qanday informaciyalar bolıw kerek? Dizimde bos qatar yamasa baǵana bolıwı mumkin be? Durıs juwaplar ushın toparlarǵa ball beriledi.

VII. Juwmaqlaw. Sabaqtı bahalaw.

Oqıwshılar kóp ball toplaw ushın háreket etedi. Oqıtıwshı toplanǵan ballardı esaplap shıǵadı. Jeńimpaz kishi topardı hám sabaq dawamında aktiv qatnasqan oqıwshılardı xoshametleydi.

Oqıtıwshı sabaqtı juwmaqlastıradı: oqıwshılar elektron tablicada jazılǵan sózlerden ózine tiyislisin jazıp aladı hám ózine tiyisli sózlerin yacheyka adresi menen belgileydi. Ol tómendegishe:

	A	B	C	D
1	Men bildim...	Qi'zi'qli' boldi'..	Qi'yi'n boldi...	Men tapsirmani' ori'nladi'm...
2	Men o'zlestirdim...	Men sezdim, onda...	Endi men isleyin...	Men tu'sindim, onda...
3	Men u'yrendim...	Mende islendi...	Men ta'wekelshimen...	Menin' qoli'mnan keledi...
4	Meni tan' qaldi'rdi'...	Mag'an kerekli...		

VIII. tapsırma.

Temanıń tiykarǵı tusiniklerin yadlaw, sabaqlıqtaǵı temaǵa tiyisli materiallar menen islew, pánler boyınsha ulgeriw elektron tablicasın jaratıw.

Ádebiyatlar

1. Boltayev B., Azamatov A., Asqarov A., Sodiqov M., Azamatova G. Informatika va hisoblash texnikasi asoslari. -T.: «Tafakkur». 2011.
2. Ro`zieva D., Usmonboeva M., Xoltqova Z. Interfaol metodlar: mohiyati va qo`llanilishi. Metodik qóllanma. Nizomiy nomidagi TDPU. -T.: 2013.
3. Qasımov M., JuginisovaJ., Il yasova Z. MS Excel dástúrinde funkciyalardıń grafiklerin jasaw metodikası. Metodikalıq qollanba. -N.: 2015.

REZYUME

Maqolada ma'lumotlarni tizimlashtirishning ilmiy metodik muammolari ko`rib chiqilgan. MS Excel dasturi yordamida ma'lumotlarni elektron jadval ko'rinishida saqlash usuli ko`rib chiqilgan. Amalda 8-sinfda o'qitiladigan mavzularga doir dasturlashtirish ko'rib chiqilgan. Unda saralash va tanlash usullari kiritilgan. Maqolada ma'lumotlarni tizimlashtirishning innovatsion texnologiyasi yaratilgan.

РЕЗЮМЕ

В статье излагаются вопросы научно-методического обеспечения систематизации информации. Описывается алгоритм сохранения информации в виде электронной таблицы на базе MS Excel. Полученные результаты используются в 8-классе, которые соответствуют теме сортировки и фильтрации информации. В работе разработаны инновационные технологии систематизации информации.

SUMMARY

The article deals with the issues of scientific-methodical supply of the information systematization. The author describes the algorithm of preservation of the information in the form of an electronic table on the basis of MS Excel. The received results are used in the 8-th form, they correspond to themes of sorting and information filtration. There have been worked out innovative technologies of systematization of the information.

ЗАМОНАВИЙ КРИПТОГРАФИК АЛГОРИТМЛАР УЧУН КАТТА ТУБ СОНЛАРНИ ГЕНЕРАЦИЯЛАШ МАСАЛАЛАРИ

Ш.Б.Норматов - *катта ўқитувчи*

ТАТУ Қарши филиали

Таянч сўзлар: ахборот хавфсизлиги, криптография, туб сонлар, шифрлаш алгоритмлари, сонларни тубликка текшириш.
Ключевые слова: информационная безопасность, криптография, простые числи, алгоритмы шифрование, проверка числа на простоту.
Key words: information security, cryptography, prime numbers, encryption algorithms, verification of the simplicity.

Кириш. Ахборот-коммуникацион технологияларининг кун сайин ривожланиб бориши ахборот хавфсизлиги муаммосининг долзарблилигини янада ошириб юбормоқда. Бу эса ахборот хавфсизлигини таъминлашга қаратилган турли хил янги усуллар ва воситаларни яратиб боришни тақозо этади. Маълумки, ахборот хавфсизлигини ишончли таъминлаш бу масалага комплекс ёндашувни талаб қилади. Яъни, ахборотларни ҳимоялашнинг ҳуқуқий, ташкилий ва мухандислик-техник таъминотларидан самарали фойдаланиш зарурлигини кўрсатади.

Жумладан, ахборотларни ҳимоялашда криптографик усулларнинг ҳам салмоқли ўрни бор. Бу соҳада ҳам мамлакатимизда қатор ислоҳотлар амалга оширилмоқда. Бунинг тасдиғи сифатида Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги «Ўзбекистон Республикасида ахборотни криптографик муҳофазасини ташкил қилиш чора-тадбирлар тўғрисида» ПҚ 614-сонли, Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги «Ахборотни криптографик муҳофаза қилиш воситаларини лойиҳалаштириш, ишлаб чиқиш, сотиш, таъмирлаш ва ишлатишни лицензиялаштириш тўғрисидаги низомни тасдиқлаш тўғрисида» ВМҚ 242-сонли қарорлари, маълумотларни шифрлаш, хэш функциялар бўйича давлат стандартларининг қабул қилинишида кўриш мумкин.

Мавжуд криптотизимларнинг барчаси бирор бир криптографик алгоритм асосида ишлайди. Ҳозирда кўпгина криптографик стандартларга асос сифатида олинаётган *RSA, El-Gamal* алгоритмлари асосида амалий жиҳатдан ечиш етарли даражада мушкул бўлган берилган сонни иккита туб кўпайтувчи шаклида ифодалаш ва чекли майдонда дискрет логарифмни ҳисоблаш масалалар ётади.

Юқорида келтирилган ҳар иккала алгоритмда ҳам маълумотларни шифрлашда, электрон рақамли имзони яратишда 1024 битли ва ундан ҳам катта туб сонлардан фойдаланилади. Шунинг учун ҳам катта туб сонлар билан ишлаш, уларни генерация қилиш криптографиянинг асосий масалаларидан бирига айланиб улгурган. Умуман криптографияда туб сонларнинг кенг қўлланилишини улар сир тутилганда топишнинг қийинчилиги билан боғлаш мумкин.

Асосий қисм. Фақат ўзига ва 1 га бўлинадиган сонлар туб сонлар дейилади [4]. Қадимдан натурал сонлар қаторида туб сонларни топиш йўллари билан кўпгина олимлар шуғуланганлилига қарамасдан ханузгача борор ораликдан фақатгина туб сонларни генерация қиладиган функция топилмаган [1]. Чунки туб сонларни бошқа сонлар асосида ифодалаб бўлмайди. Яъни, уларни бир неча соннинг кўпайтмаси шаклида ёзиш мумкин эмас. Бундан ташқари туб сонлар натурал сонлар қаторида текис тақсимланмаган. Туб сонларнинг сони чексиз кўп. Яъни улардан исталганча фойдаланиш мумкин. Лекин сонлар қаторида кам учрайди.

Бирор ораликдаги барча сонлар ҳамда шу ораликдаги туб сонларнинг сонини баҳолаб кўрайлик. Мисол сифатида иккилик саноқ системасидаги 32 разрядли сонларни қараймиз.

32 разрядли энг катта сон $2^{32}-1$. 31 разрядли энг катта сон $2^{31}-1$. Барча 32 разрядли сонлар сонини қуйидагича ҳисоблаш мумкин:

$$(2^{32}-1)-(2^{32}-1)=2^{32}-1-2^{31}+1=$$

$$=2^{32}-2^{31}=2^{31}(2^1-1)=2^{31}=2147483648$$

Энди бу сонлар орасидаги туб сонлар сонини ҳисоблаймиз. Лежандр формуласига асосан [2] n разряддан ошмаган туб сонлар сонини қуйидагича баҳолаш мумкин:

$$\frac{n}{\ln n}=\frac{(n-1)}{\frac{\log_2\left(n-1\right)}{\log_2 e}}=\frac{\log_2 e\times\left(n-1\right)}{\log_2(n-1)}$$

32 разряддан ошмаган туб сонлар сони қуйидагича ҳисоблаш мумкин:

$$\frac{2^{32}}{\ln(2^{32})}=\frac{2^{32}}{\frac{\log_2(2^{32})}{\log_2 e}}=\frac{\log_2 e\times 2^{32}}{\log_2(2^{32})}=$$

$$=1.44\times\frac{2^{32}}{2^5}\approx 193273528$$

(Бу ерда $2^{32}-1$ ни 2^{32} деб ҳисобладик).

31 разряддан ошмаган туб сонлар сони эса қуйидагича:

$$\frac{2^{31}}{\ln 2^{31}}=\frac{2^{31}}{\frac{\log_2(2^{31})}{\log_2 e}}=\frac{\log_2 e\times 2^{31}}{\log_2(2^{31})}=1.44\times\frac{2^{31}}{31}=$$

$$=1.44\times\frac{2^{31}}{2^5}\approx 99754079$$

Демак, 32 разрядли туб сонлар сони $193273528-99754079=93519449$ га тенг экан. Бундан ораликдаги ҳар 30 та сонинг биттаси туб сон бўлади деган хулосага келиш мумкин.

32 битли сонни қуйидагича ифодалашимиз мумкин:

Биз 32 разрядли сондан фойдаланишимиз керак бўлгани учун энг охирги разряд 1 га тенг бўлади. Энг биринчи разрядга 1 қўйишимиз эса бу соннинг тоқлигини билдириди. Туб сонлар тоқ бўлгани учун биз бу ораликдаги барча жуфт сонларни ташлаб юборишимиз мумкин.

Берилган ораликдаги туб сонлар генерациясни қуриш алгоритмида асосан иккита масала кўрилади:

а) берилган чегара оралиғида сон танлаш;

б) танланган сонни тубликка текшириш;

Агар ораликдан танлаб олинган сон туб сон бўлса, уни туб сонлар жадвалига ёзилади. Акс ҳолда ораликдан бошқа сон танлаб олиб тубликка текширилади.

Сонни кетма-кет танлаш кўп вақтни талаб қилиши билан бирга, кетма-кет олинган туб сонларни ишлатиш шифрлаш алгоритмларининг бардошлилигини камайтиради. Шунинг учун сонни тасодифий танлаш йўли билан бир қадар самарадорликка эришиш мумкин. Берилган ораликдан сонларни тасодифий танлаш учун тасодифий миқдорларнинг стандарт функциясини қўлланилади. Бу функция кўпгина дастурлаш тилларида мавжуд.

Эндиги масала тасодифий танлаб олинган сонни тубликка текширишдан иборат бўлади. Сонни тубликка текширишда бир неча эҳтимоллик тестларидан фойдаланилади. Шулардан бири Ферманинг кичик теоремаси ғоясига асосланган Рабин-Миллер тести ҳисобланади.

Ферманинг кичик теоремаси: Агар p туб сон ва a ихтиёрий бутун сон бўлса, унда $a^{p-1} \equiv 1 \bmod p$ бўлади [5]. Яъни p туб сон бўлиши учун барча $1 \le a < p$ лар учун $a^{p-1} \bmod p = 1$ ифода ўринли бўлиши керак. Биз аввал $p-1$ ни $2^t s$ кўринишда ёзиб оламиз. Бу ерда s тоқ сон. $2^t = k$ деб белгилайлик. У ҳолда $a^{sk} = a^{p-1}$ тенглик ўринли бўлиши керак.

Ихтиёрий сонни қуйидаги кўринишда ёзиш мумкин: $a_0 2^0 + a_1 2^1 + a_2 2^2 + ...a_m 2^m$; $a_i \in \{0,1\}$ 2^0 ни қавсдан ташқарига чиқарсак ифода $2^t s = 2^0 (a_0 + a_1 2^1 + +a_2 2^2 + ...a_m 2^m)$; кўринишга келади. Бу ерда $t = 0$; $s = (a_0 + a_1 2^1 + a_2 2^2 + ...a_m 2^m)$; $a_0 = 1$ бўлиши керак, акс ҳолда бу сон жуфт сон бўлиб қолади. Агар $a_0 = 0$ бўлса, унда 2^1 ни қавсдан ташқарига чиқарамиз: $2^t s = 2(a_1 + a_2 2^1 + a_3 2^2 + ...a_m 2^{m-1})$; Бу ерда $t = 1$; $s = (a_1 + a_2 2^1 + a_3 2^2 + ...a_m 2^{m-1})$; Энди $a_1 = 1$ бўлиши керак, акс ҳолда сон жуфт сон бўлиб қолади. Агар $a_1 = 0$ бўлса, унда 2^2 ни қавсдан ташқарига чиқарамиз: $2^t s = 2^2 (a_2 + a_3 2 + a_4 2^2 + ...a_m 2^{m-2})$; Бу ерда $t = 2$; $s = (a_2 + a_3 2 + a_4 2^2 + ...a_m 2^{m-2})$;

а) агар $a^s \equiv 1 (\bmod p)$ бўлса $a^{p-1} \bmod p = 1$ бўлади ва p эҳтимоллик билан туб сон бўлади;

б) агар $a^s \equiv 1 (\bmod p)$ бўлмаса унда a^{2s} ни текширамиз;

Агар $a^{2s} \equiv 1 (\bmod p)$ бўлса, $a^{p-1} \bmod p = 1$ бўлади ва p эҳтимоллик билан туб сон бўлади. Агар $a^{2s} \equiv 1 (\bmod p)$ бўлмаса, унда a^{4s} ни текширамиз. Худди шу тарзда 2 нинг даражасини t мартагача ошириб текшириб борамиз. Агар t нинг барча қийматларида ҳам $a^{sk} \equiv 1 (\bmod p)$ бўлмаса p туб сон бўлмайди.

Агар k та тасодифий a қийматлари учун p мураккаб эмаслиги аниқланса, у ҳолда берилган p, $(1 - \frac{1}{4^k})$ эҳтимоллик билан туб сон деб юритилади [3].

Хулоса. Юқоридагилардан келиб чиқиб катта туб сонларни генерация қилишда қуйидагиларни эътиборга олиш лозим:

а) берилган ораликдан сонни тасодифий танлаш. Тасодифий танланган сонлар калитлар бардошлилигини оширишга хизмат қилади. Бунинг учун замонавий дастурлаш тилларида мавжуд бўлган махсус функциялардан фойдаланиш мумкин.

б) танлаб олинган сонни дастлаб кичик туб сонлар бўлиб чиқиш лозим. Бу амал танланган сонни тубликка текшириш тезлигини оширишга имкон беради.

в) топилган туб сонларни туб сонлар жадвалига жойлаштиришда уларни топилган вақти бўйича эмас, балки тасодифий жойлаштириш лозим. Бу амал орқали калитлар бордишлилигини янада оширишга эришилади.

г) зарур бўлганда туб сонларлар жадвалидан сонни кетма-кет эмас, балки тасодифий танлаб олиш мақсадга мувофиқ ҳисобланади.

Ушбу алгоритмдан очиқ калитли криптоалгоритмлар учун катта туб сонларни генерация фойдаланиш мумкин.

Адабиётлар

1. Назаров Р.Н., Тошпўлатов Б.Т., Дўсимбетов А.Д. Алгебра ва сонлар назарияси. II қисм. –Тошкент: 1995.
2. Фергюсон Н., Шнайер Б. Практическая криптография. –Москва: Санкт-Петербург. –Киев: 2005. –С.421.
3. Шнайер Б. Прикладная криптография. 2-е здание. Протоколы, алгоритмы и исходные тексты на языке С. «Триумф», 2002. -С. 861.
4. http://www.sans.org/reading-room/whitepapers/vpns/prime-numbers-public-key-cryptography-969
5. http://home.sandiego.edu/~dhoffoss/teaching/cryptography/10-Rabin-Miller.pdf

РЕЗЮМЕ

Ушбу мақолада замонавий криптографияда катта туб сонларнинг тутган ўрни, берилган ораликдаги туб сонлар сонини ҳисоблаш, сонни тубликка текшириш усуллари ва олинган туб сонлар жадвалидан фойдаланиш тамойиллари таҳлил қилинган

РЕЗЮМЕ

В этой статье анализирован роль больших простых чисел в современной криптографии, вычисление количество простых чисел в данном диапазоне, методы проверка числа на простоту и принцип использование с таблицам простых чисел.

SUMMARY

This article analyzed the role of large prime numbers in modern cryptography; calculate the number of prime numbers in this range, the methods of verification of the simplicity and the principle of the use of a table of prime numbers.