

PARAMETRLI NOSIMMETRIK RSA SHIFRLASH ALGORITMINI GENERATSIYA QILISH DASTURI

Qarshiboyev Nizomiddin Abdumalik o'g'li

Jizzax politexnika instituti "ICHJA va B" kafedrası, v.b., dotsent

Email: wolkswagen1991@gmail.com

Annotatsiya: Ushbu dasturiy ta'minotni yaratishda zamonaviy dasturiy vositalari (muhitini) dan foydalanib yaratish, ularning imkoniyatlaridan foydalanish va dasturiy vositalarning universalligi, soddaligi va tarmoqda ishlay oladigan tomonlari o'rganilgan. Microsoft Visual Studio 2008 dasturi Microsoft korporatsiyasi tomonidan ishlab chiqilgan bo'lib, bu dastur dasturchilar uchun mo'ljallangandir.

Kalit so'zlar: Microsoft korporatsiyasi, Microsoft Visual Studio 2008 muhiti, Visual C#, Visual Basic, Visual J# tillari, Web dasturlar, Visual C#, Visual Basic, Visual J#, Visual C++, Windows muhiti, dastur.

Аннотация: При создании данного программного обеспечения изучались создание с использованием современных программных средств (среды), использование их возможностей, универсальность, простота и возможность работы в сети. Microsoft Visual Studio 2008 разработан корпорацией Microsoft и предназначен для разработчиков.

Ключевые слова: корпорация Microsoft, среда Microsoft Visual Studio 2008, Visual C#, Visual Basic, языки Visual J#, веб-приложения, Visual C#, Visual Basic, Visual J#, Visual C++, среда Windows, программа.

Abstract: In the creation of this software, creation using modern software tools (environment), use of their capabilities, universality, simplicity of software tools, and aspects of being able to work on the network were studied. Microsoft Visual Studio 2008 was developed by Microsoft Corporation and is intended for developers.

Keywords: Microsoft Corporation, Microsoft Visual Studio 2008 environment, Visual C#, Visual Basic, Visual J# languages, Web applications, Visual C#, Visual Basic, Visual J#, Visual C++, Windows environment, program.

Microsoft Visual Studio 2008 dasturi yordamida Windows muhiti uchun, telefonlar uchun, tarmoqlar uchun, Web dasturlarni yaratish mumkin. Microsoft Visual Studio 2008 muhitida Visual C#, Visual Basic, Visual J# tillari yordamida Web dasturlarni va Visual C#, Visual Basic, Visual J#, Visual C++ tillari yordamida Windows muhiti uchun dasturlar yaratish mumkin.

C# dasturlash tilining afzallik taraflari shundaki, bu dasturlash tilida juda ko'plab kutubxonalar bor. Bu kutubxonalar dasturchi uchun qulaylik tug'diribgina qolmasdan,

kam hato qilishga olib keladi. C# dasturlash .NET Freamwork kutubxonalarini bilan ishlaydi. [5]

Biz dastur tuzishda C# dasturlash tilidan foydalandik. Bu dastur Visual Studio umumiy paketiga kiradi. Hamda Microsoft firmasi tomonidan ishlab chiqilgan. Shuning bilan bu dastur faqat Microsoft, Macintosh operatsion muhitlarida ishlaydi. Bu dastur ishlashi uchun bir talay qo‘shimcha dasturlar kerak bo‘ladi.

Parametrlar algebrasi asosida takomillashtirilgan El-Gamal shifrlash algoritmining dasturi quyida keltirilgan.

Dasturda oshkora p , a parametrlar, e_i , d_j maxfiy kalitlar, aloqa kanalidagi i -, j -tomonlarning maxfiy kalitlari va r_{ij} – aloqa kanalida i -, j -tomonlarning parametr sifatida foydalanadigan o‘zaro maxfiy yoki oshkora kaliti hamda k_i , k_j – aloqa kanalida i -, j -tomonlarning mos tarzda har aloqa seansida tasodifiy son sifatida tanlanadigan maxfiy seans kalitlari generatsiya qilinadi. [6]

Dastur quyidagi bandlardan iborat:

1. Kalit generatori bandi. Ushbu bandda RSA shifrlash algoritmi uchun kerakli bo‘lgan kalitlar avtomatik ravishda hosil qilinadi.

The screenshot shows a software window titled "Parametrlar El-Gamal" with a blue background. It contains several sections for parameter input and generation:

- Section 1:**
 - P (256 bit): 893401566039117783577248357787852304171966778462172456511767647
 - a (192 bit): 3963223657804864027350334027097389671053481075539860454153
 - Buttons: AutGen
- Section 2:**
 - $e(i)$ (192 bit): 4927291207159112435302415170012031098199413942306469299649
 - $d(j)$ (192 bit): 6230925012475601809077044765187007667592477440789913260621
 - Buttons: AutGen
- Section 3:**
 - $r(i)$ (8 bit): 149
 - $r(j)$ (8 bit): 191
 - $r(ij)=r(i)+r(j)(\text{mod } P)$: 340
 - Buttons: AutGen
- Section 4:**
 - $k(i)$ (192 bit): 4669649089170314669719493387409347321587511142352172475047
 - $k(j)$ (192 bit): 498352925252045397769772761903684407392971671280275999123
 - Buttons: AutGen
- Section 5:**
 - $y(i)$: 770538685754528181775054268447130116565859084857098551253933017
 - $y(j)$: 386641130800324976575793400338458752344953617134908939405397138
 - Buttons: Calculate
- Section 6:**
 - Matn: [Text input field]
 - S (1): [Text input field]
 - S (2): [Text input field]
 - Dastlabki matn: [Text input field]
 - Buttons: Encryption, Decryption

1-rasm. Kalit generatsiyasi

2. Axborotni shifrlash jarayoni bandi. Ushbu bandda yaratilgan kalitlar asosida kiritilgan matnni shifrlash amalga oshiriladi. Misol uchun yaratilgan kalitlar bilan “Mumunova Mastura Maxmudjon qizi” matnini shifrlaymiz. Oynada axborotning shifr matni hosil bo‘ladi.

The screenshot shows a software application window titled "Parametrlil_EL_Gamal". It contains several sections for generating encryption parameters and performing encryption:

- Shifrlash parametrlari:** Fields for P (256 bit) and a (192 bit) with an "AutGen" button.
- Tasdiq kalitlari:** Fields for e (i) (192 bit) and d (j) (192 bit) with an "AutGen" button.
- Algoritm kanallari tomonidan modifikatsiya:** Fields for r (i) (8 bit) and r (j) (8 bit), with a calculated value for r (i)=r(i)+r(j)(modP) shown as 340. Includes an "AutGen" button.
- Modifikatsiya kalitlari:** Fields for k (i) (192 bit) and k (j) (192 bit) with an "AutGen" button.
- Tasdiqlash bosqichi:** Fields for y (i) and y (j) with a "Calculate" button.
- Shifrlash bosqichi (Shifrlash va Dastlabki):** A text input for "Matn" containing "Mumunova Mastura Maxmudjon qizi", and fields for S (1) and S (2). Includes "Encryption" and "Decryption" buttons.

2-rasm. Axborotni shifrlash jarayoni

3. Axborotning shifrini ochish jarayoni bandi. Ushbu bandda hosil qilingan shifr matnni ochiq matnga aylantirish masalasi ko‘rib chiqiladi. Buning uchun *Shifrnı ochish tugmasi bosiladi va dastur* oynasida ochiq matn “Mumunova Mastura Maxmudjon qizi” hosil bo‘ladi.

Parametrlari_El_Gamal

Dinamik parametrlar

P (256 bit) 893401566039117783577248357787852304171966778462172456511767647 AutGen

a (192 bit) 3963223657804864027350334027097389671053481075539860454153

Maxfiy kalitlar

e (i) (192 bit) 4927291207159112435302415170012031098199413942306469299649 AutGen

d (j) (192 bit) 6230925012475601809077044765187007667592477440789913260621

Sodda tanaladigan funktsioning maxfiy kalitlar

r (i) (8 bit) 149

r (j) (8 bit) 191 AutGen

r (ij)=r(i)+r(j)(modP) 340

Maxfiy sifir kalitlar

k (i) (192 bit) 4669649089170314669719493387409347321587511142352172475047 AutGen

k (j) (192 bit) 4983529252520453977769772761903684407392971671280275999123

Tashvily boqich

y (i) 770538685754528181775054268447130116565859084857098551253933017

y (j) 386641130800324976575793400338458752344953617134908939405397138 Calculate

Sifir boqich (Shifrlash va Dasturlash)

Matn Mumunova Mastura Maxmudjon qizi Encryption

S (1) 245931128439399450270697702578110848309856100546998727959688473

S (2) 320787183659211540926022263040989010863265145013684459786154898

Dastlabki matn Mumunova Mastura Maxmudjon qizi Decryption

3-rasm. Axborotning shifrini ochish jarayoni

Ishlab chiqilgan nosimmetrik shifrlash algoritmi qo‘shimcha maxfiylik sifatida R parametri kiritilishi hisoblash murakkabligi ortadi. Bu esa ishlab chiqilgan algoritmlarning bardoshligi yuqoriligidan dalolat beradi.

Xulosa: Ishlab chiqilgan takomillashtirigan shifrlash algoritmidan va dasturidan O‘zbekiston Respublikasida shakllanayotgan elektron hukumat tizimida ma’lumotlar bazalarini va axborot-kommunikatsiya tarmoqlari orqali uzatiladigan ma’lumotlarni konfidentsialligini ta’minlash jarayonida foydalanilish xavfsizlikni yuqori darajada ta’minlash uchun imkon yaratadi.

Foydalanilgan adabiyotlar ro'yxati:

1. Shlixt G.Yu. Tsifrovaya obrabotka tsvetno'x izobrajeniy. - M., Izdatelstvo EKOM, 1997. - 336 s.
2. Yane, B. Tsifrovaya obrabotka izobrajeniy G' B. Yane: per. s angl. pod red. A.M. Izmaylovoy. M.: Texnosfera, 2007 - 584s.-ISBN 978-5-94836122-2
3. [Kravchenko V.F.](#) Tsifrovaya obrabotka signalov i izobrajeniy. - M.: [FIZMATLIT](#), 2007 g.
4. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). IMAGE CONTOUR SEPARATION ALGORITHMS BASED ON THE THEORY OF FUZZY SETS. *International Journal of Contemporary Scientific and Technical Research*, 120-125.
5. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). TASVIRLARDAN MA'LUMOT OLIISHDA MATLAB MUHITINING INTELLEKTUAL TASHKIL ETUVCHILARIDAN FOYDALANISH. *International Journal of Contemporary Scientific and Technical Research*, 247-250.
6. Akhbutayevich, T. S., & Abdumalikovich, K. N. (2022). Algorithms for Selecting the Contour Lines of Images Based on the Theory of Fuzzy Sets. *Texas Journal of Engineering and Technology*, 15, 31-40.
7. Savurbaev, A., Dangalov, N.A., Shertoylov, G.M., & Eshonkulov, Sh.U. (2014). Algoritm rascheta perexodnogo protsessa pri udare tsilindricheskogo koltsa o jestkoe poluprostranstvo. *Molodoy ucheno'y*, (8), 246-250.
8. Eshonkulov, Sh., Burliev, A., & Eshonkulova, Sh. (2019). Nauchno-metodicheskiy podxod k sozdaniyu elektronnoy uchebnika.
9. Savurbaev, A., Muxammadiev, M.T., Eshankulov, Sh.U., & Guliev, A.A. (2015). Kosoy udar tsilindricheskogo koltsa o jestkoe poluprostranstvo. *Molodoy ucheno'y*, (1), 97-102.