ISSN NO: 2770-0003
Date of Publication: 17-04-2022

Protocol For Electronic Digital Signature of Asymmetric Encryption Algorithm, Based on Asymmetric Encryption Algorithm Based on the Complexity of Prime Decomposition of a Sufficiently Large Natural Number

Akhmadaliev Shakhobidin Sharifovich
Kokand state pedagogical institute, senior teacher, e-mail: 356_qabul_2009@mail.ru
Hasanov Xayrullo Maxmudovich
Kokand state pedagogical institute, teacher, e-mail: xayrullo-xasanov@mail.ru
Botirov Muzaffar Mansurovich
Kokand state pedagogical institute, teacher, e-mail: xayrullo-xasanov@mail.ru

Annotation: In article the report of the electronic digital signature on the basis of asymmetric algorithm of the enciphering based on complexity of decomposition on a proverse of numbers enough of the big natural number is developed. At which formation in process of the digital signature possibility a choice of any number from the signed is provided.

Keywords: matrix, field, parametric multiplication, sufficiently large prime number, multiplier separation, complexity, asymmetric, encryption, algorithm, protocol, electronic digital signature.

The development of information-communication and computer networking technology has set the stage for the implementation of electronic khuzhzhat exchange. To assist individuals desiring to benefit the worldwide work of Jehovah's Witnesses through some form of charitable giving, a brochure entitled Charitable Planning to Benefit Kingdom Service Worldwide has been prepared. (Matthew 24:14; 28:19, 20) Jehovah's Witnesses would be pleased to answers with you. Of course, subjective reasons include a lack of recognition of the longevity of khuzhzhat: information or signatures in khuzhzhat are treated as unbearable. The solution to these issues is solved by an electronic digital signature (EDS).

Рақамли имзо қуйидаги масалаларни ечади [1-3]:

–electron khuzhat manbaasining authenticationsini (hakiykiyligini aniklashni) amalga oshirish imkoniyatini yaratadi;

–хужжатнинг хеш-қиймати кўра унинг бутунлигини аниқлаш усулини беради;

–имзони рад эта олмасликни таъминлайди.

Hozirda ERIni amalga expanding turli usullari (schemes) mavjud bðlib, lartual ute гуруҳга ajartish mumkin:

1) симметрик шифрлашга асосланган рақамли имзо тизими (схемаси);
2) очиқ калитли шифрлашга асосланган тизим (схема);
3) рақамли имзони шакллантириш ва текширишнинг махсус ишлаб чиқилган алгоритмларига асосланган тизим (схема).

Ushbu makolada matrixalari parameterli кўpaitirish va etarli katta sonni tub кўpaytuvchilarga azhratish masalasi echimi murakkabligi asosida yaratilgan [4] nosymmetric ciphrlaš algorithmlaridan foydalanib electron akhborotning:

–mafiyligini ta'minlash imkonini beruvchi;

– In conjunction with the given HF, it is possible to address cryptographic issues, such as verifying the integrity of information and implementing solutions to ensuring its autointification, and developing protocols for practical tasty methods.

Очиқ калитли шифрлаш алгоритми асосида шакллантириладиган ЭРИ камчилиги шундан иборатки, берилган М-маълумотга мос келувчи фақат битта рақамли имзо қўйиш имконияти бор. Чунки берилган М-маълумотга мос келувчи назорат йиғиндиси *НЙ*(М)=*НЙ* ёки хеш-функция

ISSN NO: 2770-0003
Date of Publication: 17-04-2022

$H(M) = H$қийматини ҳисоблаш калитсиз алгоритимга асосланганлиги учун ҳар доим бир хил қийматга эга бўлинади ҳамда шифрлаш ва дешифрлаш натижасида ҳам ҳар доим бир хил ифодага эга бўлинади. Бундай ҳолат шундай ЭРИ алгоритмларидан фойдаланишни ноқулайликларини келтириб чиқаради.

Махсус ишлаб чиқилган (яратилган) ЭРИни ҳисоблашни шакллантириш ва уни текшириш алгоритмлари юқорида келтирилган камчиликлардан холидир. Чунки, бу алгоритмларда ЭРИни шакллантиришда имзоланадиган маълумотнинг хеш-функция қиймати, имзоловчининг маҳфий калитидан ташқари имзоловчи томонидан ихтиёрий танланадиган параметрдан ҳам фойдаланилади.

Қуйида матрицаларни параметрли кўпайтириш ва чекли майдонда дискрет логарифмлаш масаласи ечими мураккаблиги асосида яратилган [4] носимметрик шифрлаш алгоритмини берилган ХФ билан биргаликда, имзоловчи томонидан ихтиёрий танланадиган параметрдан фойдаланиб электрон рақамли имзони амалга ошириш имконини бериб, маълумотнинг бутунлигини текшириш ва унинг аутинтификациясини таъминлаш масалаларининг ечимларига қўллашнинг амалий тадбиқ усуллари ҳамда протоколлари ишлаб чиқилади.

Enough large wa secret thutyl needs to be distinguished and - tube numbers are selected and squeezed. Without this description (here - confidential) - the parameter can be found in the sonins of the relationship by giving it a cup of groceries. So - the key to the trianny okik, - zhuftlikny is confidential, $pqn = pqe_t d_t \equiv 1\, mod\, \phi\,(n)\phi(n) = (p-1)(q-1)\, e_{\iota} e_t d_t \equiv 1\, mod(p-1)(q-1) d_t (A_{n\times m}; e_t; n)(d_t; \phi(n))$kibul kiliinady.

Криптотизимнинг - фойдаланувчиси - фойдаланувчига – очиқ маълумотни$jt\, M = M_{n\times m}$ ва унинг хеш-қийматига боғлиқ бўлган рақамли имзо билан шифрлаб жўнатишни қуйдагича амалга оширади:

1.$M = M_{n\times m}$ - очиқ маълумотни танланган хеш-функция алгоритми бўйича унинг хеш қиймати$H(M) = H(M_{n\times m}) = H_{n\times m} = H$ ҳисобланади.

2. Бу хеш-қиймат бўйича P-рақамли имзоj - фойдаланувчининг d_j-ёпиқ калити ва унинг томонидан танлаб олинган $k^j_{1\,il}$ сонлари билан шакллантирилади:

(a) Facade - tasodify the number of known pieces of information that the user is attracted to, - isoblaidy (here wa). $jk^j_{1\,il} R = R^{jk_1}_{m\times n} = (k^j_{1\,il})\, mod\, n\, k^j_{1\,il} \neq pk^j_{1\,il} \neq q$

б) Шифрлашни $A^j_{n\times m}$®$H = A^j_{n\times m} + H_{n\times m} + A^j_{n\times m} R^{jk_1}_{m\times n} H_{n\times m}(mod\, p) = P_{n\times m}$=$P$ кўринишда амалга оширилиб рақамли имзо шакллантирилади.

3. Имзоланадиган маълумотM ва унинг рақамли имзосиP бирлаштирилиб $M//P = M'$-кенгайтирилган электрон хужжат олинади.

4. Фақат - фойдаланувчининг ўзигагина маълум бўлган бирор - сон$jk^j{}_{il}$ларини тасодифий ҳолда танлаб, $R = R^{jk}_{m\times n} = (k^j_{il})\, mod\, n$, яъни $R^{jk}{}_{m\times n}$ матрицанинг элементлари сифатида қабул қилинади.

5. Шифрлашни кўринишда амалга ошириб, шифрмаълумот сифатида$A^t_{n\times m}$®$M'_{n\times m} = A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m} R^{jk}_{n\times m} M'_{n\times m}(mod\, p) = w_{n\times m}C_{n\times m} = w_{n\times m}; s_t = [(k^j{}_{il})^{d_j}]^{e_t}\, mod\, n\,; s_p = [(k^j_{1\,il})^{d_j}]^{e_t}\, mod\, n)$ - учлик жўнатилади.

Шифр маълумотни$C_{n\times m} = w_{n\times m}; s_t = [(k^j{}_{il})^{d_j}]^{e_t}\, mod\, n\,; s_p = [(k^j_{1\,il})^{d_j}]^{e_t}\, mod\, n)$ қабул қилиб олган - фойдаланувчи дешифрлашни қуйидагича амалга оширади:t

1. Фақат - фойдаланувчининг ўзига маълум бўлган td_t - махфий калитдан ва j-фойдаланувчининг e_j-очиқ калитидан фойдаланиб $(s_t)^{d_t e_j}\, mod\, n = [(k^j{}_{il})^{d_j}]^{e_t d_t e_j}\, mod\, n = k^j{}_{il}$ аниқланиб$R^{jk}{}_{m\times n}$ -матрица элементлари олинади.

2. Open - the key is made up of a reverse-turned matrix with a parameter.$A^t_{n\times m}(A^t_{n\times m})^{-1} = (I_{n\times n} + A^t_{n\times m} D^{jk}_{m\times n})^{-1}(-A^t_{n\times m})\, mod\, p$

3. The deipher is carried out, having based on the action of replacing this clothing: $R = D^{jk}_{n\times m}$

ISSN NO: 2770-0003
Date of Publication: 17-04-2022

$$(A^t_{n\times m})^{-1}®w_{n\times m} = (I_{n\times n} + A^t_{n\times m}D^{jk}_{m\times n})^{-1}(-A^t_{n\times m})®$$
$$(A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{jk}_{m\times n}M'_{n\times m})(mod\ p) =$$
$$= (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m}) + (A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{jk}_{m\times n}M'_{n\times m}) +$$
$$+(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m})R^{jk}_{m\times n}(A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{jk}_{m\times n}M'_{n\times m})(mod\ p) = (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m})(I_{m\times m} + R^{jk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M'_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m})R^{jk}_{m\times n}(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M'_{n\times m}(mod\ p)$$

The resulting embryo was allowed to develop in nutrients and then inserted into her womb, where it implanted. In the latter case, the presence of the IUD could prevent the fertilized egg's implanting in the lining of the womb. For such matrixes, this equation is appropriate:

$(A^t_{n\times m})^{\backslash -1}®w_{n\times m} = (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m})(I_{m\times m} + R^{jk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} + +(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M'_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(-A^t_{n\times m})R^{jk}_{m\times n}(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M'_{n\times m}(modp) = (-A^t_{n\times m})(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(I_{m\times m} + R^{jk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M'_{n\times m} + (-A^t_{n\times m})R^{jk}_{m\times n}(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})^{-1}(I_{n\times n} + A^t_{n\times m}R^{jk}_{m\times n})M_{n\times m}(modp) = -A^t_{n\times m} + A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{jk}_{m\times n}M'_{n\times m} - A^t_{n\times m}R^{jk}_{m\times n}M'_{n\times m}(modp) = M'_{n\times m}.$

Generally speaking, if these equation expressions are selected as commutative matrixes, the decrylash zhayoniny cylindrical cylinder can be performed in the cylinder. Boo on Earth

$M'_{n\times m}$=$M_{n\times m}||P_{n\times m}$ ва $P_{n\times m} = A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}(mod\ p)$=$A^j_{n\times m}®H = P$

To determine the correctness of an electronic digital signature, the following are the following:

4. Фақат - фойдаланувчининг ўзига маълум бўлган td_t - махфий калитдан фойдаланиб$(s_p)^{d_te_j}\ mod\ n = [(k^j_{1\ il})^{d_j}]^{e_td_te_j}\ mod\ n = k^j_{1\ il}$ аниқланиб$R^{jk_1}{}_{m\times n}$ -матрица элементлари олинади.

5. Очиқ - калитга параметрли тескари бўлган матрица ҳисобланади.$A^j_{n\times m}(A^j_{n\times m})^{-1} = (I_{n\times n} + A^j_{n\times m}D^{jk_1}_{m\times n})^{-1}(-A^{jk_1}_{n\times m})\ mod\ p$

6. Ушбу қийматни алмаштириш амалини бажариб, дешифрлаш амалга оширилади: $R = D^{jk_1}_{n\times m}$

$(A^j_{n\times m})^{-1}®w_{n\times m} = (I_{n\times n} + A^j_{n\times m}D^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})®(A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m})(mod\ p) = (I_{n\times n} + A^t_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^t_{n\times m})+(A^t_{n\times m} + H_{n\times m} + A^t_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}) + (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})R^{jk_1}_{m\times n}(A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m})(mod\ p) = (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})(I_{m\times m} + R^{jk_1}_{m\times n}A^j_{n\times m}) + A^j_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^t_{m\times n})H_{n\times m} + +(I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})R^{jk_1}_{m\times n}(I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})H_{n\times m}(mod\ p)$

Бу охирги тенглик ифодасидаги матрицаларнинг фақат диагонал элементларининг ҳаммаси ноль бўлмай, бошқа барча элементлари ноллардан иборат эканлигини (бундай матрицалар коммутативлик хоссасига эгалигини) ҳисобга олиб, матрицалар кўпайтмалари қатнашган ҳадларда улар ўринларини алмаштирилса ҳам тенглик ўзгармаслигидан фойдаланиб, ушбу тенгликка эга бўлинади:

$(A^j_{n\times m})^{-1}®w_{n\times m} = (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})(I_{m\times m} + R^{jk_1}_{m\times n}A^j_{n\times m}) + +A^j_{n\times m} + (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})H_{n\times m} + (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}\left(-A^j_{n\times m}\right)R^{jk_1}_{m\times n}(I_{n\times n} + A^t_{n\times m}R^t_{m\times n})H_{n\times m}(modp) = (-A^j_{n\times m})(I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(I_{m\times m} + R^{jk_1}_{m\times n}A^j_{n\times m}) + A^j_{n\times m} + (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})H_{n\times m} + (-A^j_{n\times m})R^{jk_1}_{m\times n}(I_{n\times n} + A^{jt}_{n\times m}R^{jk_1}_{m\times n})^{-1}(I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})H_{n\times m}(modp) = -A^j_{n\times m} + A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}H_{n\times m} + A^j_{n\times m}R^{jk_1}_{n\times m}H_{n\times m} - A^t_{n\times m}R^t_{m\times n}H_{n\times m}(mod\ p) = H_{n\times m}.$

7. t-фойдаланувчининг $C_{n\times m}$- шифрланган маълумотни дешифрлаши натижасида ҳосил бўлган $M'_1 = M_1||P_1$ кенгайтрилган хужжатнинг M_1 қисми хешланади : $H(M_1) = H(M_{1_{n\times m}}) = H_1$

8. $H_1 = H(M_{1_{n\times m}}) = H_{n\times m} = H$ Electron khuzhzhat butun (ҳаqiyqiyi) ҳisoblanadi ҳamda uning electron raqamli imzosi ҳaqiyiligidan manbaasining ҳam ҳaqiyiiligi kelib chikadi.

ISSN NO: 2770-0003
Date of Publication: 17-04-2022

In addition to the signer's liquid key, the proposed EDS algorithm used a parameter that would be selected by the signer. Therefore, this EDS algorithmi has such properties as EDS algorithms based on the formation and validation of a specially developed (created) digital signature.

Шифрлаш алгоритми ва ЭРИ протоколлари алгоритмларидаги *M* -маълумот ўрнига калит ҳақидаги маълумотни қўйиб ахборот-коммуникация тармоғи фойдаланувчиларга улар маҳфий калитларини очиқ алоқа каналида тарқатишни амалга ошириш мумкин [1-3].

Адабиётлар

1. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. Osnovy cryptography: Uchebnoe posobie, 2-e ed. –M.: Helios ARV, 2002.-480 p.
2. Schneier B. Applied cryptography. Protocols, algorithms, source texts in the language of C. –M.: PUBLISHING HOUSE TRIUMPH, 2003 - 816 p.
3. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, “Ўзбекистон маркаси”, 2009 – 434 бет.
4. Khasanov P.F., Akbarov D. E., Akhmadliev Sh. Sh. Methods of creating new asymmetric algorithms based on subject-shaped complexes using parameter algebra actions. / Infocommunications: Networks-Technologies-Solutions. -1(9)/2009. -p. 31-35.