Параметрли алгебра асосида такомиллаштирилган Нюберг–Руппель “кўр-кўрона” электрон рақамли имзо алгоритми

О.П. Ахмедова т.ф.н., М.Х. Назарова ф.-м.ф.н. («UNICON.UZ» ДУК), Х.Х. Ахмедова (ТАТУ)

Ушбу мақолада замонавий электрон тизимларда ахборот хавфсизлиги муаммосини ҳал этиш учун мўлжалланган Нюберг–Руппелнинг “кўр-кўрона” электрон рақамли имзо алгоритми моҳияти ва унинг параметрли алгебра асосида такомиллаштирилган русуми келтирилган.

В данной статье приведена основная суть алгоритма «слепой» электронной цифровой подписи Нюберга–Руппеля и усовершенственный вариант алгоритма «слепой» электронной цифровой подписи на основе алгебры с параметром, который предназначен для решения проблемы информационной безопасности в современных электронных системах.

This article presents the main essence of the Nyberg-Ruppel algorithm of the “blind” digital signature and an improved version of the algorithm of the “blind” digital signature based on algebra with a parameter that is designed to solve the problem of information security in modern electronic systems.

Ривожланган давлатларда турли хил савдо ва тижорат ишлари ўша мамлакат иқтисодиётининг асосий бўғини ҳисобланади. Бизнеснинг XX аср охирида компьютерлаштирилиши ишнинг тез ва унумли амалга ошишига ҳамда самарадорликни юқори кўрсаткичга эришишига олиб келувчи фактор бўлиб хизмат қилмоқда. Интернет орқали бажариладиган электрон савдонинг ва турли интерфаол хизматларнинг кескин ривожланиши натижасида ахборот хавфсизлигини таъминлаш масаласи муҳим аҳамият касб этмоқда. Фойдаланувчилар, шу жумладан харидорлар, кредит картаси соҳиблари, бевосита тармоқ орқали турли хизматлардан фойдаланиши ва тўловларни бажариши учун ишончли ҳимояланган дастурий ва аппарат воситаларга эга бўлиши лозим. Бугунги кунда Интернет тармоқлари орқали амалга ошириладиган хизматларнинг хавфсизлигини таъминлашда энг ишончли восита сифатида криптографик усуллар ва воситалардан фойдаланилмоқда. Шунга кўра дастурий таъминотлар ва аппарат воситалар ишлаб чиқарувчилар ушбу йўналишга катта эътибор қаратмоқдалар.

Ушбу мақолада замонавий электрон тўлов тизимларида тўловларни амалга ошириш ҳамда яширин овоз бериш жараёнларидаги ахборот хавфсизлиги муаммосини ҳал этишда муҳим ўрин эгаллаган криптографик восита - “кўр-кўрона” электрон рақамли имзо алгоритмининг моҳияти ва унинг такомиллаштирилган русуми баён этилади.

“Кўр-кўрона” электрон рақамли имзонинг асосий моҳияти қуйидагича [1]. **A** юборувчи ҳужжатни **B** томонга юборади. **B** томон эса ҳужжатни имзолайди ва қайта **A** томонга юборади. **A** томон қабул қилган имзосидан фойдаланиб **B** томоннинг имзосини ҳисоблаб топиши ва уни ўзи учун муҳим бўлган ҳужжатни

имзолашда ишлатиши мумкин. Бу протоколнинг бажарилиш якунида **B** томон махфий хабар ҳақида ҳам ва унинг тагидаги имзо ҳақида ҳам ҳеч нарсани билмайди.

Ушбу схемани ичига ҳужжат ва нусха кўчирувчи қоғоз жойланган конверт билан таққослаш мумкин. Агар конверт имзоланса, имзо ҳужжатга ҳам кўчиб қолади, бунда конверт очилганда ҳужжат имзоланган бўлади.

Бунда “кўр-кўрона” имзодан мақсад имзоловчи шахс **B** нинг **A** томон хабари остига имзосини қўйиш асносида, **B** нинг ушбу хабар билан танишишига тўсқинлик қилишдан иборат.

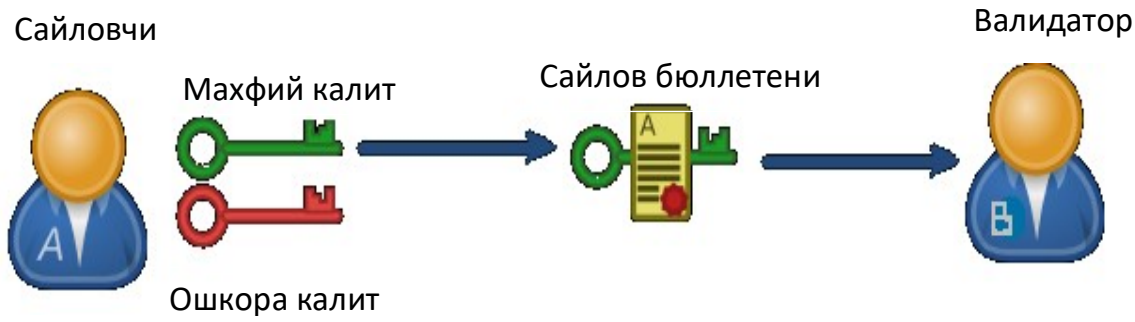
“Кўр-кўрона” имзо протоколлари рақамли пул соҳасида кенг қўлланилади. Масалан, банк омонатчи алдамаслиги учун қуйидаги протоколдан фойдаланиши мумкин: омонатчи бир хил купюра номиналини 100 та турли рақамли ҳужжатларга ёзади ва банкда шифрланган ҳолда депозитга қўяди. Банк тасодифий равишда 99 тасини танлайди ва барчасида $10 ўрнига $1000 ёзилмаганлигини текшириш учун очишни талаб қилади. Сўнгра очилмай қолган конвертдаги купюрани кўрмасдан имзолайди.

Замонавий электрон тўлов тизимларининг асосий криптографик хусусияти уларда қўлланилган “кўр-кўрона” электрон рақамли имзо ғоясидир. Бу ғоя биринчи марта Дэвид Шаум ишларида таклиф этилган [2].

Қуйида “кўр-кўрона” электрон рақамли имзо алгоритмининг умумий схемаси келтирилган:

1. **B** ҳар бирида қандайдир уникал сўз ёзилган *n* та ҳужжат тайёрлайди.
2. Ҳар бир ҳужжатни **B** бирор бир тасодифий сонга кўпайтиради, яъни уни уникал ниқобловчи (маскаловчи) кўпайтувчи билан ниқоблайди ва ҳосил бўлган ҳужатларни **A** га юборади.
3. **A** барча ҳужжатларни қабул қилади ва тасодифий ҳолда улардан *n-1* тасини танлайди.
4. **A** томон **B** дан танланган ҳужжатлар учун ниқобловчи кўпайтувчиларни юборишини сўрайди.
5. **B** юборади.
6. **A** *n-1* та ҳужжатни очади ва уларнинг ҳақиқийлигига ишонч ҳосил қилади.
7. **A** қолган ҳужжатларни имзолайди ва **B** га юборади.
8. Энди **B** да **A** томонидан имзоланган уникал сўзли ҳужжат бор бўлиб, буни **A** билмайди.

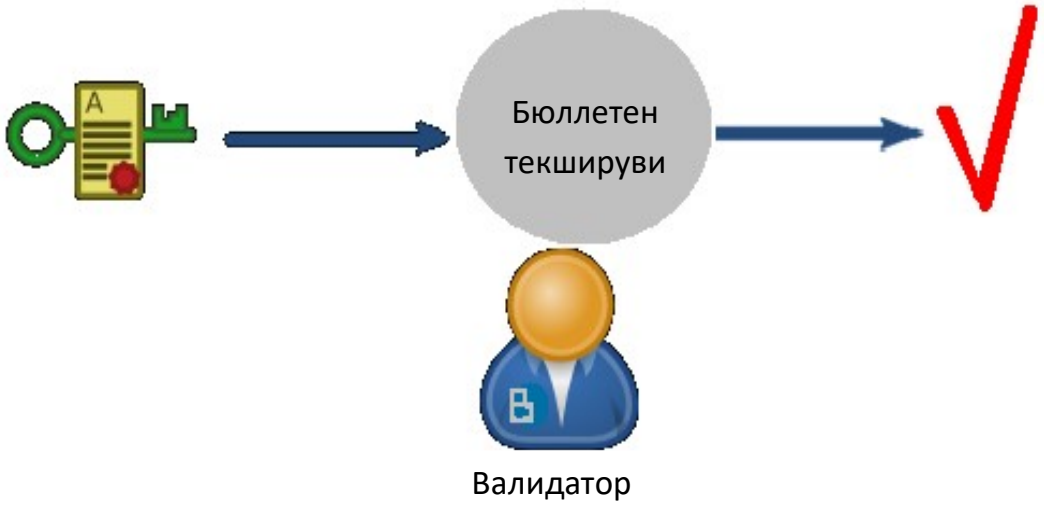
“Кўр-кўрона” электрон рақамли имзодан шунингдек яширин овоз беришда ҳам фойдаланилади. Фуджиока, Окамото ва Охта [3] томонидан таклиф этилган протоколда сайловчи ўзи танлаган сайланувчи акслантирилган сайлов бюллетенини тайёрлайди, сўнгра уни махфий калити билан шифрлайди ва ниқоблайди. Сайловчи сайлов бюллетенини имзолайди ва валидаторга юборади (1-расм).



1-расм. Сайловчининг сайлов бюллетенини имзолаши ва валидаторга юбориши

Валидатор имзони рўйхатдан ўтган аммо ҳали овоз бермаган сайловчига тегишлилигини текширади.

Агар сайлов бюллетени ҳақиқий бўлса, валидатор сайлов бюллетенини имзолайди ва уни сайловчига қайтаради (2-расм).

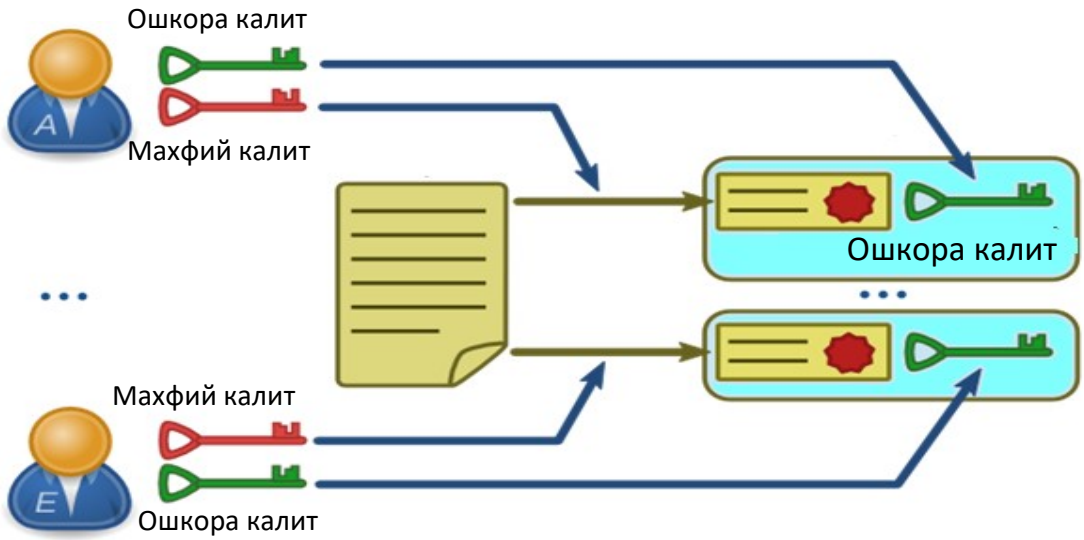


2-расм. Валидаторнинг сайлов бюллетенини текшириши

Сайловчи валидатор томонидан имзоланган шифрланган сайлов бюллетенини очиб, ниқобни олиб ташлайди. Сўнгра сайловчи олинган имзоланган, шифрланган сайлов бюллетенини ҳисоблагичга юборади, ҳисоблагич шифрланган сайлов бюллетенидаги имзони текширади. Агар сайлов бюллетени ҳақиқий бўлса, ҳисоблагич уни овоз беришдан кейин чоп этиладиган рўйхатга киритиб қўяди.

Рўйхат чоп этилганидан кейин сайловчи сайлов бюллетенини рўйхатда мавжудлигини текширади, сўнгра ҳисоблагичга ўз сайлов бюллетенини очиши учун шифрни очиш калитини юборади. Ҳисоблагич бу калитдан сайлов

бюллетенларини шифрини очишда ва овозни умумий ҳисобга қўшишда фойдаланади.



3-расм. Шифрланган сайлов бюллетени ҳамда шифрни очиш калитининг бирга чоп этилиши

Сайловлардан сўнг сайловчилар ўзлари мустақил сайлов натижаларини текшириб кўришлари учун ҳисоблагич шифрланган сайлов бюллетени ҳамда шифрни очиш калитини бирга чоп этади (3-расм).

“Кўр-кўрона” электрон рақамли имзо алгоритмлари асосланган муаммосига кўра бир неча синфларга бўлинади:

1. Факторлаш муаммосига асосланган “кўр-кўрона” электрон рақамли имзо алгоритмлари.
2. Дискрет логарифмлаш муаммосига асосланган “кўр-кўрона” электрон рақамли имзо алгоритмлари.
3. Эллиптик эгри чизиқларда дискрет логарифмлаш муаммосига асосланган “кўр-кўрона” электрон рақамли имзо алгоритмлари.

Қуйида дискрет логарифмлаш муаммосига асосланган Нюберг–Руппелнинг электрон рақамли имзо ва “кўр-кўрона” электрон рақамли имзо алгоритмлари баён этилади.

Нюберг–Руппелнинг электрон рақамли имзо алгоритми [4].

Параметрларни генерация қилиш босқичи:

1. Туб p сон танланади, унинг узунлиги *1024* бит.
2. Бошқа туб сон q ни шундай танлаш керакки, у $p-1$ нинг бўлувчиси бўлсин, яъни $p-1 \equiv 0 \pmod q$. q нинг ўлчови *160* бит қилиб танлаш қабул қилинган.
3. *1* дан фарқли g ни шундай танлаш керакки, $g^q \equiv 1 \pmod p$ бўлсин.
4. **A** томон q дан кичик бўлган ихтиёрий бутун x сонини махфий калит сифатида танлайди.
5. **A** томон ошкора калитни $y=g^x \pmod p$ ҳисоблайди.

6. **A** томоннинг ошкора калити – *(p, q, g, y)*, махфий калити – *x* бўлади.

m хабар учун электрон рақамли имзони шакллантириш босқичи:

1. **A** томон *q* дан кичик бўлган ва *y* билан ўзаро туб бўлган ихтиёрий бутун *k* сонини танлайди ва *r, s* ни ҳисоблайди.

2. $r=mg^k \pmod q$ ни ҳисоблайди.

3. $s=xr+k \pmod q$ ни ҳисоблайди, бунда *(r,s) m* хабарнинг электрон рақамли имзоси бўлади.

4. **A** томон **B** га *m* хабарни *(r,s)* электрон рақамли имзо билан юборади.

Электрон рақамли имзони текшириш босқичи:

1. **B** томон $m = g^{-s}y^r r \pmod p$ ни ҳисоблайди,

бунда *–s* - *s* нинг *q* модул бўйича қарама-қаршиси. Агар тенглик бажарилса, демак электрон рақамли имзо ҳақиқий бўлади.

1-*мисол*

Туб *p* сон танланади *p=47.*

p-1 нинг туб кўпайтувчиси *q=23.*

g=6.

Махфий калит *x=11.*

Ошкора калит: $y= g^x \pmod p=6^{11} \pmod{47}= 14.$

Имзоланадиган хабар: *m=17.*

A томон ихтиёрий сон танлайди: *k=5.*

A қуйидагиларни ҳисоблайди:

$r=mg^k \pmod q=17\cdot 6^5 \pmod{23}=28;$

$s=xr+k \pmod q=11\cdot 28+5 \pmod{23}=14.$

A томон **B** га *m=17* хабарни *(28,14)* электрон рақамли имзо билан юборади.

Имзони текшириш босқичи:

B қуйидаги ифодани ҳисоблаб, имзони ҳақиқийликка текширади:

$m = g^{-s}y^r r \pmod p = 6^{-14}\cdot 14^{28}\cdot 28 \pmod{47}=3\cdot 3\cdot 28 \pmod{47}=17.$

Демак, хабарга қўйилган электрон рақамли имзо ҳақиқий.

Қуйида Нюберг–Руппелнинг “кўр-кўрона” электрон рақамли имзо алгоритми келтирилди [5].

Параметрларни генерация қилиш босқичи худди электрон рақамли имзо *алгоритмидаги каби бўлади:*

1. Туб *p* сон танланади, унинг узунлиги *1024* бит.

2. Бошқа туб сон *q* ни шундай танлаш керакки, у *p-1* нинг бўлувчиси бўлсин, яъни $p-1\equiv 0 \pmod q$. *q* нинг ўлчови *160* бит қилиб танлаш қабул қилинган.

3. *1* дан фарқли *g* ни шундай танлаш керакки, $g^q \equiv 1 \pmod p$ бўлсин.

4. **A** томон *q* дан кичик бўлган ихтиёрий бутун *x* сонини махфий калит сифатида танлайди.

5. **A** томон очиқ калитни $y=g^x \pmod p$ ҳисоблайди.

6. **A** нинг очиқ калити – *(p,q,g,y)*, махфий калити – *x* бўлади.

m хабар учун "кўр-кўрона" электрон рақамли имзони шакллантириш босқичи:

1. **A** томон *q* дан кичик бўлган ва *y* билан ўзаро туб бўлган ихтиёрий бутун $\tilde{k}$ сонини танлайди ва $\tilde{r} = g^{\tilde{k}} (mod\ q)$ ни ҳисоблайди. Ҳосил бўлган $\tilde{r}$ қийматни **B** га юборади.

2. *a)* **B** тасодифий равишда $\alpha \in Z_q$ ва $\beta \in Z_q$ сонларни танлайди ва $r = mg^{\alpha}\tilde{r}^{\beta}\ (mod\ p)$ ни ва $\tilde{m} = r\beta^{-1}\ (mod\ q)$ ни ҳисоблайди.

b) **B** томон $\tilde{m} \in Z_q$ шартни текширади, агар шарт бажарилса, $\tilde{m}$ ни **A** томонга юборади, акс ҳолда *a)* қадамга қайтади.

3. **A** томон $\tilde{s}=\tilde{m}x+\tilde{k}$ ни ҳисоблайди ва $\tilde{s}$ ни **B** га юборади.

4. **B** томон $s = \tilde{s}\beta + \alpha (mod\ q)$ ни ҳисоблайди.

5. Электрон рақамли имзони текшириш босқичи:

1. **B** томон $m = g^{-s}y^{r}r\ (mod\ p)$ ни ҳисоблайди,

бунда *–s* сони - *s* нинг *q* модул бўйича қарама-қаршиси. Агар тенглик бажарилса, демак имзо ҳақиқий бўлади.

2-мисол

1-мисолда келтирилган қийматлар учун Нюберг–Руппель алгоритми асосида берилган хабар учун "кўр-кўрона" электрон рақамли имзони ҳосил қиламиз.

p=47, q=23, g=6, m=17.

Махфий калит *x=11.*

Ошкора калит: $y= g^{x} (mod\ p)=6^{11} (mod\ 47)= 14.$

A томон ихтиёрий сон танлайди: $\tilde{k}$ *=5.*

A томон қуйидагини ҳисоблайди: $\tilde{r} = g^{\tilde{k}} (mod\ q)=6^{5} (mod\ 23)=4.$

Ҳосил бўлган $\tilde{r} = 4$ қийматни **B** га юборади.

B томон α*=5* ва β*=13* сонларни танлайди ва

$r = mg^{\alpha}\tilde{r}^{\beta}\ (mod\ p)$ *=*$17\cdot 6^{5}\cdot 4^{13}$ *(mod 47)=36.*

$\tilde{m} = r\beta^{-1}\ (mod\ q)$*=*$36\cdot 13^{-1}$ *(mod 23)=*$36\cdot 16$ *(mod 23)=1* ҳисоблайди.

B томон $\tilde{m} = 1 \in Z_q$ шартни текширади, $\tilde{m}$ ни **A** томонга юборади.

A томон $\tilde{s}=\tilde{m}x+\tilde{k}\ (mod\ q)$ *=1·11+5(mod 23)=18* ни ҳисоблайди ва

$\tilde{s} = 18$ ни **B** га юборади.

B томон $s = \tilde{s}\beta + \alpha (mod\ q)$*=18·13+5 (mod 23)=9* ҳисоблайди.

Имзони текшириш босқичи:

B томон $m = g^{-s}y^{r}r\ (mod\ p)$ *=*$6^{-9}\cdot 14^{36}\cdot 36$ *(mod 47)=17* ҳисоблайди.

Тенглик бажарилди, демак "кўр-кўрона" имзо ҳақиқий.

Қуйида Нюберг–Руппель "кўр-кўрона" электрон рақамли имзо алгоритмини такомиллаштириш учун асос бўлиб хизмат қилувчи параметрли алгебранинг таърифи ва асосий амаллари келтирилди [6].

Таъриф. F_n – чекли, яъни, *n* та элементдан иборат бутун сонлар тўплами, ® – F_n устида $a®b \equiv a + b + a \cdot R \cdot b \ (mod\ n)$ кўринишида аниқланган алгебраик амал бўлса, (F_n; Ω) – жуфтлик параметрли мультипликатив группа деб аталади; бу ерда $a,\ b,\ R \in F_n$, параметр $R>0$, +, · – бутун сонлар устида қўшиш, кўпайтириш амалларининг ва ® – параметрли кўпайтириш амалининг белгилари.

Нолдан фарқли тўплам элементи *a* учун тескари элемент $a^{\backslash -1}$ ва қарама-қарши элемент *n-a* мавжуд. $a^{\backslash -1}$ параметрли тескари элемент деб аталади ва $a®a^{\backslash -1} \equiv 0 \ (mod\ n)$ шартини қаноатлантиради. Бу ерда *0* – параметрли бирлик элементи бўлиб, $a®0 \equiv a$ аксиомани қаноатлантиради.

Параметрли тескари элемент қуйидагича ҳисобланади:

$$a^{\backslash -1} \equiv - a(1+ aR)^{-1} \ (mod\ n).$$

Бу ерда $^{-1}$ - *n* модул бўйича тескарилаш амалининг белгисидир.

Таъриф. Модул арифметикасида параметр $R \geq 1$ билан даражага ошириш функцияси параметрли функция деб аталади.

Модул *n* бўйича асос *a* ни *R* параметрли *x* даражага ошириш натижаси $a^{\backslash x} (mod\ n)$ шаклида ифодаланади, бу ерда $^{\backslash}$ – *R* параметрли даражага ошириш белгисидир**.**

R параметр билан дискрет даражага ошириш худди анъанавий дискрет даражага ошириш жараёни каби рекурсив тарзда ҳисоблашлар орқали амалга оширилади, масалан, *a* нинг *e=37 R* параметрли даражасини қуйидагича ҳисобланади:

$$a^{\backslash 37} (mod\ p) \equiv a^{\backslash (32+4+1)} (mod\ p) \equiv (((((a^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})®(a^{\backslash 2})^{\backslash 2})®a \ (mod\ p),$$

бунда: $a^{\backslash 2} (mod\ p) \equiv a \cdot (2+R \cdot a) \ (mod\ p)$.

Ушбу келтирилган параметрли алгебра ва параметрли функцияни қўллаб, Нюберг–Руппель протоколига асосланган “кўр-кўрона” электрон рақамли имзо алгоритмини такомиллаштирамиз.

Нюберг–Руппель протоколига асосланган такомиллаштирилган “кўр-кўрона” электрон рақамли имзо алгоритми.

Параметрларни генерация қилиш босқичи:

1. Туб *p* сон танланади, унинг узунлиги *1024* бит.
2. Бошқа туб сон *q* ни шундай танлаш керакки, у *p-1* нинг бўлувчиси бўлсин, яъни $p-1 \equiv 0 \ (mod\ q)$. *q* нинг ўлчови 160 бит қилиб танлаш қабул қилинган.
3. *R* – параметр, $R < q$ шартни қаноатлантирувчи натурал сон бўлиб, фойдаланувчиларнинг чекланган гуруҳи учун очиқ ҳисобланади.
4. *1* дан фарқли *g* ни шундай танлаш керакки, $g^q \equiv 1 \ (mod\ p)$ бўлсин.
5. **A** томон *q* дан кичик бўлган ихтиёрий бутун *x* сонини махфий калит сифатида танлайди.
6. **A** томон очиқ калитни $y=g^{\backslash x} \ (mod\ p)$ ҳисоблайди.
7. **A** томоннинг очиқ калити – *(p,q,g,y)*, махфий калити – *x* бўлади.

m хабар учун “кўр-кўрона” электрон рақамли имзони шакллантириш босқичи:

1. **A** томон *q* дан кичик бўлган ва у билан ўзаро туб бўлган ихтиёрий бутун $\tilde{k}$ сонини танлайди ва $\tilde{r} = g^{\backslash \tilde{k}} (mod\ p)$ ни ҳисоблайди. Ҳосил бўлган $\tilde{r}$ қийматни **B** га юборади.

2. *a)* **B** томон тасодифий равишда $\alpha \in Z_q$ ва $\beta \in Z_q$ сонларни танлайди ва $r = m \cdot g^{\alpha} \cdot \tilde{r}^{\beta} \pmod p$ ни ва $\tilde{m} = r\beta^{-1} \pmod q$ ни ҳисоблайди.

b) **B** томон $\tilde{m} \in Z_q$ шартни текширади, агар шарт бажарилса $\tilde{m}$ ни **A** томонга юборади, акс ҳолда *a)* қадамга қайтади.

3. **A** томон $\tilde{s}=\tilde{m}x+\tilde{k}$ ни ҳисоблайди ва $\tilde{s}$ ни **B** га юборади.

4. **B** томон $s = \tilde{s}\beta + \alpha \pmod q$ ни ҳисоблайди.

Имзони текшириш босқичи:

1. **B** томон $m = g^{-s} \cdot y^{r} \cdot r \pmod p$ ни ҳисоблайди,

бунда *–s* сони - *s* нинг *q* модул бўйича қарама-қаршиси. Агар тенглик бажарилса, демак имзо ҳақиқий бўлади.

3-мисол.

2-мисолда келтирилган қийматлар учун Нюберг–Руппель алгоритми асосида берилган хабар учун параметрли алгебра асосида такомиллаштирилган “кўр-кўрона” *электрон рақамли имзо*ни ҳосил қилиш жараёнида қандай ўзгаришлар юз беришини кўриб чиқамиз.

Туб *p* сон танланади *p=47.*

p-1 нинг туб кўпайтувчиси *q=23.*

Параметр *R=17.*

g=6.

Махфий калит *x=11.*

Ошкора калит: $y=g^x \pmod p = 6^{11} \pmod{47} = 23.$

Имзоланадиган хабар: *m=17.*

A томон ихтиёрий сон танлайди: $\tilde{k}=5.$

A томон қуйидагини ҳисоблайди:

$\tilde{r} = g^{k} \pmod q = 6^5 \pmod{23} = 12.$

Ҳосил бўлган $\tilde{r} = 12$ қийматни **B** томонга юборади.

B томон $\alpha=5$ ва $\beta=13$ сонларни танлайди ва

$r = m \cdot g^{\alpha} \cdot \tilde{r}^{\beta} \pmod p = 17 \cdot 6^5 \cdot 12^{13} \pmod{47} = 18.$

$\tilde{m} = r\beta^{-1} \pmod q = 18 \cdot 13^{-1} \pmod{23} = 18 \cdot 16 \pmod{23} = 12.$

A томон $\tilde{s}=\tilde{m}x+\tilde{k} \pmod q = 12 \cdot 11+5 \pmod{23} = 22$ ни ҳисоблайди ва $\tilde{s} = 22$ ни **B** томонга юборади.

B томон $s = \tilde{s}\beta + \alpha \pmod q = 22 \cdot 13+5 \pmod{23} = 15$ ни ҳисоблайди.

Имзони текшириш босқичи:

B томон $m = g^{-s} \cdot y^{r} \cdot r \pmod p = 6^{-15} \cdot 23^{18} \cdot 18 = 17$ ифодани ҳисоблайди.

Демак, хабарга қўйилган “кўр-кўрона” электрон рақамли имзо ҳақиқий.

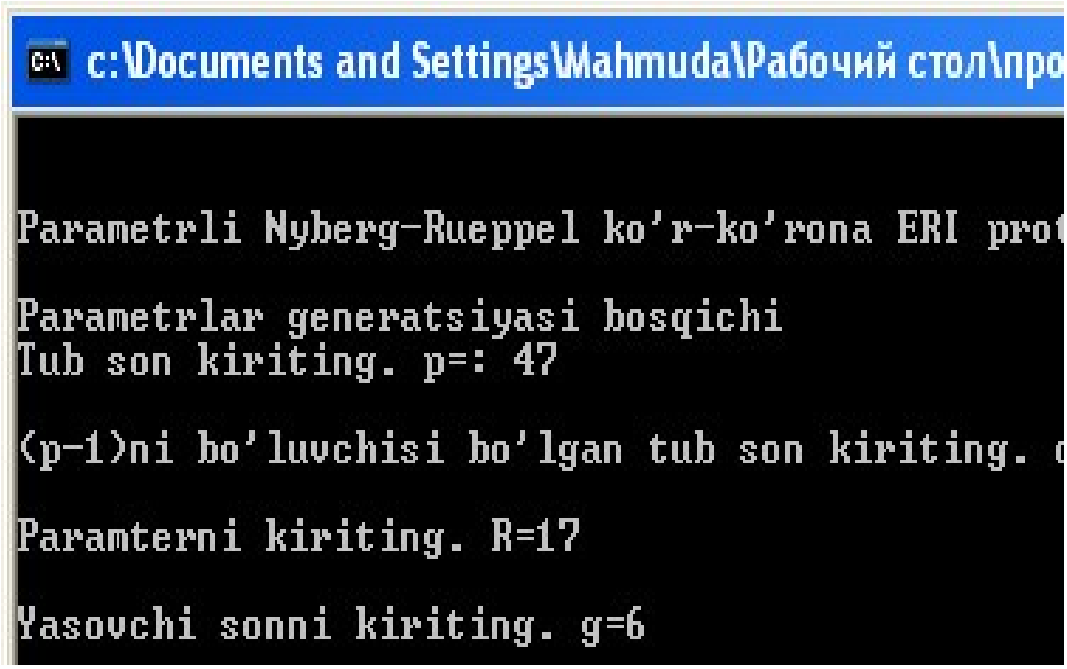
Дискрет логарифмлаш муаммосига асосланган такомиллаштирилган “кўр-кўрона” электрон рақамли имзо алгоритми асосида ишлаб чиқилган дастурнинг ишлаши қуйида келтирилган.

“Кўр-кўрона” электрон рақамли имзонинг параметрли алгебра асосида такомиллаштирилган Нюберг – Руппель протоколи алгоритмининг дастури:

Параметрларни генерация қилиш босқичида асосий параметрлар ва калитлар генерация қилинади:

- туб сон,
- уни битта камайтирганда бўлувчиси бўладиган яна бир туб сон,
- *R* – параметр,
- майдон ясовчиси бўлган сон,
- махфий калит ва унга мос бўлган ошкора калит.

Қуйидаги 4-расмда *ташкилий босқичнинг дастур ойнаси* келтирилган.

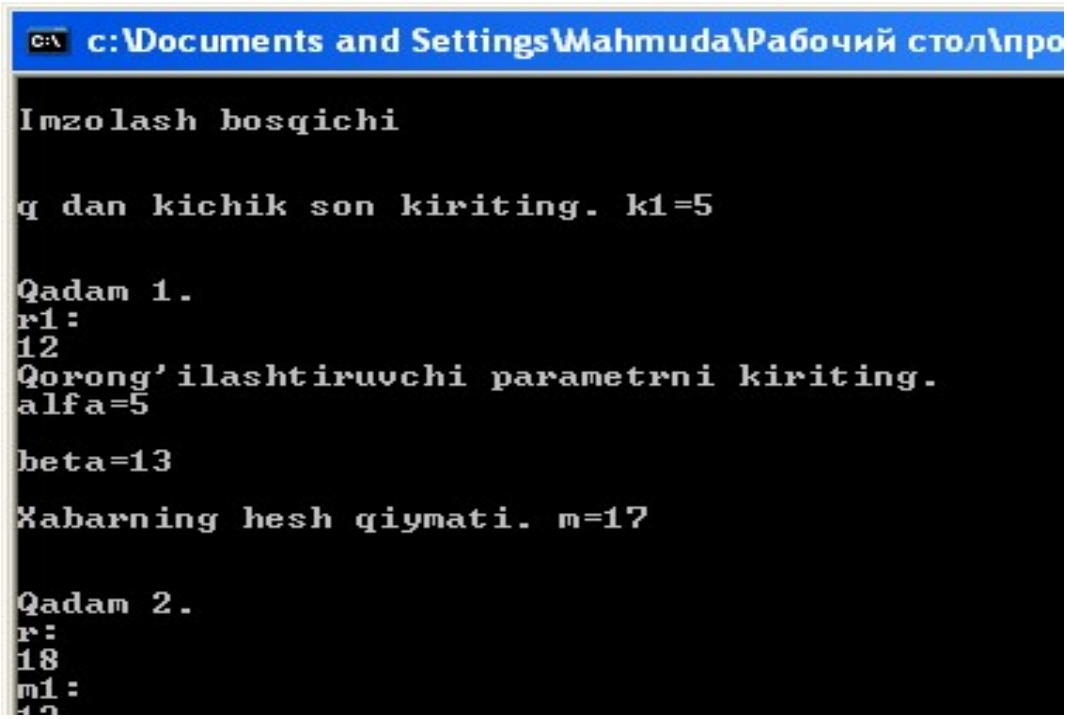


4-расм. Ташкилий босқич дастур ойнаси

“Кўр-кўрона” электрон рақамли имзонинг параметрли алгебра асосида такомиллаштирилган Нюберг–Руппель алгоритми асосида *m* хабар учун “кўр-кўрона” электрон рақамли имзо шакллантириш босқичида:

- **A** томон *q* дан кичик бўлган ихтиёрий бутун $\tilde{k}$ сонини танлайди ва $\tilde{r} = g^{\tilde{k}} (mod\ p)$ ни ҳисоблайди.
- **B** тасодифий равишда қоронғилаштириш коэффициентлари бўлган $\alpha \in Z_q$ ва $\beta \in Z_q$ сонларни танлайди ва $r = m \cdot g^{\alpha} \cdot \tilde{r}^{\beta} \ (mod\ p)$ ҳамда $\tilde{m} = r\beta^{-1} \ (mod\ q)$ ни ҳисоблайди.
- **A** томон $\tilde{s}=\tilde{m}x+\tilde{k}$ ни ҳисоблайди ва $\tilde{s}$ ни B га юборади.
- **B** томон $s = \tilde{s}\beta + \alpha \ (mod\ q)$ ни ҳисоблайди.

Ушбу босқичнинг дастурий ойнаси қуйидаги 5–расмда маълум бир қийматлар учун келтирилган.



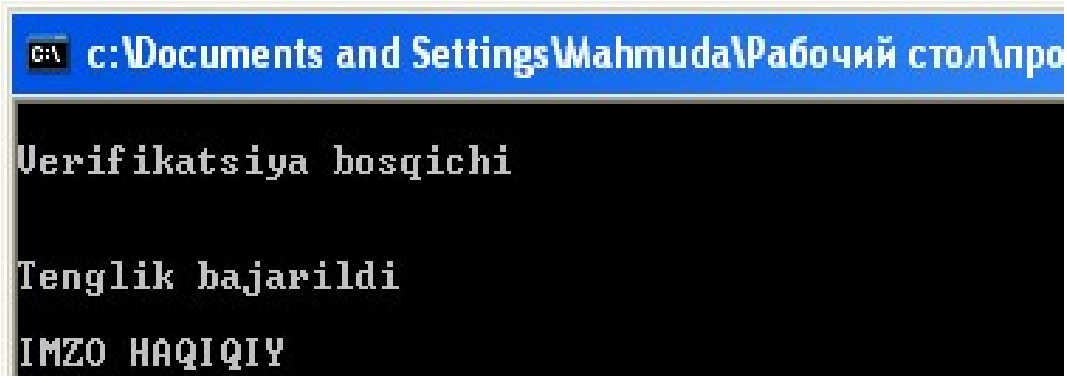
5-расм. *Нюберг – Руппель* протоколига асосланган такомиллашган “кўр-кўрона” ЭРИни шакллантириш босқичи

Нюберг–Руппель протоколига асосланган параметрли алгебра асосида такомиллаштирилган “кўр-кўрона” электрон рақамли имзони сўнгги босқичи бўлган текшириш босқичида:

B томон $m = g^{\backslash -s} \circledR y^{\backslash r} \circledR r \ (mod\ p)$ ни ҳисоблайди,

бунда - *s* сони - *s* нинг *q* модул бўйича қарама-қаршиси. Агар тенглик бажарилса, демак имзо ҳақиқий бўлади.

Қуйидаги 6–расмда Нюберг–Руппель протоколига асосланган параметрли алгебра асосида такомиллаштирилган “кўр-кўрона” электрон рақамли имзо протоколи *текшириш босқичининг дастур ойнаси* келтирилган.



6-расм. Нюберг–Руппель протоколига асосланган такомиллашган “кўр-кўрона” электрон рақамли имзони текшириш босқичи

“Кўр-кўрона” электрон рақамли имзонинг параметрли алгебра асосида такомиллаштирилган дискрет логарифмлаш муаммосига асосланган Нюберг–Руппель алгоритмининг дастури қуйидаги конфигурацияли компьютерда ишлаб чиқилди:

Операцион тизим: Windows 7.

Тезкор хотира: 4.00 ГБ.

Тизим тури: 64 разрядли ОТ.

Процессор: Intel (R) Pentium (R) CPU G2020, 2.90 GHz.

Келтирилган “кўр-кўрона” электрон рақамли имзо алгоритмида модул сифатида туб сондан фойдаланилган. Таклиф этилган “кўр-кўрона” электрон рақамли имзо алгоритмида бардошлилик параметрли функциялар билан боғлиқ янги муаммолар мураккаблиги билан асосланади.

Хулоса. Параметрли алгебра асосида такомиллаштирилган дискрет логарифмлаш муаммоси мураккаблигига асосланган “кўр-кўрона” электрон рақамли имзо алгоритмига Нюберг–Руппель “кўр-кўрона” электрон рақамли имзо алгоритми прототип сифатида қабул қилинган. “Кўр-кўрона” электрон рақамли имзо алгоритми криптобардошлигининг ортиши бир томонлама параметрли функция ифодасида қатнашадиган даражага ошириш параметри R ни ноқонуний фойдаланувчилардан сир сақланиши ҳисобига эришилади.

Мазкур мақолада келтирилган криптографик алгоритм ва унинг дастурий таъминотидан фойдаланиш Ўзбекистон Республикасининг миллий электрон тўлов тизимларида ахборот хавфсизлигини юқори даражада таъминлаб бериши мумкин. Шунингдек ишлаб чиқилган криптографик алгоритм ва унинг дастурий таъминотидан бугунги кунда Интернет тармоқлари орқали амалга ошириладиган хизматларнинг хавфсизлигини таъминлашда фойдаланиш учун тавсия этиш мумкин.

Фойдаланилган адабиётлар рўйхати:

1. М. Иванов, Д. Михайлов, И. Чугунков. Защита информации в электронных платежных системах. Электронный учебник на CD-R. Из-во КноРус – CD-Book. 2011 г.
2. Chaum D. Bilind Signatures for untraceable payments // Advances in Cryptology – Proc. of CRYPTO’82.
3. С.Запечников Криптографические протоколы и их применение в финансовой и коммерческой деятельности, Москва Горячая линия - Телеком 2007.
4. Blind signatures based on the discrete logarithm problem. /Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler // ftp://ftp.inf.ethz.ch /pub/crypto/publications/CaPiSt94b.ps.
5. A blind signature based on the discrete logarithm problem. / Victor P.L. Shen, Yu Fang Chung, Tzer Shyong Chen, Yu An Lin // www.ijicic.org /ijicic-10-05047.pdf.
6. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. Тошкент, ФТМТМ, 2008.