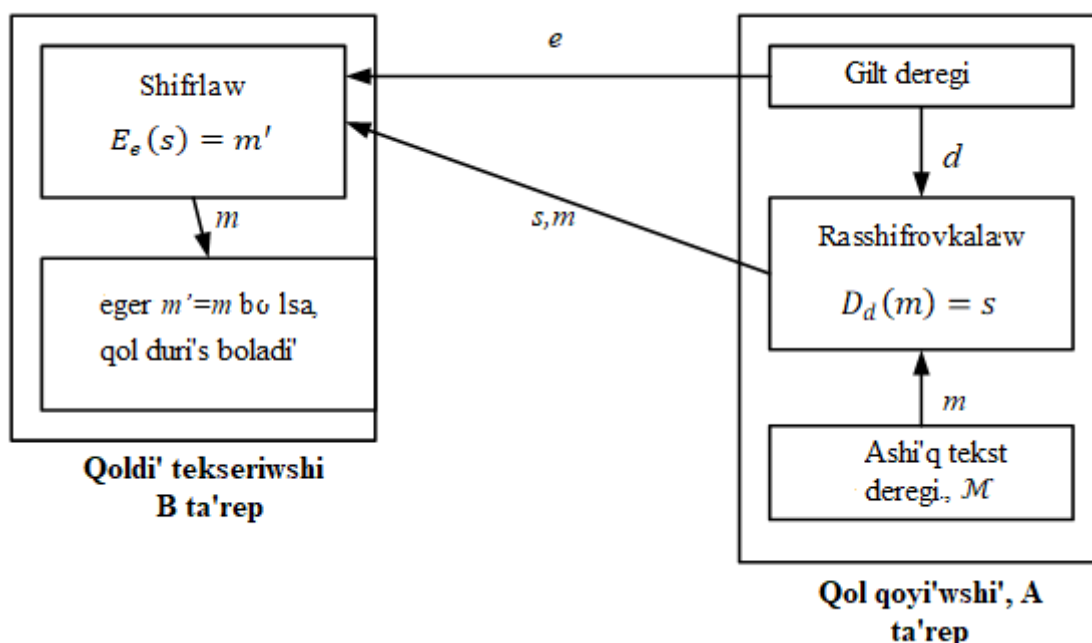
3-súwret. Eki ta'rep arasındagı baylanıstıń abıroysızlanıwı

Elektron sanlı qol sistemaların qurıw tómendegi tártıpte ámelge asırıladı (4-súwret):

1. Meyli qol qoyıw sxeması ushın ashıq tekst maydanı bolsın.
2. Meyli qol qoyıw maydanı ushın orınlı bolsın.
3. Meyli () – ashıq gıltli shifrlaw sxeması ushın gılt jubı bolsın.
4. Qol qoyıw funkciyası di ge teń dep alsaq, onda xabarlar ushın qol ge teń boladı.

5. Qoldı tekseriw funkciyası bolsa to'mendegige teń boladı:

$$V_A(m, s) = \begin{cases} true, & \text{Eger } E_e(s) = m \\ false, & \text{Qalg'an jag'daylarda.} \end{cases}$$



4-súwret. Elektron sanlı qoldıń ápiwayı sxeması

Simmetrik gıltli kriptosistemalar sıyaqlı ashıq gıltli shifrlaw arqalı maǵlıwmattıń konfidenciallıǵın támiyinlew ámelge asırıladı. Biraq, elektron sanlı qol sistemaları maǵlıwmattıń pútinligin hám biykar etiwden qorgalıwın támiyinlewdi maqset etedi.

Joqarıda kórip ótilgen simmetrik hám ashıq gıltli kriptosistemalar ayrıqsha bir qansha qolaylılıq hám kemshiliklerge iye. Olarǵa tómendegilerdi keltiriw múmkin (1-keste).

1-keste. Simmetrik hám ashıq gıltli kriptosistemalardıń qolaylılıq hám kemshilikleri

Qásiyetleri Kriptosistema	Qolaylılıqlar	Kemshilikler
Simmetrik kriptosistemalar	1. Simmetrik gıltli shifrlar maǵlıwmattı shifrlawda joqarı operativlik usınısın beredi. 2. Simmetrik kriptosistema gıltiniń uzınlıǵın salıstırǵanda qısqa.	1. Simmetrik kripto sistemadan paydalanıw ushın eki tárepte de birden-bir gılt bolıwı shárt. 2. Simmetrik gıltlerden paydalanıw dáwiri kem.
Ashıq gıltli kriptosistemalar	1. Tek jeke gıltti jasırın saqlaw talap etiledi. 2. Jeke hám ashıq gıltler jubınan jetkiliklishe uzaq waqt paydalanıw múmkin.	1. Ashıq gıltli shifrlar maǵlıwmatlardı shifrlawda tómén dárejede háreketlenedi. 2. Ashıq gıltli kripto sistemalarda gılt uzınlıǵı salıstırmalı úlken.

Paydalanılǵan ádebiyatlar

1. A.J.Menezes, P.C. hám Oorschot, S.A.Hám Stone. Handbook of Applied Cryptography. CRC Press, 2001, 816 p.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 -816 стр.
3. С.К.Ганиев, М.М.Каримов, З.Т.Худойкулов, М.М.Кадиров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках. –Т.: «Иқтисод-молия», - 2017, 480 с.
4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –Т.: «Fan hám texnologiya», 2016, 372 bet.
5. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O'quv qo'llanma. –Т.: «Aloqachi», 2008, 382 bet.
6. Stamp M. Information security: principles and practice // John Wiley & Sans, 2011, -P. – 606.
7. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari. O'quv qo'llanma. –Т.: «Iqtisod-moliya», - 2021, 228 bet.
8. D.Ya.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedohám, I.U.Xolimtoehám. Kriptografiyaning matematik asoslari. O'quv qo'llanma. –Т.: «Aloqachi», 2019, 192 bet.
9. New York: Dover, 1992. – 398 p.
10. Zienkiewicz O.C., Taylor R.L., Zhu J.Z. The Finite Element Method: Its Basis and Fundamentals. 7th ed. – Oxford: Butterworth-Heinemann, 2013. – 756 p.
11. Quarteroni A., Sacco R., Saleri F. Numerical Mathematics. 2nd ed. – Berlin: Springer, 2007. – 655 p.
12. Isroilov M.I. Hisoblash metodlari. 1-qism. – Toshkent: O'zbekiston, 2003. – 432 b.
13. Roos H.-G., Stynes M., Tobiska L. Robust Numerical Methods for Singularly Perturbed Differential Equations. 2nd ed. – Berlin: Springer, 2008. – 604 p.