**Բովանդակություն**

**Ներածություն……………………………………………………………………………...........5**

**Խնդրի դրվածքը………………………………………………………………………………....**7

**1. Գլուխ 1: Օգտագործվող գործիքամիջոցների և միջավայրի նկարագրությունը**

**1.1 ASP.Net Core միջավայրի նկարագրությունը..................................................................8**

**1.2 .Net Framework – ի նկարագրությունը...............................................................................9**

**1.3 C# լեզվի նկարագրությունը..............................................................................................12**

**1.4 Microsoft SQL Server.............................................................................................................13**

1.4.1 Ֆունկցիոնալություն..........................................................................................................15

1.4.2 Ծրագրերի մշակում...........................................................................................................17

**1.5 AES:ալգորիթմի նկարագրությունը.................................................................................19**

1.5.1 Գաղտնագրում....................................................................................................................21

1.5.2 Բանալիների ստացում......................................................................................................24

1.5.3 Գաղտնավերծանում..........................................................................................................25

**1.6 RC4 ալգորիթմի նկարագրությունը..................................................................................28**

**2. Գլուխ 2 Համակարգի աշխատանքի և ալգորիթմի նկարագրությունը**

2.1 Նույնականացում..................................................................................................................31

2.2 Գրանցում համակարգում....................................................................................................32

2.3 Լոկալ գաղտնագրում և վերծանում..................................................................................35

2.4 Բաց կապուղիով ֆայլերի անվտանգ փոխանակումը...................................................36

2.5 Գաղտնագրված ամպային տարածք.................................................................................38

2.6 Հիշեցումներ............................................................................................................................38

**Եզրակացություն........................................................................................................................39**

**3 . Գլուխ 3: Ճյուղային տնտեսագիտություն........................................................................40**

**4. Գլուխ 4: Բնապահպանություն..........................................................................................44**

**5. Գլուխ 5: Կենսագործնեության անվտանգություն.....................................................................49**

**Գրականություն ցանկ...............................................................................................................54**

**Ներածություն**

Գաղտնագրության համակարգի իմաստն այն է, որ գաղտնի տեղեկատվությունը քողարկվի այնպես, որ այն անմատչելի լինի անիրավասու անձանց: Անկախ այն բանից, պահպանված է տեղեկատվությունը համակարգչի մեջ, թե հաղորդվում է համացանցի միջոցով, այն ապահովում է այն, որ ոչ իրավասու անձինք չեն կարող հասկանալ տեղեկատվության բովանդակությունը: Գաղտնահամակարգերը կարողեն լինել համաչափ կամ անհամաչափ ։ Իրենց հերթին տարբերակվում է նաև հոսքային կամ հատվածային ալգորիթմեր:

**Հոսքային** գաղտնագրի դեպքում տեքստը գաղտնագրվում է առանձին տառերով կամ բիտերով։ Յուրաքանչյուր տարրի (տառի կամ բիտի) գաղտնագրման կանոնը որոշվում է հաղորդագրության մեջ նրա դիրքով։

Հոսքային գաղտնագրերը ի տարբերություն հատվածայինի պարզ ու արագ են։ Բացի դրանից եթե ստացված հաղորդագրության ինչ֊որ հատվածում 1 բիթ սխալ է ստացվել, դա չի ազդի հաղորդագրութան մյուս հատվածների ճիշտ վերծանման վրա։

Սա հարմար է օրինակ բջջային կապի գաղտնագրման ժամանակ։

**Հատվածային** գաղտնագրի դեպքում երկուական հաջորդականությունը բաժանվում է տրված չափով հատվածների, և յուրաքանչյուր հատված գաղտնագրվում է առանձին։

Գաղտնակայուն հատվածային գաղտնագրերը օժտված են այս հատկություններով՝

• **Դիֆուզիա**՝ տեքստի նույնիսկ 1 բիթի փոփոխությունը պետք է առաջացնի

անկանխատեսելի փոփոխություններ գաղտնագրված տեքստում։

• **Անկարգայնություն**՝ հատարկման ժամանակ հակառակորդը չպետք է հասկանա, որ գտնվում է ճիշտ բանալու կողքին։

• **Ամբողջականություն**` գաղտնագրված տեքստի յուրաքանչյուր նիշ պետք է

կախված լինի բանալու յուրաքանչյուր նիշից։

Հատվածային գաղտնագրերը ի տարբերություն հոսքայինի ավելի գաղտնակայուն են։

Հաշվի առնելով գաղտնահամակարգերի առավելությունները և թերությունները մշակվեց հետևայլ համակարգը, որտեղ առկա են և հոսքային և հատվածային ալգորիթմեր:

**Ամպային տեխնոլոգիաները** կամ ամպային գործողությունները (Cloud Computing) ՏՏ ծառայությունների մատուցման նոր մոդելներ են, որոնք համացանցի միջոցով տրամադրում են դինամիկ, մասշտաբային և վիրտուալ ռեսուրսներ։ Այս դեպքում տեղեկատվությունը մշտապես պահպանվում է համաշխարհային ցանցի սերվերներում։ Այն հարմար միջավայր է ինֆորմացիայի պահպանման և մշակման համար,և որի օգնությամբ համացանցի միջոցով պահանջի դեպքում համակարգիչներին և այլ սարքերին (օրինակ` սմարտֆոններ) տրամադրվում են ընդհանուր ռեսուրսներ (shared resources), լիցենզավորված ծրագրային ապահովում և տեղեկատվություն:

Ամպը կլասիկ սերվերներից տարբերվում է նրանով, որ իր ռեսուրսներն օգտագործում է որպես գլոբալ վիրտուալ համակարգիչ, որտեղ ծրագրերն աշխատում են անկախ համակարգչից և իր կոնֆիգուրացիաներից:

Ամպային տեխնոլոգիայի առանձնահատկությունը կայանում է նրանում, որ այն կախված չէ ապարատային հարթակից: Օգտագործողը կարող է օգտվել ամպային ծառայություններից աշխարհի ցանկացած վայրից և ցանկացած սարքից, որն ունի ինտերնետի հասանելիություն:

Բացի վերը նշվածից, նկատվել է ՏՏ ենթակառուցվածքի սպասարկման ծախսերի զգալի նվազեցում: Ու եթե չես ալարել կարդալ, ու հասել ես ստեղ, ժպտա, գնա շոկոլադ կեր ու հանգստացի: Ներածությունը շտապ չի: Չկա անհրաժեշտություն ձեռք բերել թանկարժեք սերվերային սարքավորումներ, ներդնել անխափան աշխատանքն ապահովող համակարգեր, և այլն:

Ամպային տեխնոլոգիաների այլ առավելություններից են հանդիսանում ծառայությունների ներդրման ժամկետների զգալի կրճատումը:

Ամպային տեխնոլոգիաները հարմար միջոց են տվյալների պահպանման և տեղափոխման համար: Սակայն ամպային համակարգերի ստեղծման օրվանից քննարկվում է տվյալների անվտանգության հարցը:

**Խնդրի դրվածք**

**Գլուխ 1**

**Օգտագործվող գործիքամիջոցների և միջավայրի նկարագրությունը**

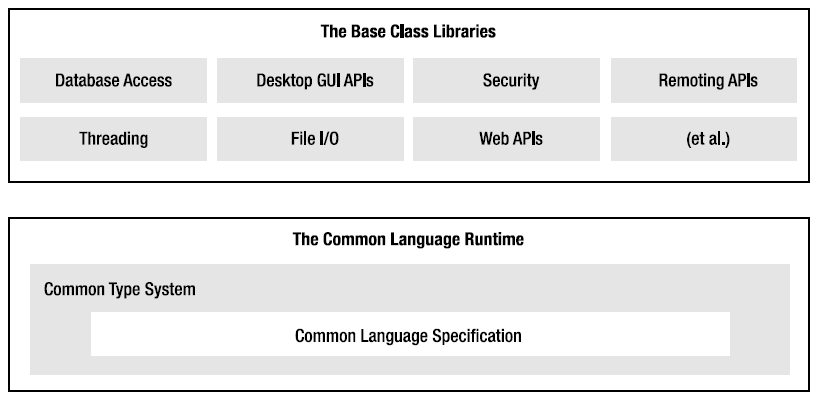
**1.1 ASP.Net Core միջավայրի նկարագրությունը**

**1.2 .Net Framework – ի նկարագրությունը**

.NET հենքը ստեղծված է աջակցելու բարդ և խիստ բաշխված կոմպոնենտային ծրագրերի նախագծման և աշխատեցման պրոցեսներին: Նա հնարավորություն է տալիս համատեղ օգտագործել տարբեր ծրագրային լեզուներ, ինչպես նաև ապահովում է ծրագրերի անվտանգությունը, տեղափոխելիությունը և Windows ՕՀ-ի ծրագրավորման ընդհանուր մոդելը: Ծրագրավորողի տեսանկյունից .NET-ը իրենից ներկայացնում է կատարող միջավայր և բազային տիպերի ահռելի գրադարան: Կատարման միջավայրի մակարդակը կոչվում է լեզուների համընդհանուր կատարման միջավայր (Common Language Runtime-CLR): Այս համակարգը կառավարում է ծրագրերի կատարումը: CLR-ը հանդիսանալով .NET-ի բաղադրիչ մաս, ապահովում է բազմալեզու ծրագրավորում, ինչպես նաև ծրագրերի տեղափոխելիությունը և անվտանգ կատարումը: CLR-ի հիմնական խնդիրը դա .NET-ի տիպերի ավտոմատ հայտնաբերման, բեռնման և կառավարման գործընթացն է(ծրագրավորողի փոխարեն): CLR-ը նաև զբաղվում է մի շարք ցածր մակարդակի խնդիրներով, ինչպիսիք են` հիշողության կառավարումը, ծրագրի սպասարկումը, հոսքերի վերամշակմամբ և անվտանգության հետ կապված զանազան ստուգներով: .NET-ի մյուս բաղադրիչը դա ընդհանուր տիպերի համակարգն է(Common Type System) կամ կրճատ` CTS համակարգ: CTS-ի հատկորոշման մեջ ներկայացված է բոլոր հնարավոր տիպերի և ծրագրային կառուցվածքների ամբողջ նկարագարությունը, որոնց աջակցում է կատարող միջավայրը, այն, թե ինչպես են այդ էությունները միմյանց հետ համագործակցում, և այն, թե ինչպես կարող են նրանք հանդես գալ որպես .NET-ի մետատվյալ:

Կարևոր է հասկանալ , որ CTS- ում ցանկացած որոշված ֆունկցիա կարող է չաջակցվել .NET-ի որոշակի լեզուների հետ: Դրա համար գոյություն ունի համընդհանուր լեզուների հատկորոշում (Common Language Specifiaction) կամ կրճատ` CLS հատկորոշում, որում նկարագրված է միայն այն ընդհանուր տիպերի ենթաբազմությունը և ծրագրային կառուցվածքները, որոնց կարող են աջակցել .NET –ի ծրագրավորման բոլոր լեզուները:

Ուստի .NET –ի միայն ֆունկցիոնալ հատկություններով տիպեր կառուցելու դեպքում, որոնք դիտարկված են CLS-ում, կարելի է լիովին վստահ լինել նրանում , որ .NET–ի հետ համատեղելի բոլոր լեզուները կարող են դրանք օգտագործել:Եվ հակառակը` CLS-ում չգտնվող որևէ տիպի տվյալների կամ ծրագրավորման կառուցվածքների օգտագործման դեպքում չի կարելի կարծել, որ .NET–ի հետ համատեղելի բոլոր լեզուները կարող են դրանք օգտագործել:

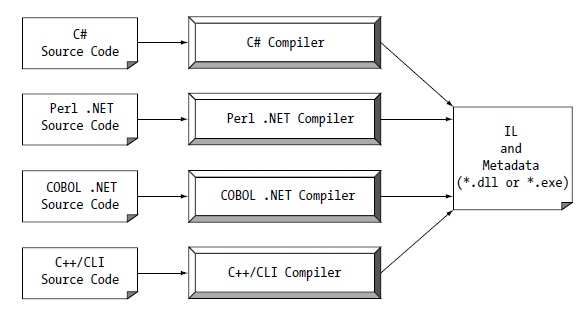


*CLR-ի, CTS-ի, CLS-ի և հենքի բազային դասերի գրադարանների միջև հարաբերությունը*

.NET-ի ծրագրավորման լեզուներից յուր­­­աքանչյուրն ընտրելիս, կարևոր է հիշել, որ .NET-ի երկուական կոդերի ֆայլերը ունեն նույն ընդլայնումները ինչ որ Win32-ի չկառավարվող ծրագրերի ֆայլերը(\* . dll կամ \* . ехе), բայց նրանց ներքին

կառուցվածքը տարբեր է: .NET-ի երկուական կոդերի ֆայլերը պարունակում են ոչ թե հատկորոշիչ տվյալներ այլ ընդհակառակը` հենքից անկախ տվյալներ, միջանկյալ

լեզվով(Intermediat Language -IL), ինչպես նաև տիպերի մետատվյալներ:



*Բոլոր .NET կոմպիլիատորները գեներացնում են IL կոդ և մետատվյալներ*

.NET-ի կոմպիլյատորի միջոցով \*.dll կամ \*.exe ֆայլ ստեղծելիս, ստացվում է մեծ երկուական օբյեկտ, որը կոչվում է հավաքածու (assembley): Այդ հավաքածուի մեջ է գտնվում CIL կոդը, որը հիմնովին նման է Java-ի բայթ կոդին նրանով, որ չի թարգմանվում հենքին հատուկ կոդի, մինչև չի լինում դրա անհրաժեշտությունը: Սովորաբար անհրաժեշտությունը լինում է, երբ CIL-կանոնների մի մասը դիմում է ֆունկցիայի, որը գտնվում է .NET-ի կատարող միջավայրում:

**1.3 C# լեզվի նկարագրությունը**

Քանի որ .NET-ը այդքան տարբերվում է իրեն նախորդող տեխնոլոգիաներից, Microsoft-ում ստեղծեցին հատուկ հենքի տակ աշխատող նոր ծրագրավորման լեզու` C#: C#-ը հանդիսանում է C ծրագրավորման լեզվի ընտանիքի անդամ դրա համար է, որ ունեն նման սինտակսիս:

Սինտակսիսի տեսանկյունից C#-ը հանդիսանում է մի քանի լեզվից ստեղծված գործնականում հզոր միջավայր, ինչպես C++-ը: Թվարկենք C# լեզվի մի քանի հատկություն՝

* Ցուցիչների կիրառման կարիք չկա: C# լեզվով գրված ծրագրերում սովորաբար ցուցիչներ կիրառելու պահանջ չի լինում (չնայած լեզուն հնարավորություն տալիս է օգտագործել ցուցիչներ):
* Հիշողության կառավարումը իրականացվում է ավտոմատ, այսպես կոչված` աղբ հավաքողի կողմից, դրա համար C#-ում չի կիրառվում delete հանգույցային բառը:
* Տրամադրվում են ֆորմալ սինտակսիսային կառուցվածքային տիպերի, ինտերֆեյսների, ստրուկտուրաների, թվարկությունների և դելեգատների համար:

.NET-ի տվյալ թողարկման մեջ C# լեզուն թարմացվել է, և օժտված է մի շարք նորություններով, որոնցից կարևորները թվարկված են ստորև`

* Ոչ անհրաժեշտ պարամետրերի հնարավորություն, ինչպես նաև անունով արգումենտներ:
* Անդամների դինամիկ որոնման հնարավորություն կատարման ընթացքում, dynamic բանալիային բառի միջոցով:
* Ընդհանրացված տիպերի հետ աշխատանքը բավականին հեշտացել է, ի շնորհիվ տվյալների հեշտ արտապատկերմա:

C#-ով ծրագրավորման ժամանակ կարելի է ստեղծել միայն այնպիսի կոդ, որը կթարգմանվի միայն .NET-ի միջավայրում:

**1.4 Microsoft SQL Server**

Microsoft SQL Server, ռելացիոն տվյալների բազաների կառավարման համակարգ ([DBMS](http://hy.wikipedia.org/w/index.php?title=DBMS&action=edit&redlink=1))` մշակված [Microsoft](http://hy.wikipedia.org/wiki/Microsoft) կորպորացիայի կողմից: Հարցումների օգտագործվող հիմնական լեզուն [Transact-SQL](http://hy.wikipedia.org/w/index.php?title=Transact-SQL&action=edit&redlink=1) է, որը ստեղծվել է համատեղ` Microsoft-ի և Sybase-ի կողմից։ Transact-SQL-ը հանդիսանում է ANSI/ISO ստանդարտի իրագործումը՝ ըստ հարցումների ենթակառուցվածքային լեզվի (SQL) ընդլայնումների։ Օգտագործվում է անհատականից մինչև հսկա կազմակերպությունների տվյալների բազաների հետ աշխատանքների համար, այն մրցակցում է շուկայի տվյալ սեգմենտում այլ ռելացիոն տվյալների բազաների կառավարման համակարգերի հետ։

**Պատմությունը**

MS SQL Server-ի ելակետային կոդը (մինչ 7.0 տարբերակը) հիմնվում էր [Sybase SQL Server](http://hy.wikipedia.org/w/index.php?title=Sybase_SQL_Server&action=edit&redlink=1) կոդի վրա, և դա թույլ տվեց Microsoft-ին՝ դուրս գալ կազմակերպությունների տվյալների բազայի շուկա, որտեղ այդ ժամանակ մրցակցում էին [Oracle](http://hy.wikipedia.org/w/index.php?title=Oracle&action=edit&redlink=1), [IBM](http://hy.wikipedia.org/wiki/IBM), իսկ ավելի ուշ ինքը՝ [Sybase](http://hy.wikipedia.org/w/index.php?title=Sybase&action=edit&redlink=1)-ը։ Microsoft-ը, [Sybase](http://hy.wikipedia.org/w/index.php?title=Sybase&action=edit&redlink=1)-ը և [Ashton-Tate](http://hy.wikipedia.org/w/index.php?title=Ashton-Tate&action=edit&redlink=1)-ը ի սկզբանե միավորվեցին՝ մի ծրագրի ստեղծման և շուկա բացթողնման համար, որը ստացավ [SQL Server 1.0](http://hy.wikipedia.org/w/index.php?title=SQL_Server_1.0&action=edit&redlink=1) OS/2 -ի համար անվանումը ([1989](http://hy.wikipedia.org/wiki/1989) թ.), որը փաստացի համարժեքն էր Sybase SQL Server 3.0 Unix, VMS-ի և այլնի համար։ Microsoft SQL Server 4.2-ը թողարկվել է 1992թվականին և գտնվում էր Microsoft OS/2 1.3 տարբերակի օպերացիոն համակարգի կազմում։ Microsoft SQL Server Windows NT օպերացիոն համակարգի համար 4.21 տարբերակի պաշտոնական հրապարակումը տեղի ունեցավ հենց [Windows NT](http://hy.wikipedia.org/w/index.php?title=Windows_NT&action=edit&redlink=1)-ի (տարբերակ 3.1) պաշտոնական հրապարակման (հանրայնացման) հետ միաժամանակ։

[Microsoft SQL Server 6.0](http://hy.wikipedia.org/w/index.php?title=Microsoft_SQL_Server_6.0&action=edit&redlink=1)-ը առաջին [SQL Server](http://hy.wikipedia.org/w/index.php?title=SQL_Server&action=edit&redlink=1)-ի տարբերակն էր, որը ստեղծված էր բացառապես Windows NT-ի ճարտարապետության համար և առանց մշակման գործընթացում Sybase-ի մասնակցության։

Այն ժամանակ, երբ շուկա դուրս եկավ Windows NT օպերացիոն համակարգը, [Sybase](http://hy.wikipedia.org/w/index.php?title=Sybase&action=edit&redlink=1)-ն ու Microsoft-ը բաժանվեցել էին և հետևում էին ծրագրային արտադրանքի սեփական մոդելներին և մարքեթինգային սխեմաներին։ Microsoft-ը ձգտում էր Windows-ի համար SQL Server-ների բոլոր տարբերակների գծով բացառիկ իրավունքի ձեռքբերմանը։ Ավելի ուշ, Sybase-ը փոխեց իր արտադրանքի անվանումը և անվանեց այն Adaptive Server Enterprise, խուսափելու համար Microsoft SQL Server-ի հետ շփոթելի լինելուց։ Մինչև 1994 թվականը Microsoft-ն արդեն ստացել էր երեք ծանուցում Sybase-ից՝ որպես ակնարկ Microsoft SQL Server-ի ծագման մասին։

Բաժանվելուց հետո ընկերությունները թողարկեցին մի քանի ինքնուրույն ծրագրեր։ SQL Server 7.0-ը դարձավ տվյալների բազայի առաջին սերվերը, որն օժտված էր օգտագործողի համար կառավարման իսկական գրաֆիկական ինտերֆեյսով։ Sybase-ի կողմից հեղինակային իրավունքի պահանջներից խուսափելու նպատակով 7-րդ տարբերակի ողջ ժառանգվող կոդը վերագրվեց։  
SQL Server 2005 տարբերակը ներկայացվել է 2005 թվականի նոյեմբերին։ Տարբերակի թողարկումն իրականացվում էր Visual Studio 2005-ի թողարկման հետ զուգահեռ։ Գոյություն ունի նաև Microsoft SQL Server-ի կրճատված տարբերակը՝ Microsoft SQL Server Express։ Այն հասանելի է բեռնման համար և կարող է անվճար տարածվել այն օգտագործող ծրագրային ապահովման հետ մեկտեղ։

SQL Server (SQL Server 2000)-ի նախորդ տարբերակի թողարկման պահից իրականացվում էին աշխատանքներ՝ մշակման ինտեգրացված ոլորտի և SQL Server 2005-ի կազմ մտնող մի շարք լրացուցիչ ենթահամակարգերի զարգացման ուղղությամբ։ Փոփոխություններից անմասն չմնացին նաև ETL (Տվյալների դուրսբերում, ձևափոխում և բեռնում) տեխնոլոգիայի իրացումը, որը մտնում էր SQL Server Integration Services (SSIS)-ի կազմի մեջ, ծանուցման սերվերը, տվյալների բազմաչափ մոդելների մշակման վերլուծական միջոցները (OLAP)-ը և անհրաժեշտ տեղեկատվության հավաքագրումը (երկու ծառայություններն էլ մտնում են Microsoft Analysis Services կազմի մեջ), ինչպես նաև մի քանի հաղորդագրության ծառայություններ, մասնավորապես՝ Service Broker և Notification Services։

Բացի այդ կատարվում էին աշխատանքներ նաև արտադրողականության բարելավման ուղղությամբ։

**1.4.1 Ֆունկցիոնալություն**

Տվյալների բազաների սերվերը Microsoft SQL Server որպես լեզվի հարցումներ օգտագործում է SQL լեզվի տարբերակը, որը ստացել է Transact-SQL (կրճատ T-SQL)։ T-SQL լեզուն [SQL-92](http://hy.wikipedia.org/w/index.php?title=SQL-92&action=edit&redlink=1)-ի (ISO ստանդարտ SQL լեզվի համար) իրականացումն է մի քանի ընդլայնումներով։ Պահվող պրոցեդուրաների համար T-SQL-ը թույլ է տալիս օգտագործել լրացուցիչ սինտաքսիս և ապահովում է գործարքի աջակցություն (կառավարման ծրագրով տվյալների բազաների փոխգործակցում)։

Microsoft SQL Server և Sybase ASE ցանցերի փոխգործակցության ժամանակ օգտագործվում է Tabular Data Stream (TDS, աղյուսակային տվյալների փոխանցման արձանագրություն) ծրագրային մակարդակի արձանագրություն։

TDS արձանագրությունը նույնպես իրականացվել է FreeTDS նախագծում, որպիսի տարբեր ծրագրերին տալ հնարավորություն փոխգործակցել Microsoft SQL Server և Sybase տվյալների բազաների հետ։

Տվյալներին մուտք ապահովելու համար Microsoft SQL Server-ը ապահովում է Open Database Connectivity (ODBC) – ծրագրերի փոխգործակվման ինտերֆեյս ՌՏԲԿՀ-ի հետ (Ռելացիոն տվյալների բազաների կառավարման համակարգ)։

SQL Server 2005 տարբերակը ապահովում է օգտագործողների վեբ-ծառայությունների միջոցով միացում՝ օգտագործելով SOAP արձանագրություն։ Այն թույլ է տալիս օգտագործողների ծրագրերին քրոսհարթակային կապով միանալ SQL Server-ին, նույնիսկ եթե ծրագրերը նախատեսված չեն Windows օպերացիոն համակարգի վրա։ Microsoft նույնպես թողարկել է հավաստագրված JDBC դրայվեր, որը թույլ է տալիս JAVA պլատֆորմի վրա աշխատող ծրագրերին (ինչպիսիք BEA и IBM WebSphere) կապվել Microsoft SQL Server-ին։

SQL Server-ը ապահովում է տվյալների բազաների հայլեացում և կլաստերզացիա։ SQL սերվերի կլաստերը նույն կոնֆիգուրացիա ունեցող սերվերների հավաքածու է. այդպիսի սխեման օգնում է աշխատանքի ծանրաբեռնվածությունը բաշխել մի քանի սերվերների միջև։ Բոլոր սերվերները ունեն միևնույն վիրտուալ անունը և տվյալները բաշխվում են կլաստերի IP հասցեների օգնությամբ, աշխատանքի փուլի ընթացքում։ Բացի այդ, մի սերվերի կլաստերի խափանման կամ անսարքության դեպքում հնարավոր է ծանրաբեռնման ավտոմատ փոխանցում ուրիշ սերվերին։

SQL սերվերը ապահովում է հավելյալ տվյալների կրկնապատկումը 3 սցենարներով.

Նկար. Ստեղծվում է տվյալների բազաների «նկարը», որը սերվերը ուղարկում է ստացողներին

Փոփոխումների պատմություն. Տվյալների բազաների բոլոր փոփոխությունները անընդհատ փոխանցվում են օգտագործողներին

Ուրիշ սերվերների հետ համաժամացում(սինխրոնիզացիա). Մի քանի սերվերների տվյալների բազաները համաժամացվում են միմյանց միջև։ Բոլոր տվյալների բազաների փոփոխությունները յուրաքանչյուր սերվերում կատարվում են միմյանցից անկախ, իսկ համաժամացման ժամանակ բոլոր տվյալները համեմատվում են։ Այդպիսի կրկնապատկման տեսակը ապահովում է տվյալների բազաների միջև տարաձայնությունների լուծման հնարավորությունը։

[SQL Server 2005](http://hy.wikipedia.org/w/index.php?title=SQL_Server_2005&action=edit&redlink=1)-ում ներդրված է [.NET Framework](http://hy.wikipedia.org/w/index.php?title=.NET_Framework&action=edit&redlink=1)-ի ապահովում։ Դրա շնորհիվ տվյալների բազաների պահպանելի պրոցեդուրաները կարող են գրվել .NET պլատֆորմի ցանկացած լեզվով՝ օգտագործելով գրադարանների ամբողջ հավաքածուն, որը առկա է .NET Framework-ի համար, գումարած Common Type System-ը (Microsoft .NET Framework-ում տվյալների տեսակների դիմելու համակարգ)։ Սակայն, ուրիշ պրոցեսների հետ համեմատած, .NET Framework-ը, լինելով բազիսային համակարգ SQL Server 2005-ի համար, հատկացնում է հավելյալ հիշողություն և օգտագործում է SQL Server-ի կառավարման միջոցները, Windows-ի միջոցները օգտագործելու փոխարեն։ Դա բարձրացնում արտադրողականությունը՝ համեմատած Windows-ի ընդհանուր ալգորիթմների հետ, քանի որ ռեսուրսների բաշխման ալգորիթմները հատուկ կարգավորված են SQL Server-ի կառուցվածքներում օգտագործվելու համար։

**1.4.2 Ծրագրերի մշակում**

Microsoft-ը և մյուս ընկերությունները ստեղծում են մեծ քանակությամբ մշակման միջոցներ, որը թույլ է տալիս, օգտվելով Microsoft SQL Server-ի տվյալների բազաներից, ստեղծել բիզնես-ծրագրեր։ Microsoft SQL Server 2005-ը նույնպես իր մեջ ներառում է Common Language Runtime (CLR) [Microsoft .NET](http://hy.wikipedia.org/w/index.php?title=Microsoft_.NET&action=edit&redlink=1), որը թույլ է տալիս իրականացնել պահպանվող պրոցեդուրաներ և տարբեր ծրագրային ֆունկցիաներ՝ ստեղծված .NET (օրինակ, [VB.NET](http://hy.wikipedia.org/w/index.php?title=VB.NET&action=edit&redlink=1) կամ [C#](http://hy.wikipedia.org/wiki/C)) լեզուների պլատֆորմի վրա։ Microsoft-ի նախորդ ստեղծված միջոցների տարբերակները օգտագործել են միայն API, որպիսի ստանան Microsoft SQL Server-ին ֆունկցիոնալ մուտք։

**SQL Server Express Edition**

[Microsoft SQL Server Express](http://hy.wikipedia.org/w/index.php?title=Microsoft_SQL_Server_Express&action=edit&redlink=1)-ը SQL Server տարբերակի անվճար տարածվող տեսակն է, [MSDE](http://hy.wikipedia.org/w/index.php?title=MSDE&action=edit&redlink=1) համակարգի զարգացմամբ։ Տվյալ տարբերակը ունի տեխնիկական որոշ սահմանափակումներ։ Այդպիսի սահմանափակումները դարձնում են նրան մեծ տվյալներ բազաների ստեղծման համար ոչ պիտանի, բայց այն միանգամայն պիտանի է փոքր ընկերությունների սահմաններում ծրագրային կոմպլեքսների ներմուծման համար։ Լիարժեք ապահովում է տվյալների նոր տիպերի օգտագործումը, այդ թվում [XML](http://hy.wikipedia.org/wiki/XML)-հատկորոշումներ (սպեցիֆիկացիա)։ Փաստորեն, այն լիարժեք MS SQL Server է, որը ներառում է իր ծրագրավորման բոլոր բաղադրիչները, ապահովում է ազգային և[Unicode](http://hy.wikipedia.org/wiki/Unicode) այբուբեններ։ Այդ պատճառով օգտագործվում է ծրագրերում, նախագծման կամ ինքնուրույն հետազոտման համար։ Չկա ոչ մի խոչընդոտ՝ հետագայում կուտակած MS SQL Server ոչ էքսպրես տարբերակի տվյալների բազաների տեղակայման համար։ [2007](http://hy.wikipedia.org/wiki/2007) թ. Microsoft-ը թողարկեց գրաֆիկական ինտերֆեյսով առանձին գործիք այդ տարբերակի կառավարման համար, որը նույնպես կարելի է անվճար բեռնել ընկերության պաշտոնական կայքից։

**Սահմանափակումներ**

1 պրոցեսոր(այն կարող է տեղադրված լինել ցանկացած սերվերում)

1 գբ հասցեային հիշողություն

4 գբ բազայի առավելագույն չափս (10 գբ SQL Server 2008 R2-ի համար)

SQL Server Management Studio 2005-ի ինտերֆեյսից անհնար է տվյալների մուտքագրում/արտածում (2008 տարբերակի մեջ այդ հնարավորությունը կա)

[Windows](http://hy.wikipedia.org/wiki/Windows)-ի համար նախատեսված տարբերակներ

1992 - SQL Server 4.2

1993 - SQL Server 4.21 Windows NT-ի համար

[SQL Server 2008](http://hy.wikipedia.org/w/index.php?title=SQL_Server_2008&action=edit&redlink=1)-ը ուղղված է տվյալների ղեկավարումը ինքնակարգավորվող, ինքնակառավարվող և ինքնասպասարկող մեխանիզմ դարձնելուն. այդպիսի հնարավորությունների իրականացման համար ստեղծվել են SQL Server Always On տեխնոլոգիաները: Այն հնարավորություն է ընձեռում զրոյացնել սերվերի չաշխատելու վիճակի ժամանակը:

SQL Server 2008-ում ավելացվել է կառուցվածքային և կիսակառուցվածքային տվյալների ապահովումը, ներառելով` նկարների, ձայնային, վիդեո և այլ թվային մուլտիմեդիա տիպի ֆորմատներ։ Մուլտիմեդիա-ֆորմատների ապահովումը բազաներում թույլ տվեց հատուկ ֆունկցիաների փոխգործակցել այդ տիպի տվյալների հետ։

Բացի այդ, ներառվեցին նաև հատուկ ֆորմատներ՝ ամսաթիվ և ժամանակ և տարածային (անգլ. Spatial) տիպ հատուկ տարածակախյալ տիպի տվյալների համար։ Ոչ կառուցվածքային տվյալների համար ստեղծվեց հատուկ տիպ. օրինակ՝ Պատկեր։

SQL Server-ում կառավարման էֆեկտիվությունը բարձրացնելու համար ներառվեցին [Declarative Management Framework](http://hy.wikipedia.org/w/index.php?title=Declarative_Management_Framework&action=edit&redlink=1) գրադարանները, որի շնորհիվ հնարավոր է բաշխել լիազորություններ տվյալների բազաների կամ առանձին աղյուսակների համար։ Նորացվել են տվյալների խտացման եղանակները։ [. SQL Server Katmai](http://hy.wikipedia.org/w/index.php?title=._SQL_Server_Katmai&action=edit&redlink=1)-ն[[1]](http://hy.wikipedia.org/wiki/Microsoft_SQL_Server#cite_note-2k8-1)[[2]](http://hy.wikipedia.org/wiki/Microsoft_SQL_Server#cite_note-PaulFlessner-2)ապահովում է [ADO.NET Entity Framework](http://hy.wikipedia.org/w/index.php?title=ADO.NET_Entity_Framework&action=edit&redlink=1) գրադարանների հավաքածուն և կրկնման ծանուցումների միջոցներ ու տվյալների տիպի որոշում։

**AES գաղտնագրում**

Գաղտնագրման համար AES ալգորիթմում կիրառվում են տվյալների ձևափոխության հետևյալ գործընթացները՝

1. ExpandKey - Բոլոր փուլերի համար փուլային բանալիների հաշվում:

2. SubBytes - Փոխարինման աղյուսակի միջոցով բայթերի փոխարինում:

3. ShiftRows - Վիճակում տողերի, տարբեր քանակությամբ, ցիկլիկ տեղաշարժ:

4. MixColumns - Վիճակի յուրաքանչյուր սյունյակում տվյալների խառնում:

5. AddRoundKey - Փուլի բանալու գումարումը վիճակին:

Գաղտնագրումը տեղի է ունենում նկ. 1-ում պատկերված ալգորիթմով:

**SubBytes ձևափոխությունը**

SubBytes ձևափոխությունը կայանում է վիճակի ամեն {xy} բայթը (որտեղ x և y 16-ական համակարգի թվեր են), աղ. 1-ի համաձայն, մեկ քայլով փոխարինման մեջ:

**ShiftRows** **ձևափոխությունը**

ShiftRows ձևափոխությունը իրենից ներկայացնում է վիճակի տողերի ցիկլիկտեղաշարժ դեպի ձախ: Առաջին տողը մնում է նափոփոխ, երկրորդում կատարվում է տեղաշարժ մեկ բայթով, երրորդում 2 բայթով, չորրորդում՝ 3:

**MixColumns ձևափոխությունը**

MixColumns ձևափոխության ժամանակ կատարվում է 4-րդ աստիճանի քառակուսային մատրիցի բազմապատկում վիճակի յուրաքանչյուր սյունյակի հետ: Յուրաքանչյուր սյունյակի հետ գործողությունը կատարվում է առանձին:

**AddRoundKey** **ձևափոխությունը**

AddRoundKey ձևափոխության ժամանակ փուլային բանալու 32-բիթանոց բառերը XOR բիթային գործողության միջոցով գումարվում են վիճակի սյուներին: Յուրաքանչյուր սյունյակի հետ գործողությունը կատարվում է առանձին:

**ExpandKey** **գործընթացը**

AES ալգորիթմում փուլային բանալիները գեներացվում են գաղտնագրման բանալու հիման վրա՝ ExpandKey գործընթացի միջոցով: ExpandKey գործընթացը ստեղծում է Nb \* (Nr + 1) բառ, որտեղ Nb-ն բլոկում բառերի քանակն է, Nr-ը՝ փուլերի քանակը: Ալգորիթմին անհրաժեշտ է Nb երկարությամբ սկզբնական բանալի, ինչպես նաև Nr փուլերից յուրաքանչյուրը պահանջում է Nb բառերից կազմված բանալի:

**AES վերծանում**

Վերծանման ժամանակ բոլոր ձևափոխությունները կատարվում են հակառակ հերթականությամբ: Գոյություն ունեցող գաղտնագրող ձևոփոխությունների փոխարեն օգտագործվում են հետևյալ հակադարձ ձևափոխությունները՝

1. InvSubBytes - Բայթերի փոխարինում հակադարձ փոխարինման աղյուսակի միջոցով,

2. InvShiftRows - Վիճակում տողերի ցիկլիկ տեղաշարժ տարբեր քայլերով,

3. InvMixColumns - Վիճակի յուրաքանչյուր սյունյակում տվյալների խառնում:

ExpandKey և AddRoundKey գործընթացները մնում են անփոփոխ: Փուլի բանալիները օգտագործվում են հակառակ հերթականությամբ: Վերծանման ալգորիթմը ներկայցաված է նկ. 2-ում:

**InvShiftRows ձևափոխությունը**

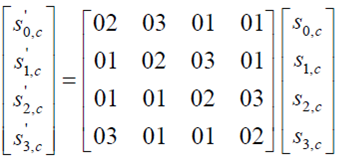
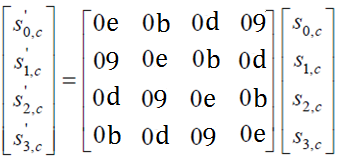
Սա ShiftRows ձևափոխությանը հակադարձ ձևափոխություն է: Վիճակի առաջին տողը մնում է անփոփոխ, երկրորդը 1 բայթով ցիկլիկ տեղաշարժվում է աջ, երրորդը 2 բայթով, չորրորդը՝ 3:

**InvSubBytes ձևափոխությունը**

Սա SubBytes ձևափոխությանը հակադարձ ձևափոխություն է: Բայթերի փոխարինումը իրականացվում է համանմանորեն՝ հակառակ փոխարինումների աղյուսակի համաձայն:

**InvMixColumns ձևափոխությունը**

Սա MixColumns ձևափոխությանը հակադարձ ձևափոխություն է: Վիճակի յուրաքանչյուր սյունյակը ձևափոխվում է առանձին:



InvMixColumns

ձևափոխությունը

MixColumns

ձևափոխությունը

**RSA գաղտնագրային ալգորիթմը**

RSA-ը հանդիսանում է գաղտնագրման առաջին լիակատար անհամաչափ ալգորիթմը, որը կարելի է օգտագործել ինչպես տեղեկատվության գաղտնագրված փոխանակման, այնպես էլ թվային ստորագրության ձևավորման համար և ստեղծվել է 1977թ.: Այն անվանվել է ալգորիթմը մշակոած երեք գիտնականների՝ Ռոն Ռիվեստի (Ron Rivest), Ադի Շամիրիր (Adi Shamir) և Լեոնարդ Էդլմանի (Leonard Adleman) անզգանունների սկզբնատառերով: Գոյություն ունեցող անհամաչափ գաղտնագրային ալգորիթմներից RSA-ն հավանաբար ամենահեշտն է հասկանալու և իրագործելու տեսակետից և միաժամանակ գործնականում ամենատարածվածը: Այս ալգորիթմը երկար տարիներ դիմակայում է ինտենսիվ գաղտնավերլուծությանը: Չնայած գաղտնավերլուծությունը ո՛չ ապացուցել է, ո՛չհակասել RSA-ի ավտանգությունը, այն, ըստ էության, հիմնավորում է ալգորիթմի հանդեպ վստահությունը:

RSA-ի անվտանգությունը հիմնված է մեծ թվերը բազմապատկիչների վերլուծելու բարդության մեջ: Բաց և փակ բանալիները հանդիսանում են երկու մեծ պարզ թվերի ֆունկցիաներ: Ենթադրվում է, որ ըստ գաղտնագրված տեքստի և բաց բանալու, բաց տեքստի վերականգնումը համարժեք է երկու մեծ թվերը բազմապատկիչների վերլուծելուն:

**RSA բանալիների ստացումը**

Երկու բանալիների գեներացման համար օգտագործվում են երկու մեծ պարզ թիվ՝ P և Q: Առավելագույն անվտանգության համար P-ն և Q-ն ընտրվում են միևնույն երկարության: Հաշվում ենք հետևյալ արտադրյալը.

N = P \* Q

Այնուհետև ընտրվում է 1-ից մեծ E թիվ, որը (P-1) \* (Q-1) արտադրյալից փոքր է և փոխադարձաբար պարզ է նրա հետ: N և E թվերը հանդիսանում են բաց բանալին: Վերջում Էվկլիդեսի ընդլայնված ալգորիթմով հաշվվում է D փակ բանալին.

D = E-1 mod ((P-1)(Q-1))

D և N թվերը նույնպես փոխադարձաբար պարզ են: P և Q թվերը այլևս պետք չեն, սակայն պետք է գաղտնի պահվեն, քանի որ նրանց միջոցով կարելի է հաշվարկել D փակ բանալին:

**RSA գաղտնագրում և վերծանում**

M հաղորդագրությունը գաղտնագրելու համար նախևառաջ այն բաժանվում է N-ից փոքր թվային բլոկների (երկուական տվյալների համար ընտրվում է N-ից փոքր 2-ի ամենամեծ աստիճանը): Այսինքն, եթե P-ն և Q-ն 100-կարգանի պարզ թվեր են, ապա N-ը կպարունակի մոտ 200 կարգ և հաղորդագրության յուրաքանչյուր Mi բլոկի երկարությունը պետք է լինի մոտ 200 կարգ: C գաղտնագրված հաղորդագրությունը բաղկացած կլինի միևնույն երկարությամբ Ci բլոկներից: Գաղտնագրման բանաձևն ունի հետևյալ տեսքը՝

ci = mie mod n

Հաղորդագրությունը վերծանելու համար պետք է վերցնել գաղտնագրված Ci բլոկներից յուրաքանչյուրը և հաշվել

mi = cid mod n

Քանի որ

cid = (mie(mod n))d = mied(mod n) = mik(p-1)(q-1)+1(mod n) =

= mi\*mik(p-1)(q-1) (mod n) = mi\*1(mod n) = mi (mod n)

հետևաբար բանաձևը վերականգնում է հաղորդագրությունը:

Նույն կերպ հաղորդագրությունը կարող է գաղտնագրվել D-ի միջոցով և վերծանվել E-ի միջոցով:

**RSA ալգորիթմի արագությունը**

RSA-ի գլխավոր թերությունը կայանում է շատ ցածր արագագործության մեջ: Այդ իսկ պատճառով, մեր խնդրում RSA ալգորիթմով գաղտնագրվում է միայն AES ալգորիթմի բանալին, իսկ տեքստը գաղտնագրվում է AES ալգորիթմով, այսինքն՝ ընդհանուր համակարգի արագագործությունը էականորեն չի տուժում:

RSA ալգորիթմով գաղտնագրում իրականացվում է զգալիորեն ավելի արագ, եթե E-ի արժեքը ճիշտ է ընտրվում: Ամենից հաճախ կիրառվող երեք տարբերակներն են՝ 3, 17 և 65537 (65537 թվեի երկուական ներկայացումները պարունակում է երկու հատ մեկ, ինչի շնորհիվ աստիճան բարձրացնելիս պետք է կատարել ընդամենը 17 բազմապատկում): Այս երեք թվերից ոչ մեկի կիրառության դեպքում չկա անվտանգության խնդիր (այն պայմանով, որ հաղորդագրությունը լրացվում է պատահական թվերով), նույնիսկ եթե E-ն օգտագործվում է օգատագործողների մի ամբողջ խմբի կողմից:

Փակ բանալիներով գործողությունները կարելի արագացնել նաև մնացորդների մասին չինական թեորեմի միջոցով, եթե պահպանվել են P, Q, արժեքները, ինչպես նաև d mod (p - 1), d mod (q - 1) և q-1 mod p լրացուցիչ արժեքները:

**RSA ալգորիթմի անվտանգությունը**

RSA-ի անվտանգությունը ամբողջությամբ կախված է մեծ թվերը բազմապատկիչների վերլուծելու խնդրից: Տեխնիկապես, անվտանգության մասին այս պնդումը կեղծ է: Երբևէ մաթեմատիկորեն չի ապացուցվել, որ ըստ C-ի և E-ի M-ը վերականգնելու համար պետք է N-ը վերլուծել բազմապատկիչների: Հասկանալի է, որ հնարավոր է հայտնաբերվի RSA-ի գաղտնավերլուծության ամբողջովին այլ մեթոդ: Սակայն, եթե այդ մեթոդը օգնի գաղտնավերլուծողին ստանալ D-ն, այն կարող է օգտագործվել նաև մեծ թվերը բազմապատկիչների վերլուծելու ժամանակ:

RSA-ն կարելի է կոտրվել նաև գուշակելով (P-1)(Q-1) արժեքը, ինչն ավելի հեշտ չէ քան N-ը բազմապատկիչների վերլուծելը:

N-ը բազմապատկիչների վերլուծելը կոտրելու ամենաակնհայտ տարբերակն է: Ցանկացած հակառակորդ կարող է ունենալ E բաց բանալին և N մոդուլը: Վերծանման D բանալին գտնելու համար հակառակորդը պետք է N-ը վերլուծի բազմապատկիչների: Ներկա դրությամբ ամենամեծ թիվը, որը վերլուծվել է բազմապատկիչների պարունակում է 129 թվանշան՝ տասական համակարգով: Հետևաբար N-ը պետք է մեծ լինի այդ թվից:

Իհարկե, գաղտնավերլուծողը կարող է փորձել D-ի բոլոր հնարավոր տարբերակները, մինչև գտնի ճիշտ թիվը: Այսպիսի մոտեցումը նվազ արդյունավետ է քան N-ը բազմապատկիչների վերլուծելը:

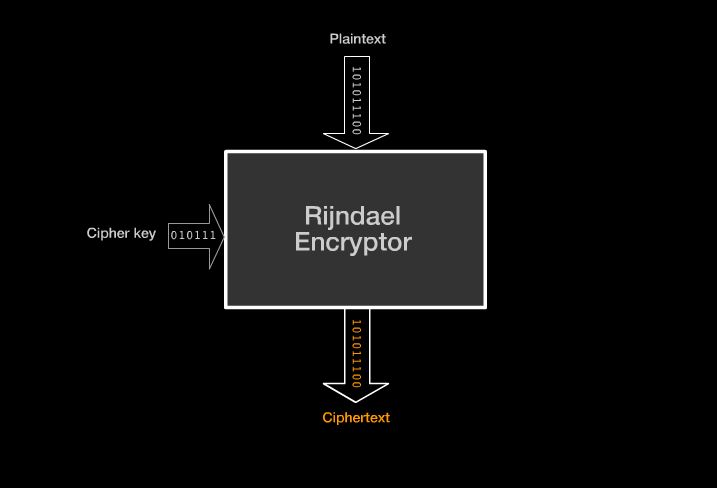
Ժամանակ առ ժամանակ տարբեր հայտարարաություններ են հայտնվում այն մասին, իբր RSA-ը կոտրելու հեշտ մեթոդը գտնվել է, սակայն դեռևս այդ հայտարարություններից ոչ մեկը չի հաստատվել:

Կա RSA ալգորիթմի անհանգստության համար վստահ լինելու ևս մեկ առիթ: P և Q պարզ թվերի հաշվարկման ալգորիթմների մեծամասնությունը հավանականային են: Իսկ ի՞նչ կլինի, եթե P-ն և Q-ն լինեն բաղադրյալ: Առաջին հերթին կարելի է նման դեպքի հավանականությունը հասցնել նվազագույնի: Եվ նույնիսկ, եթե այդպիսի բան տեղի ունենա, ամենայն հավանականությամբ նմանատիպ դեպքը միանգամից կհայտնաբերվի՝ գաղտնագրումն ու վերծանումը չեն աշխատի: Գոյություն ունեն թվեր, որոնք չեն հայտնաբերվում պարզ թվերի որոմնան հավանականային ալգորիթմների կողմից: Այդ թվերը շատ հազվադեպ են և կոչվում են Կարլմայքլի թվեր:

**1.5 AES: ալգորիթմի նկարագրությունը**

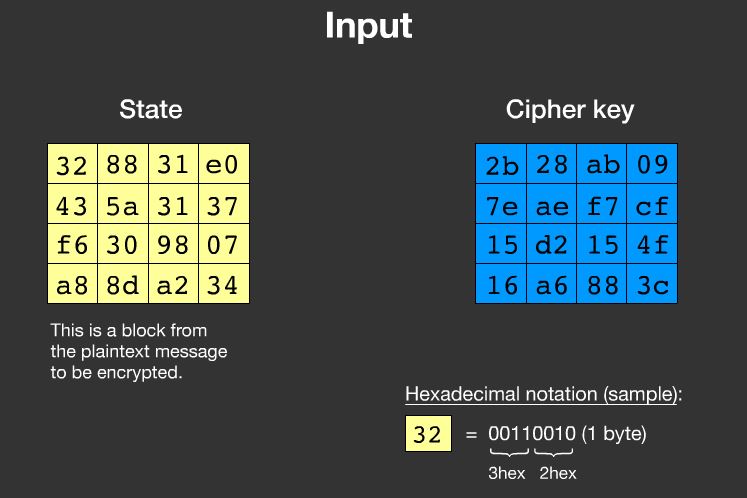
AES գաղտնագրման ալգորիթմը ստեղծվել է DES-ին փոխարինելու համար, որ գաղտնակայունությունն այդ ժամանակ արդեն խոցելի էր: Ի տարբերություն DES- ի AES-ում մտցվել է գաղտնիության մակարդակներ: Գաղտնագրումը կարելի է կատարել 128,192,256 բիթ երկարությամբ բանալիներով (կախված նրանից ինչ կարևորություն ունի գաղտնագրվող ինֆորմացիան): AES – ը այսօր աշխարհում ամենատարածված համաչափ գաղտնագրման ալգորիթմն է և մինչ այսօր չի կոտրվել:

AES – ը դա Rijndael ալգորիթմն է (չնայած կա որոշակի տարբերություն` Rijndael – ում գաղտնագրվող բլոկի չափը կարող է լինել 128,192 կամ 256 բիթ, իսկ AES – ում ֆիքսված է և հավասար է 128 - բիթի): Ալգորիթմում օգտագործվում են հետևյալ ընդունված նշանակումները .

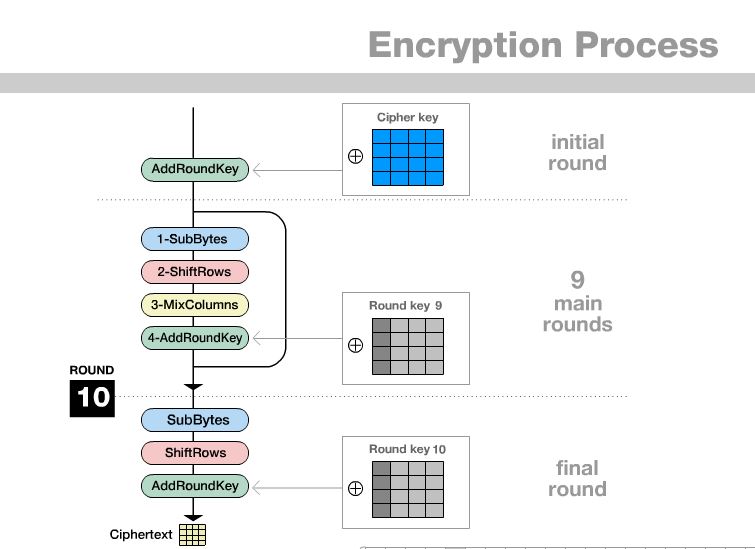
**

*Նկ.1*

Գաղտնագրման պրոցեսսը բաղկացած է երկու մասից` բաց հատվածի գաղտնագրում և բանալիների ստացում: Նախ դիտարկենք բաց հատվածի գաղտնագրման պրոցեսսը:



Նկ.2

State-ը համապատասխանում է բաց տեքստի հատվածին, Ciper Key-ն բանալին է:

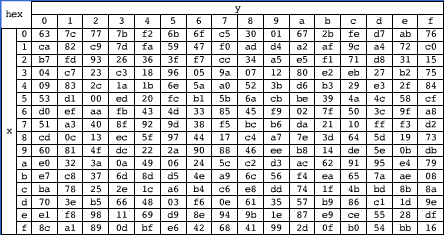
Նկ.3

Վերը ցուցադրված նկարից երևում է, որ գաղտնագրման պրոցեսը բաղկացած 9-ը հիմնական ր 1 վեևջին 10-րդ փուլերից:Բոլոր փուլերին համապատասխանում է տվյալ փուլի բանալին, որոնց ստացումը կդիտարկենք ավելի ուշ: Դիտարկենք ալգորիթմի բլոկերն առանձին-առանձին:

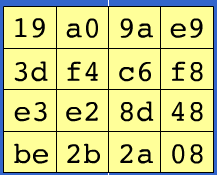
**1.5.1 Գաղտնագրում**

**SubBytes/Բայթերի փոխարինում**

Բայթերի փոխարինման պրոցեսսում օգտվում ենք նախապես հաշվարկված և բոլորին հայտնի Ս-բոքսից, որն իրենից ներկայացնում է 16\*16 երկչափ զանգված, որի ամեն մի անդամ իրենից ներկայացնում է 0 – 255 միջակայքի որևէ թիվ նկ. 3:

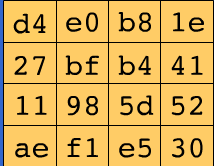


Նկ.4 Ս-բոքս



Նկ. 5 Բաց տեքստի բլոկ

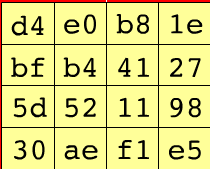
Հերթականությամբ բաց տեքստի ամեն բլոոկի ամեն բայթի համար դիտարկում ենք ավագ բայթը որպես տողի համար, իսկ կրտսերը` սյան: Այդ համարներին համապատասխան գտնում ենք նշված տողի և սյան հատման անդամը Ս-բոքսում և փոխարինում բաց տեքստի բայթը վերջինովս:



Նկ.6 Բայթերի փոխաինման արդյունք

**Shift Rows/Տողերի տեղաշարժ**

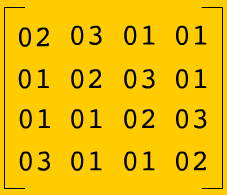
Նախորդ փուլի արդյունքում ստացված արդյունքի տողերը ցիկլիկ տեղաշարժում ենք դեպի ձախ համապատասխանաբար առաջին տողը` 0, երկրորդը` 1, երրորդը` 2, չորրորդը` 3 անգամ:



Նկ.7 Տողերի տեղաշարժի արդյունք

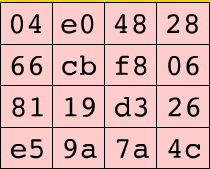
**Mix Columns/Սյուների խառնում**

Նախորդ փուլի արդյունքի յուրաքանչյուր սյուն բազմապատկվում է հետևյալ հաշվարկված և հայտնի մատրիցի հետ:



Նկ.8 Սյուների փոխանակման մատրից

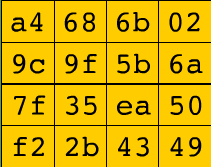
Արդյունքում ստանում ենք՝



Նկ.9 Սյուների խառնման արդյունք

**Add Round Key/Փուլի բանալիի գումարում**

Նախորդ փուլում ստացված արդյունքի յուրաքանչյուր սյուն ըստ մոդուլ 2-ի գումարվաում է տվյալ փուլի բանալիի հետ և արդյունքը գրվում է առաջին սյան տեղը:

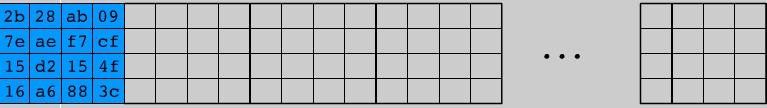


Նկ.10 Փուլի բանալու գումարման արդյունք

**1.5.2 Բանալիների ստացում**

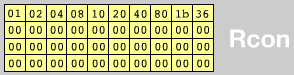
Այժմ դիտարկենք փուլերի բանալիների ստացման գործընթացը:

Մենք ունենք 128 բիթանոց բանալի, որը կօգտավործվի նախնական փուլում: Այժմ պետք է ստանալ մյուս 10 փուլերի բանալիները:



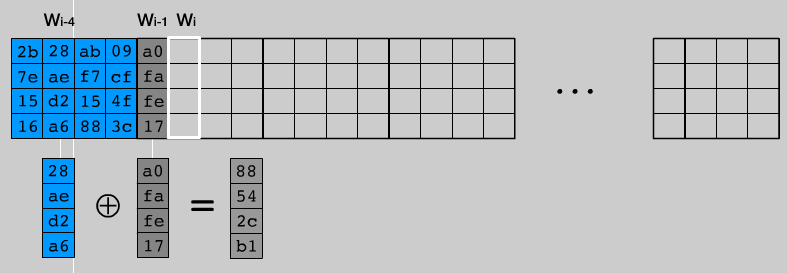
Պետք է ստանալ 10 փուլերի բանալիները

Բանալիների ստացման գործընթացում կկիրառենք նախապես հաշվարկված և բոլորին հայտնի RCon երկչափ զանգվածը:



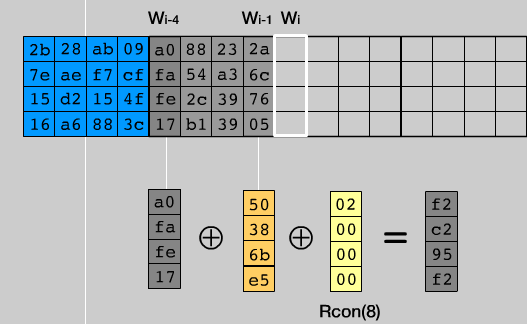
Նկ.11 RCon երկչափ զանգված

Նախ վերցվում է նախնական բանալու վերջին սյունը և ցիկլիկ տեղաշարժ կատարվում մեկ քայլ դեպի վերև: Ապա սյան հետ կատարվում է բայթերի փոխարինման գործողությունը: Ստացված սյանը ըստ մոդուլ 2-ի գումարվում է նրանից 3-ով ետ գտնվող սյունը և RCon ի հերթական սյունը, որը այնուհետև դուրս է հանվում: Արդյունքը գրվում է առաջին փուլի բանալու առաջին սյան դիրքում: Այնուհետև ստացված սյունը ըստ մոդուլ 2-ի գումարվում է նախորդ բանալու երկրորդ սյանը և ստացվածը գրվում է նոր բանալու երկրորդ սյան դիրքում:



Նկ.12 Առաջին փուլի բանալու ստացումը

Նույն պրոցեսսով ստացվում են նոր բանալու երրորդ և չորրորդ սյուները: Այնուհետև երկրորդ փուլի բանալին ստացվում է նույն գարծողությունները կատարելով, այս դեպքում արդեն առաջին փուլի բանալիի հետ:

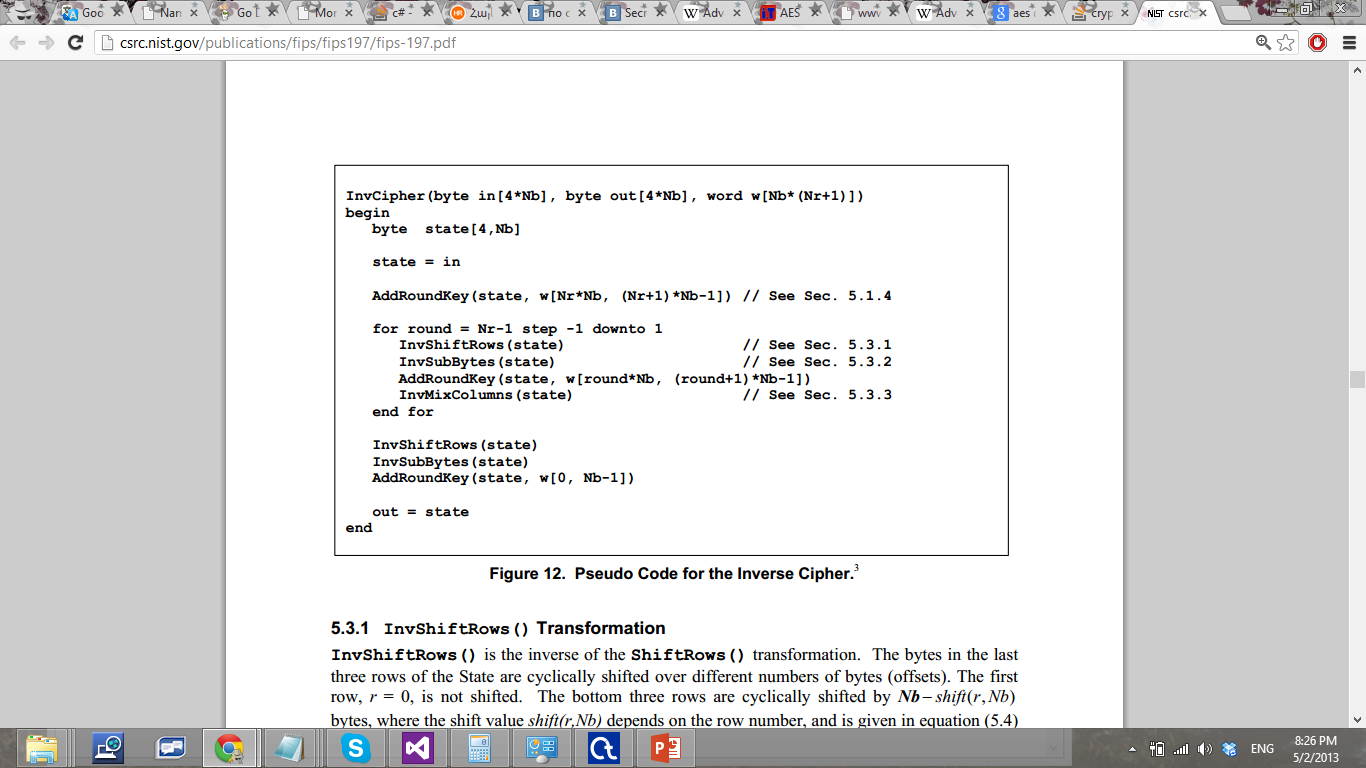


Նկ.13 Երկրորդ փուլի բանալու ստացումը

Արդյունքում ստանում ենք բոլոր 10 փուլերի բանալիները:

**1.5.3 Գաղտնավերծանում**

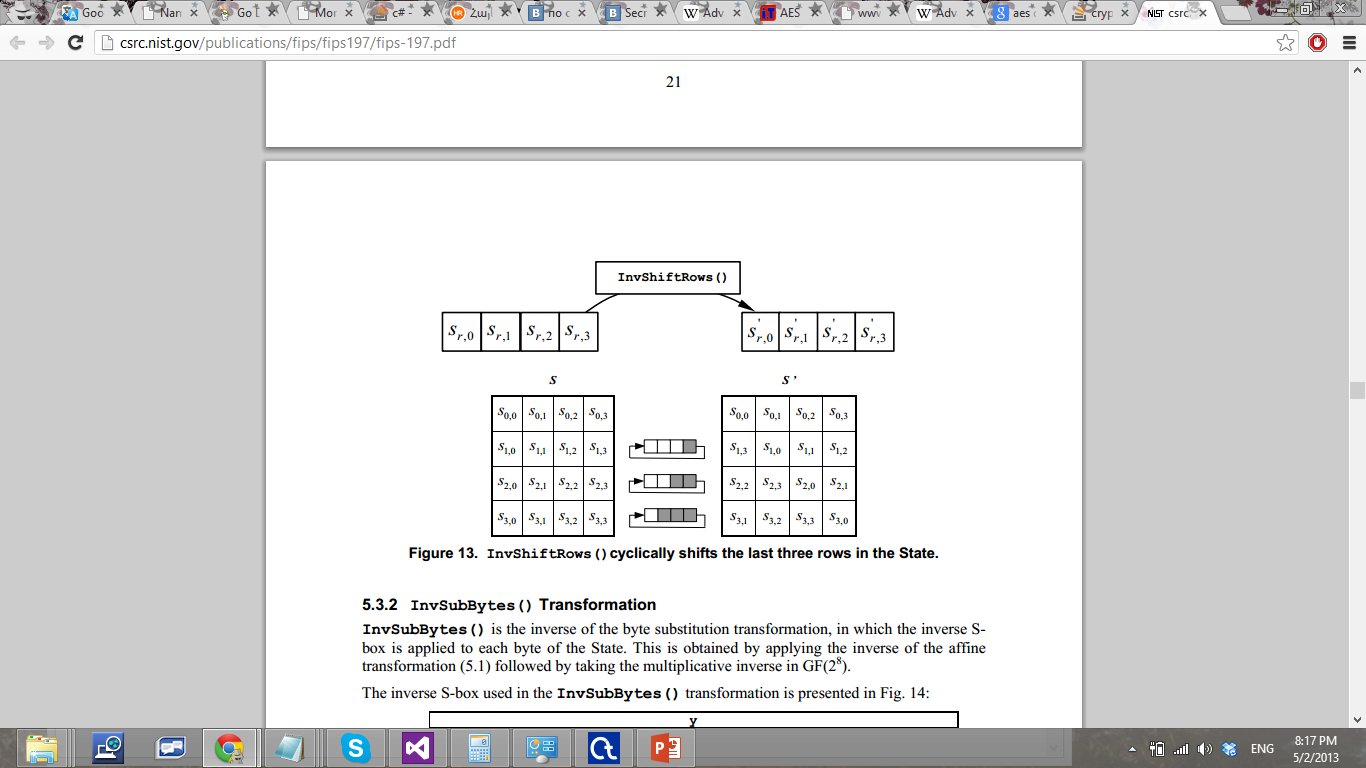
Գաղտնավերծանման պրոցեսսը կատարվում է կրկին նախնական փուլով , 9 միջանկյալ փուլերով և վերջնական փուլով և օգտագործվում են նույն փուլերի բանալիներն ինչ գաղտնագրման դեպքում էր: Սակայն փուլերի գործողություններն և հերթականությունն փոքր ինչ ուրիշ է:



Նկ.14 Գաղտնավերծանման ալգորիթմը

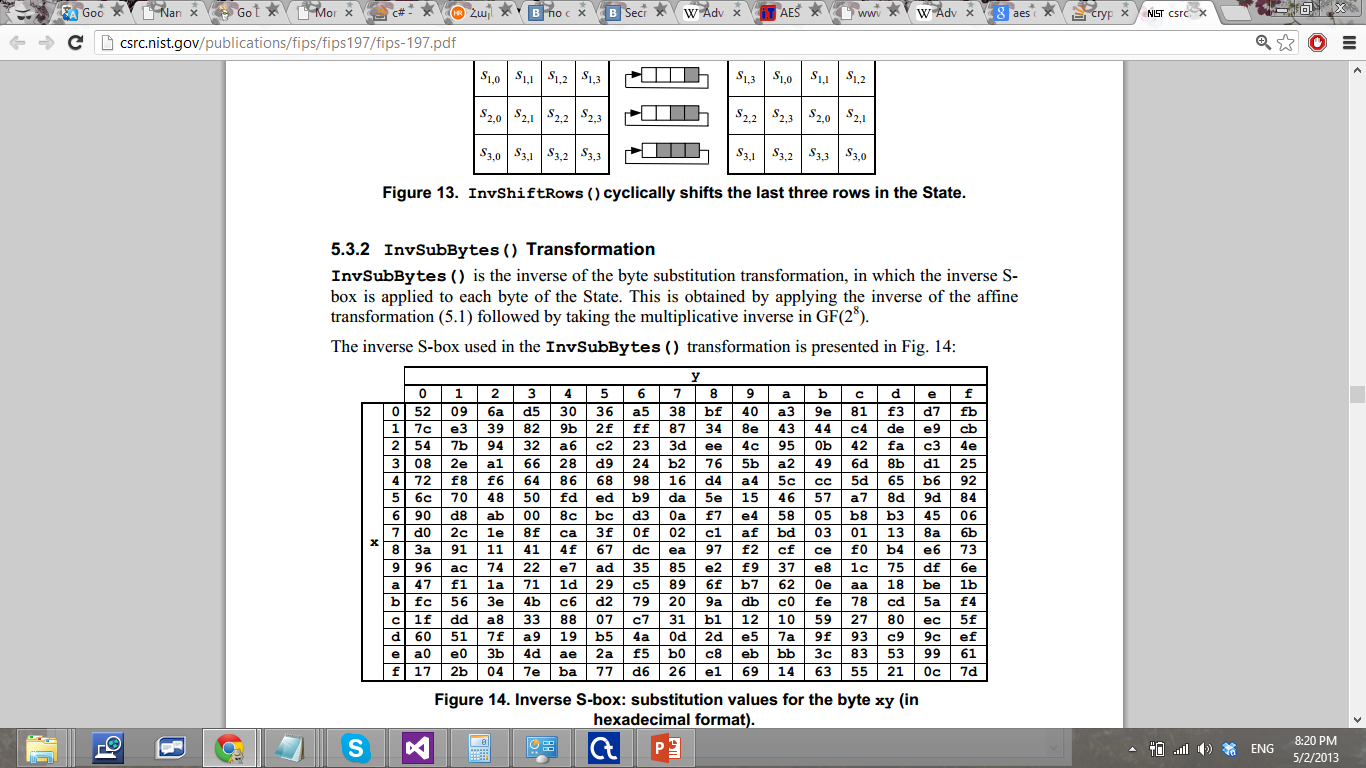
Սկզբում կատարվում է փուլի բանալու գումարում, որը ոչինչով չի տարբերվում նման փուլից գաղտնագրման դեպքում: Այնուհետև 9 փուլ կատարվում է տողերի ինվերս տեղաշարժ, ապա բայթերի ինվերս փոխարինում, ապա փուլի բանալու գումարում և սյուների ինվերս խառնում: Վերջին փուլում չի կատարվում սյուների ինվերս խառնում:

**Տողերի ինվերս տեղաշարժ**

Կատարվում է տողերի տեղաշարժ գործողությունը, բայց այս դեպքում դեպի աջ:

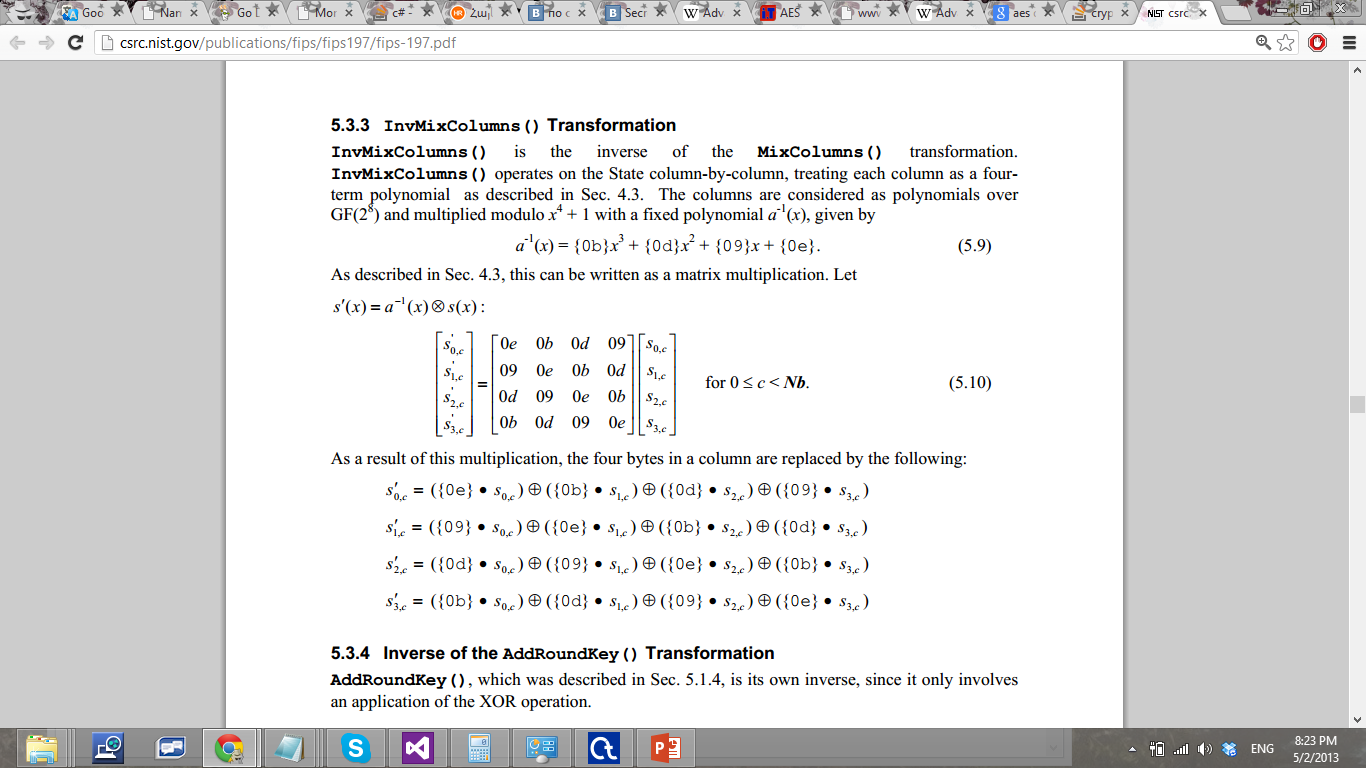
Նկ.15 Տողերի ինվերս տեղաշարժ

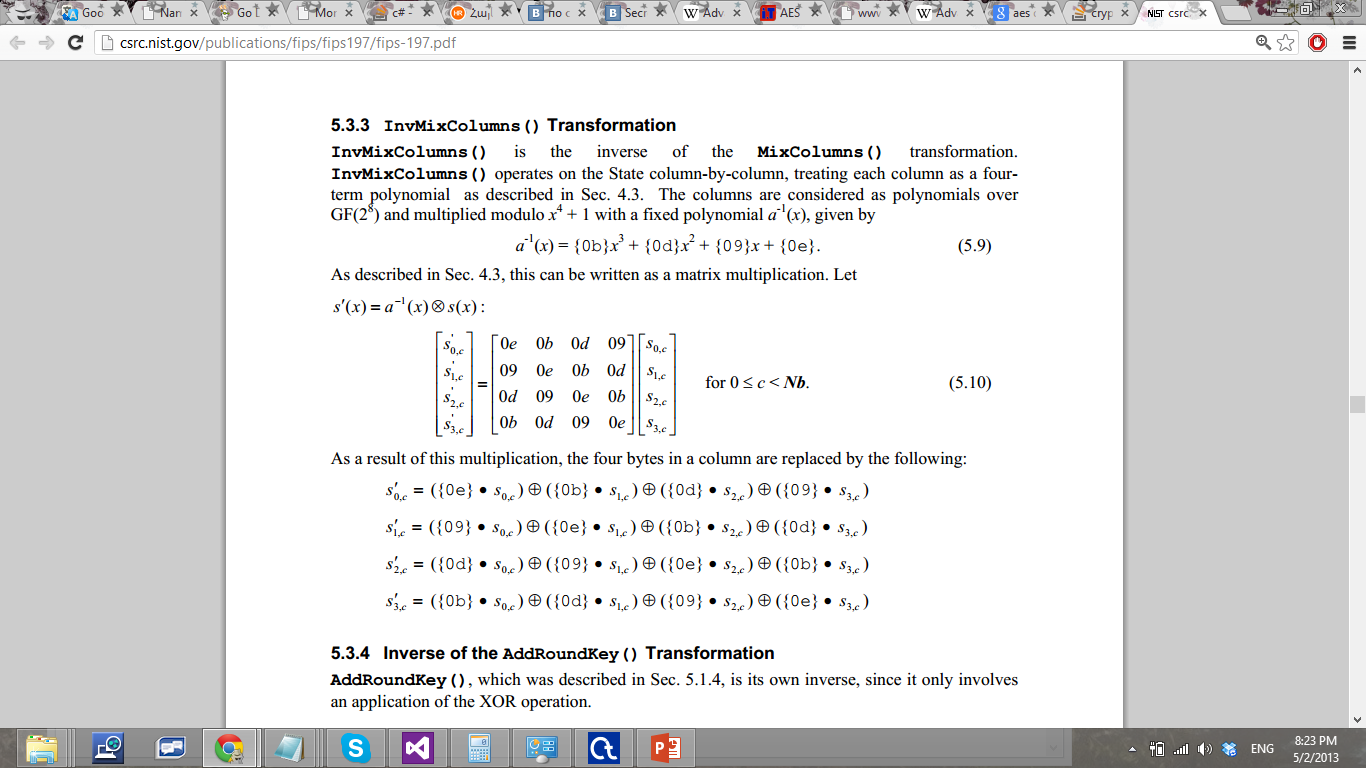
**Բայթերի ինվես փոխարինում**

Կատարվում է բայթերի փոխարինման գործողությունը օգտագործելով ինվերս Ս-բոքս: Նկ.16 Ինվերս Ս-բոքս

**Սյուների ինվերս խառնում**

Կատարվում է սյուների խառնման գործողությունը հաշվարկված ինվերս մատրիցի հետ:





Նկ.17 Սյուների ինվերս խառնում

**1.**

**Գլուխ 2**

**Ծրագրի աշխատանքի և ալգորիթմի նկարագրությունը**

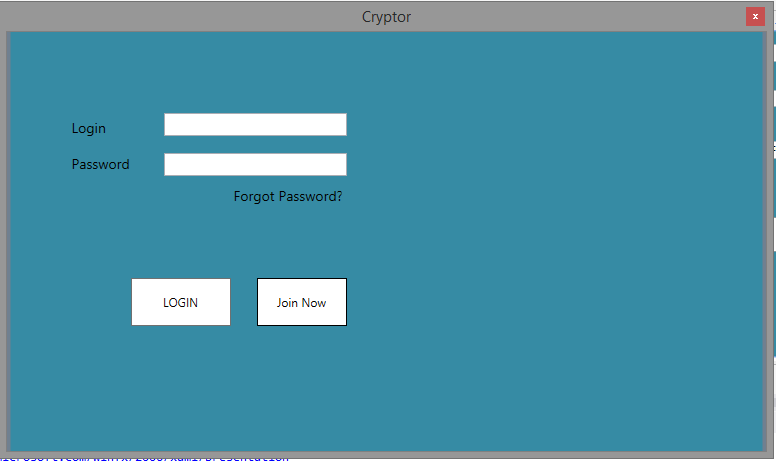
**2.1 Նույնականացում**

Հիմք ընդունելով նշանակված խնդիրները՝

* Ավտոմատացնել գաղտնագրման և վերծանման գործողությունները և բանալիների փոխանակումը
* Բաց կապուղիով երկու օգտատերի միջև անվտանգ փոխանցել տվյալները
* Ստեղծել գաղտնագրված ամպային համակարգ

Առաջարկվում է հետևայլ լուծումը. Ստեղծել ընդհանուր մեկ համակարգ որը կոգտագործի բաց կապուղի, միևնույն ժամանակ լինի անվտանգ և հեշտ կիրառելի ցանկացած ոլորտի օգտագործողի համար: Պետք է ավտոմատացված լինի բանալինների փոխանակումը երկու օգտագործողների միջև:

Դիտարկենք համակարգի սկզբնական պատուհանը:

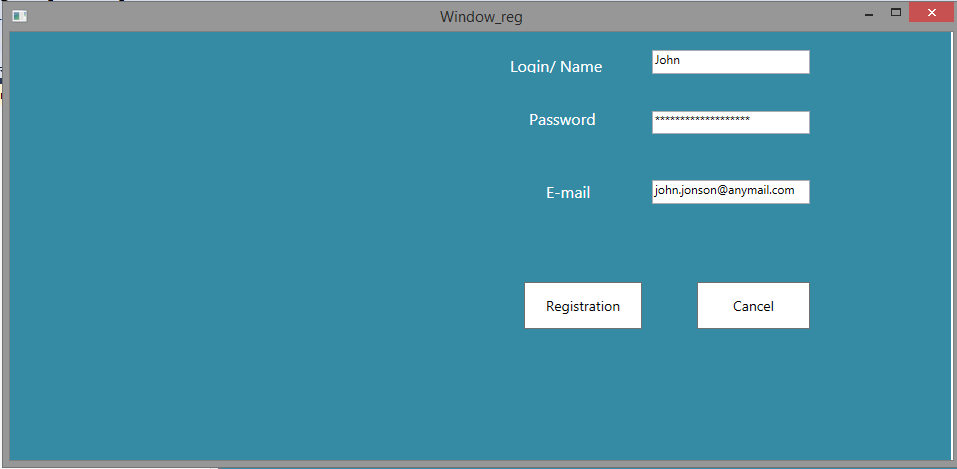


Նկ. 18 Համկարգի սկզբնական պատուհան

Համակարգ մուտք գործելու համար անհրաժեշտ է ունենալ նույնականացման տվյալներ: Որը մուտքագրելուց հետո համեմատում է տվյալների բազայում առկա տվյալների հետ և որոշում թույլ տա, թե` ոչ:

**2.2 Գրանցում համակարգում**

Համակարգում գրացվելու համար պետք է սեղմել Join Now կոճակը, որից հետո կբացվի գրացման պատուհանը (նկ. 19)



Նկ. 19 Գրանցման պատուհան

Գրանցման պատուհանի մեջ առկա են նույնականացման անհրաժեշտ մինիմալ պահանջները: Քանի որ բոլոր օգտատերերը լինելու են հավասար պայմաններում, երեք դաշտը բավական է անվտանգ նույնականացում կիրառել: Պետք է լրացնել Login, password և e-mail դաշտերը:

**Login**- դաշտը յուրահատուկ է լինելու բոլորի համար, այսինքն նա չի կրկնվի, որի շնորհիվ կարողանում ենք կիրառել նույնականացման ժամանակ:

**Password**-իհարկե գաղտնաբառի յուրահատկությունը ավելորդ է: Անվտանգությունը ապահովելու համար այն հեշավորվում է և պահվում սերվերում:

**E-mail-** էլեկտրոնային հասցեն պետք է լինի յուրահտւկ և օգտագործվում է գաղտնաբառը վերականգնելու համար:

Համակարգը ավտոմատ ստուգում է բոլոր յուրահատուկ պայմանները բազային մակարդակի վրա:

cmd.CommandText = "SELECT \* FROM [diplom].[dbo].[user] WHERE Login='" + this.textBox\_Login.Text + "' OR E-mail ='"+this.textBox\_email+"'";

Տվյալները լրացնելուց հետո պետք է սեղմել «Registration» և համակարգը հայտնում է գրանցումը հետևայլ նախադասությամբ- "Data Entered Successfully"

Համակարգում կիրառվում է SHA-2 հեշավորման ֆունկցիան:

**Հեշ ֆունկցիաները** պարզապես անհակադարձելի գաղտնագրեր են։ Հա-

ղորդագրության հեշը նրա «խտացված պատկերն» է։

Հեշ ֆունկցիայի արգումենտը կարող է լինել կամայական երկարություն, իսկ նրա

արդյունքը ունի ֆիքսված երկարություն։

Հնարավոր է այնպիսի դեպք, երբ 2 արժեք ունեն նույն հեշը։ Այդ վիճակը կոչվում է

բախում (collision)։

Եթե գործնականում հնարավոր է գտնել մի արժեք, որի հեշը տալիս է որոշակի

արժեք, ապա հեշը համարվում է կոտրված, և չպետք է օգտագործվի անվտանգության

ապահովման համար։

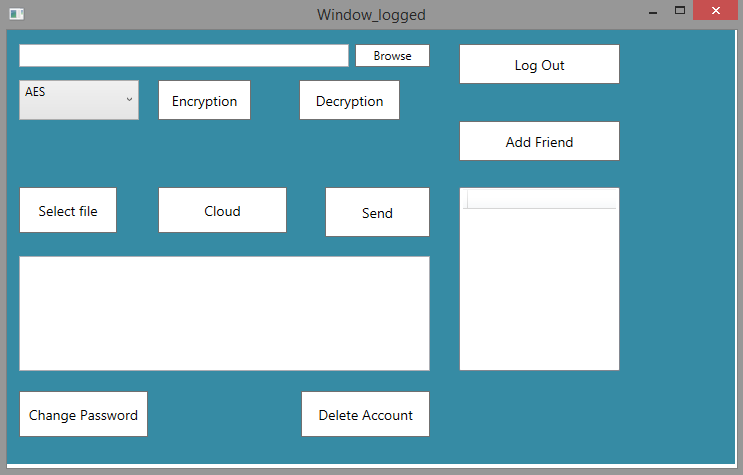
Հեշեր օգտագործվում են օր․՝ գաղտնաբառերի պահպանման ժամանակ, ֆայլերի

ամբողջականության ստուգման ժամանակ, և այլն։

Ամենաշատ օգտագործվող հեշ ֆունկցիաներից են MD5, MD4, SHA256, SHA512,

CRC32։

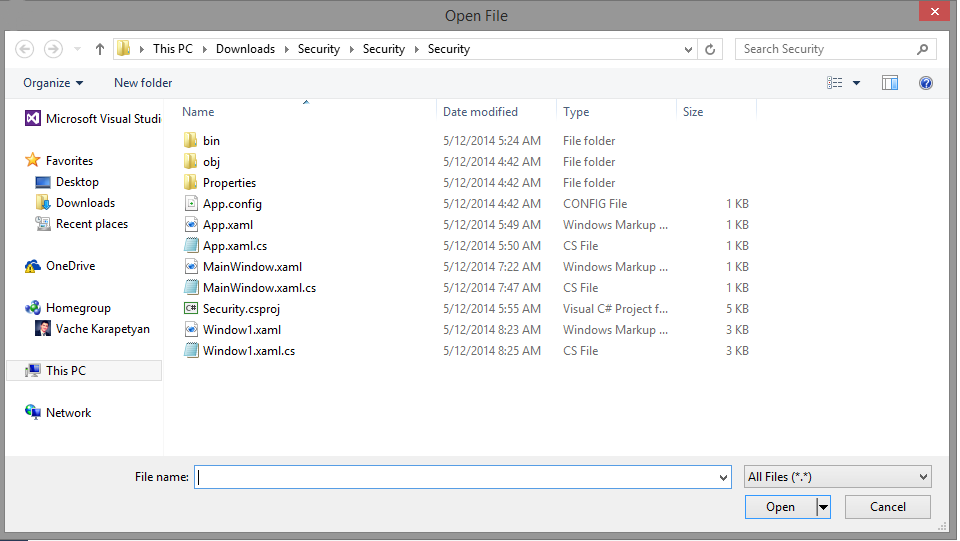
Համակարգ մուտք գործելուց հետո բացվում է նկ. 20-ում պատկերված պատուհանը:



Նկ. 20 Հիմնական պատուհան

**2.3 Լոկալ գաղտնագրում և վերծանում**

**Գաղտնագրումը** հնարավոր է կատարել լոկալ և գատնագրված ֆայլը պահպանել համակրգչում: Սեղմելով **Browse** կոճակը բացվվում է ընտրելու պատուհանը(նկ.21), որից հետո ընտրում ենք գաղտնագրման ալգորիթմը (**AES** հատվածային կամ **RC4** հոսքային) և սեղմում **Encryption** կոճակը, որից հետո պետք է նորից հավաքել գաղտնաբառը(նկ. 22): Գացտնագրված ֆայլը պահպանելու համար ևս մեկ անգամ կբացվի նկ.21-ի պատուհանը:



Նկ. 21 ընտրության պատուհան

**Վերծանման** գործողությունը կատարվում է հակառակ հերթականությամբ: Այսինքն սկզբից պետք է ընտրել գաղտնգրված ֆայլը և սեղմել **Decryption** կոճակը և նույնպես կրկին հավաքել գաղտնաբառը(նկ. 21):

**2.4 Բաց կապուղիով ֆայլերի անվտանգ փոխանակումը**

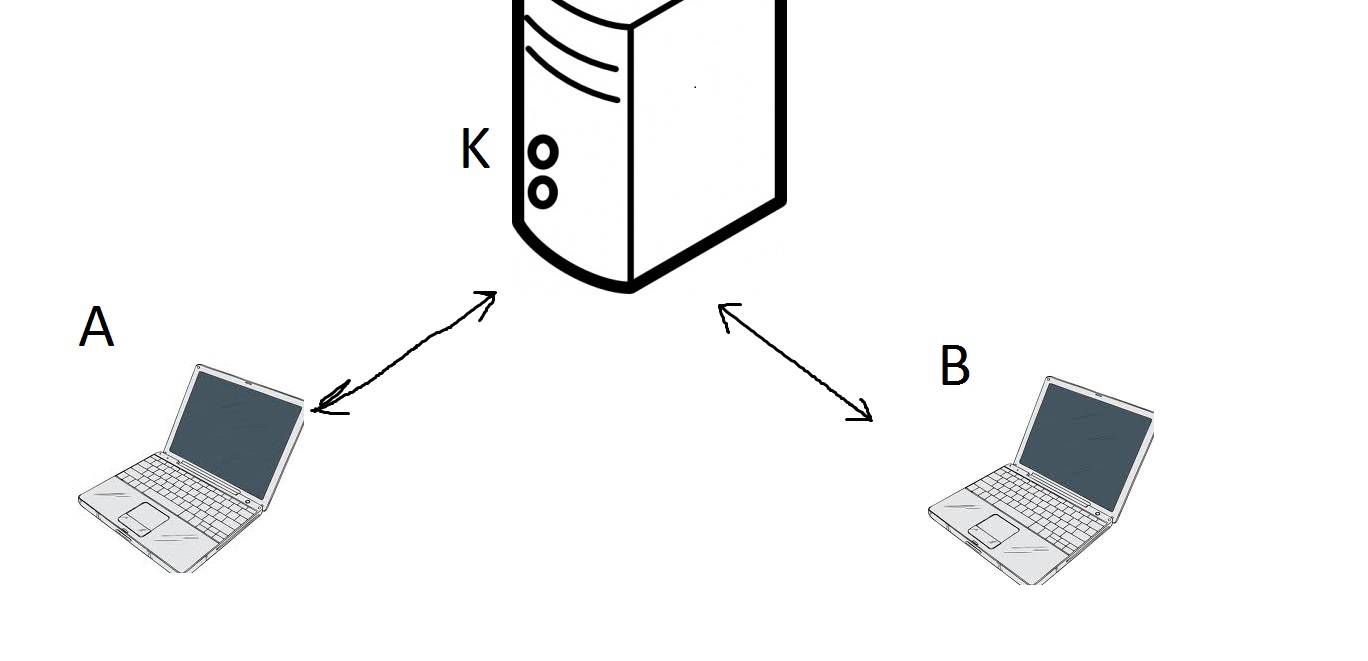
Ֆայլերը անվտանգ փողանցելու համար պետք նախ ընտրել օգտատերին ում ցանկանում եք ուղարկել: Այդպես ակտիվանում է տվյալ դաշտը: Համակարգը ավտումատ սերվերից ստանում նրա հեշավորված գաղտնաբառը: Այնուհետև օգտատերը ընտրում է այն ֆայլը որը պետք է ուղղարկի Select File կոճակի օգնությամբ: Ուղարկելու համար սեղմում ենք Send կոճակը:

Ունենալով երկու օգտատերերի հեշավորված գաղտնագրերը, կարելի է հեշտությամբ ստանալ մեկ ընդհանուր բանալի երկուսի համար:

Գաղտնագրման և վերծանման բանալինները պետք ստացվի երկու օգտատերերի գաղտնաբառերի հեշերից: Դրա շնորհիվ երկուսի մոտ էլ առկա է լինում գաղտնագրման և վերծանման բանալինները: Օգտագործելող տրամաբանական XOR-ը գեներացվում է մեկ բանալի:

**Օրինակ՝**

K=A XOR B , որտեղ K-ն դա մեր ընդհանուր, հեշերից ստացված արժեքն է , որը պահվում է սերվերում, իսկ A-ն և B-ն օգտատերերը:



Նկ.22

Բանալին ֆայլերի փոխանակման ժամանակ չի փոխանցվում, այլ փոխանցվում է բացասակայող մասը, որից հեշտությամբ կստանանք ընդհանուր բանալին:

Քանի որ ՝

A=K XOR B

B=K XOR A

Այսպիսով եթե նույնիսկ երրորդ անձը կապուղիով փոխանցման ժամանակ ստանա ֆայլերը նա չի տեսնի ոչ ուղարկվող տեղեկությունը, ոչ էլ բանալին:

Ստացող կողմի ծրագիրը անընդհատ թարմամացվում է ID-ների քանակը և նոր ID-ի տեսնելու ժամանակ հայտնում է օգտատերին և առաջարկում նեռբեռնել համակարգչի մեջ նոր ֆայլը: Օգտատերը պետք է կրկին մուտքագրի իր գաղտնաբառը որպեսզի համակարգը կատարի վերծանում և պահպանի:

**2.5 Գաղտնագրված ամպային տարածք**

Քանի որ բոլոր ֆայլերը սերվեր մուտք են գործում գաղտնագրված , ապա այն անհասանելի է ոչ իրավասու մարդկանց համար: Օգտատերը սեղմելով Cloud կոճակը կտեսնի նրա բոլոր ֆայլերը, որոնք պահված են սերվերում: Նա կարող այն նեռբեռնել համակարգիչ կամ ջնձել ընդմիշտ:

**2.6 Հիշեցումներ**

Երբ օգտատերը փոխի իր գաղտնաբառը, ապա բոլոր հին տվյալները անահասանելի կլինեն և իրեն և ում նա ուղարկել էԼ այդ իսկ պատճառով կարաջարկվի կրկին սինխրոնիզացիա կատարվի բոլոր ֆայլերի հետ կամ ոչնչացվի: Իրավասությունով ուղարկողը ավելի բարձր է, այդ իսկ պատճառով գաղտնաբառը փոփխելու դեպքում կերևա միայն տվյալ օգտատերի ուղարկածները:

**Եզրակացություն**

Այսպիսով աշխատանքի ընթացքում ուսումնասիրվեցին առկա ամպային տարածքները, նրանցում ֆայլերի փոխանցման հնարավորությունները ինչպես նաև առկա մեթոդների դրական և բացասական կողմերը: Մշակվեց նոր համակարգ որն ամպային համակարգում ապահովում է բաց կապուղիով երկու օգտատերի միջև տվյալների անվտանգ փոխանցումը, ֆայլերի հոսքային գաղտնագրում, ինչպես նաև գաղտնագրման և վերծանման գործողությունների ու բանալինների փոխանակման ավտոմատացում:

**Գլուխ 3**

Ավարտական աշխատանքի տնտեսական մասի

հաշվարկներ

Ներդրումային օբյեկտը ծրագրային համակարգ է։ Ձեռք բերման հետ կապված տվյալները ներկայացված են հետևյալ աղյուսակում, որի հիման վրա կատարվում է հաշվարկը։

1. **Ծրագրի ձեռք բերման կապիտալ ներդրումների հաշվարկը:**
2. **Ծրագրի նախագծման և արտադրության կապիտալ ներդրումների հաշվարկ**
3. **Թողարկվող արտադրանքի ինքնարժեքի հաշվարկը.**

* Նյութական ծախսեր

Փոքր հզորությունների դեպքում կորուստները կարելի է անտեսել և ընդունել Kց=Kշ=0, այդ դեպքում

* Աշխատանքի վճարման ծախսեր
* Սոցիալական ապահովագրական վճարների տարեկան գումարը
* Անուղղակի արտադրական ծախսեր
* Արտադրական ինքնարժեք
* Արտադրանքի միավորի արտադրական ինքնարժեք
* Արտադրանքի լրիվ ինքնարժեք
* Արտադրանքի միավորի լրիվ ինքնարժեք

1. **Ներդրումներից եկամուտներ և NPV-ի հաշվարկը.**

Պարզության համար ընդունենք, որ ներդրումից եկամուտների ստացումը կատարվում է հավասարաչափ։ Այդ դեպքում եկամուտների որոշման համար կունենանք.

NPV-ի հաշվարկի համար պետք է օգտվենք (5.3) բանաձևից

Ներդրումների հետգնման ժամկետը հավասար է տարիների այն թվին, որի դեպքում ներդրումներից ստացված եկամուտը հավասար է դառնում ներդրումային ծախսերին, այսինքն երբ NPV=0;

Այս բանաձևից որոշված n2-ը կլինի ներդրումների հետգնման ժամկետը: Քանի որ

Ապա ներդրումները 3 տարվա ընթացքում հետ չեն գնվում: Վերցնելով n2=4 կունենանք`

հետևաբար ներդրումների ժամկետը 4 տարի է:

Այժմ ընդունենք, որ ներդրումից եկամուտների ստացումը կատարվում է անհավասարաչափ, որը պետք է հաշվարկվի հետևյալ տվյալների համաձայն

|  |  |  |  |
| --- | --- | --- | --- |
| Տարի | Qj (հատ) | Xj (դրամ) | Cj (դրամ) |
| 1 | 1000 | 6000 | 2811 |
| 2 | 1200 | 6250 | 2450 |
| 3 | 1400 | 6800 | 1800 |
| 4 | 1650 | 6650 | 2100 |

Այս դեպքում NPV-ի որոշման համար պետք է օգտվենք (5.2) բանաձևից.

1. **Հաշվարկի տվյալները**

|  |  |  |  |
| --- | --- | --- | --- |
| Տվյալների անվանումը | Նշանակումը | Միավորը | Մեծությունը |
| Սարքավորման ձեռք բերման ներդրումների հաշվարկի տվյալներ | | | |
| Ծրագրի գնման գինը | P | դրամ | 150000 |
| Վաճառքի հարկը որոշող գործակից | σ1 |  | 0.3 |
| Տրանսպորտային ծախսերի գործակից | σ2 |  | 0.2 |
| Ներմուծման մաքսատուրքի գործակից | σ3 |  | 0.20 |
| Սարքավորման նախագծման և արտադրության ներդրումների հաշվարկի տվյալներ | | | |
| Ծրագրավորողի աշխատավարձ | A1 | դրամ | 150000 |
| Լրացուցիչ աշխատավարձի որոշման տոկոս | α1 |  | 12 |
| Ծրագրի արտադրության ժամանակը | m | ամիս | 2 |
| Աշխատավարձի տեսակարար կշռի տոկոս | d | % | 50 |
| Թողարկվող արտադրանքի ինքնարժեքի հաշվարկի տվյալներ | | | |
| Գնովի նյութերի ծախսը | Cգ | դրամ | 6000 |
| Ծրագրավորողի աշխատավաձ | A3 | դրամ | 150000 |
| Արտադրական տարածքի մակերեսը | b | մ2 | 12 |
| Ծրագրի ամորտիզացիայի ժամկետը | T | տարի | 10 |
| Ծրագրի հզորությունը | N | ԿՎտ | 1 |
| 1 ԿՎժ էլեկտրաէներգիայի սակագինը | Υ | դրամ | 38 |
| Ծրագրում հայտնաբերված սխալների թիվը | q | հատ | 2 |
| 1 նորոգման արժեքը | α2 | % | 2 |
| Իրացման ծախսերի որոշման տոկոս | α3 | % | 25 |
| Վարչական ծախսերի որոշման տոկոս | α4 | % | 15 |
| Սարքավորման ներդրումից եկամուտների և NPV-ի հաշվարկի տվյալներ | | | |
| Թողարկվող արտադրանքի տարեկան ծավալը | Q | հատ | 1000 |
| Արտադրանքի միավորի գինը | X | դրամ | 6000 |
| Ներդրումների իրականացման տարիների թիվը | n1 | տարի | 1 |
| Եկամուտների ստացման տարիների թիվը | n2 | տարի | 5 |
| Դիսկոնտի տոկոսադրույքը | r | % | 15 |
| Շահույթահարկի տոկոսադրույքը | t | % | 25 |

1. **Եզրակացություն**

Հաշվարկների արդյունքում հանգեցինք այն եզրակացության, որ NPV-ն կազմում է 7073203 դրամ։ Քանի որ

NPV>0

ապա նախագիծը ընդունվում է:

**Գլուխ 4**

**Լազերային ճառագայթման ազդեցությունը մարդու օրգանիզմի վրա**

Լազերային ճառագայթումը բոլոր կենդանի օրգանիզմների համար հանդիսանում է անսովոր գրգռիչ: Այն չի հանդիպում բնական նորմալ պայմաններում: Լազերային ճառագայթման կենսաբանական ներգործությունը կախված է ճառագայթման ինտենսիվությունից և ալիքի երկարությունից: Ալիքի երկարության ամբողջ միջակայքը դրա հետ կապված բաժանվում է մի քանի տիրույթների՝

1. Ուլտրամանուշակագույն տիրույթ՝ 180-380նմ
2. Տեսանելի լույսի տիրույթ՝ 380-780նմ
3. Մոտակա ինֆրակարմիր տիրույթ՝ 780-1400նմ
4. Հեռակա ինֆրակարմիր տիրույթ ՝ 1400նմ-ից բարձր:

Ըստ կենդանի օրգանիզմների վրա ներգործունեության տարբերվում են լազերային ճառագայթման հետևայլ տեսակները՝

* Ջերմային. կարճ ժամանակամիջոցում ոչ մեծ ծավալով զգալի քանակի ջերմության անջատում:
* Էներգետիկական. էլեկտրական դաշտի մեծ լարվածություն, որն առաջացնում է մոլեկուլների բևեռացում և այլ էֆֆեկտներ:
* Լուսաքիմիական. մի շարք պիգմենտների գունաթափում:
* Մեխանիկական. ճառագայթահարված օրգանիզմում անդրադարձայինի նման տատանումների առաջացում:
* Էլեկտրակծկում. լազերային ճառագայթման էլեկտրական դաշտում մոլեկուլի ձևափոխություն:
* Միկրոալիքային. էլեկտրամագնիսական դաշտի ձևավորում բջջի սահմաներում:

Լազերային ճառագայթման ներգործության տակ կարող են տեղի ունենալ ինչպես առանձին օրգանների խանգարումներ, այնպես էլ ամբողջ օրգանիզմի: Ընդ որում ավելի խոցելի են աչքերը և մաշկը: Ուժեղ չափով աչքի ախտահարման բնույթը կախված է ճառագայթման ալիքի երկարությունից: Աչքի հյուսվածքը 180-380նմ ալիքի երկարության ժամանակ ուլտրամանուշակագույն միջակայքում անթափանց է լազերային ճառագայթահարման համար, այդ պատճառով աչքի ախտահարումը կրում է մակերեսային այրվածքների բնույթ: Ընդ որում, սովորաբար ախտահարվում են եղջերաթաղանթը և աչքի շաղկապող թաղանթը: Այրվածքի արդյունքում առաջանում է բորբոքային գործընթաց, աչքերում ՝ խիստ այրոց:

Ուլտրամանուշակագույն ճառագայթման իմպուլսապարբերական կամ ընդհատուն ներգործության ժամանակ նկատվում է նրա ազդեցության կուտակում, որը գումարային կենսաբանական էֆֆեկտ է, ընդ որում, մոտավորապես համեմատական է ճառագայթման էներգիայի խտությանը:

Տեսանելի ճառագայթման միջակայքը 380-780նմ հանդւիսանում է աչքի համար ավելի վտանգավոր, քանի որ ազատ անցնում է աչքի օպտիկական հյուսվածքի միջով և կիզակետվում է ցանցաթաղանթի մակերևույթին: Ընդ որում ցանցաթաղանթի վրա հզորության հոսքի խտությունը կարող է լինել 45 կարգից բարձր, քան կիզակետման հաշվին աչքի եղջերաթաղանթի վրա:

Լազերի համեմատական ոչ մեծ հզորության դեպքում նկատվում է «կուրացման բռնկում» երևույթը ՝ ճառագայթման ազդեցության տակ գունաթավում է գեսողական պիգմենտները և աչքը ի որոշ ժամանակ կորցնում է իրեր տարբերելու ունակությունը: Ցանցաթաղանթի վրա 2 Ջ/սմ2 ավելի էներգիայի խտության ժամանակ տեղի է ունենում ցանցաթաղանթի այրվածք: Ախտահարված տեղի զգայունությունը լույսի նկատմամբ լիովին կորչում է և հետագայում չի վերականգնվում: Լազերային ճառագայթի էներգիան, որը ընկնում է աչքի մեջ, կախված է աչքի բիբի տրամագծից, ոևն էլ կախված շրջապատող առարկաների լուսավորումից, փոխվում է 1.6-2-ից մինչև 7-8մմ: Ըբդ որում էներգիան, որը ընկնում է աչքի մեջ, փոխվում է 15-20 անգամ:

Այսպիսով լազերային ճառագայթումը ավելի վտանգավոր մութ տեղերում: Ինֆրակարմիր միջակայքի հեռավոր մասի լազերային ճառագայթումը 780-1400նմ ավելի երկարությամբ բավականին լավ անցնում է աչքի օպտիկական հյուսվածքի միջով, ընդ որում, հնարավոր է ցանցաթաղանթի այրվածք: Այս միջավայրի ճառագայթումը հատկապես վտանգավոր է, քանի որ այն աչքի համար անտեսանելի է: 1.4մկմ-ից ավելի ալիքի երկարության ժամանակ ճառագայթումը կլանվում է հյուսվածքներում, որոնք ջուր են պարունակում(եղջերաթաղանթ, ակնաբյուրեղ և աչքի առջևի խոռոչում եղած հեղուկը), և չի հասնում ցանցաթաղանթին: Հատկապես ուժեղ տաքանում է այդ դեպքում ծիածանաթաղանթը, որը պարունակում է գունյանութ: 4 Ջ/սմ2 ավելի էներգիայի խտության ժամանակ տեղի է ունենում ջերմային այրոց, որը կարող է հանգեցնել ակնաբյուրեղի պղտորման: 1700 նմ-ից ավելի երկարությամբ լազերային ճառագայթումը ամբողջովին կլանվում է եղջերաթաղանթում և հյուսվածքներում: Հզոր չափերի ճառագայթումը կարող է առաջացնել եղջերաթաղանթի լուրջ այրոցներ:

Մաշկի ախտահարումը սովորաբար նկատվում է դեմքի վրա պաշտպանիչ ակնոցների շուրջը, ձեռքերի արտաքին մակերևույթին, օձիքի գծից վերև, ավելի ճիշտ այն տեղերում, որոնք ենթարկվում են արևային ճառագայթահարման: Մաշկի վրա ավելի ուժեղ է ազդում ուլտրամանուշակագույն միջակայքի ճառագայթումը: Ուլտրամանուշակագույն ճառագայթահարման համեմատական ոչ մեծ չափաբաժիններն առաջացնում են կարմրություն, որն անցնում է հաջորդ օրերի ընթացքում: Ավելի հզոր ճառագայթումը հանգեցնում է մոլեկուլների քայքայմանը, որոնք մտնում են հյուսվածքների կազմի մեջ: Տեսանելի և ինֆրակարմիր ճառագայթումների ներգործությունը հանգեցնում է հիմնականում մաշկի տաքացմանը , և կարող է հասցնել այրվածքների, որոնք ունեն կտրուկ գծված սահմաններ և հիշեցնում են սովորական ջերմային այրվածքներ:

Մարդու մաշկը բավականին լավ է դիմակայում անընդհատ ինֆրակարմիր ճառագայթմանը, քանի որ այն ընդունակ է արյան շրջանառության շնորհիվ տարածել ջերմությունը և մակերևույթից իջեցնել ջերմաստիճանը խոնավության գոլորշիացման հետևանքով: Իմպուլսային ճառագայթումը, և հատկապես լազերային ճառագայթումը, ավելի վտանգավոր է մաշկի համար, քանի որ ջերմությունը չի հասցնում տարածվել հարևան հյուսվածքներում: Այս դեպքում առաջանում են կտրտված սահմաններով այրվածքներ, հյուսվածքների սահմանափակ մահացած օջախներ, շիճահեղուկով լցված պղպջակներ: 3-100Ջ էներգիայով լազերների ճառագայթման ազդեցության տակ առաջանում են տարբեր չափերի արյունազեղումներ: 3Ջ-ից քիչ էներգիայով ճառագայթման ժամանակ մաշկի կառուցվածքային փոփոխություն չի նկատվում, բայց տեղի է ունենում ֆերմենտների գործունեության խանգարումներ: Դա նվազեցնում է մաշկի հակամանրէային դիմադրողականությունը, վատացնում է նրա սնուցումը և բարձրացնում է նրա զգայությունը բարձր ջերմաստիճանի նկատմամբ: Ֆերմենտների գործունեության խանգարումները մաշկի մեջ կարող են հանգեցնել թունավոր նյութերի ձևավորմանը, որոնք, տարածվելով ողջ օրգանիզմով, վատացնում են մարդու ընդհանուր վիճակը՝ առաջացնելով հոգնածության զգացում, գրգռվածություն, գլխացավ: Այս տհաճ երևույթները կարող են պահպանվել աշխատանքային օրվա ավարտից մի քանի ժամվա ընթացքում: Լազերային սարքավուրումով աշխատող մարդկանց մոտ հայտնաբերվել է արյան կազմության փոփոխություն. այն արտահայտվում հեմոգլոբինի, տրոմբոցիտների, էրիտրոցիտների և լեյկոցիտների քանակի նվազեցմամբ:

Համաձայն CH51045804-91 «Լազերներին օկտագործման և սարքավորումների առողջապահական չափորոշիչների և կանոնների» ՝ բոլոր լազերային սարքավորումները ստորաբաժանվելու են 4 կարգի՝ ըստ մարդու օրգանզիմի համար լազերային ճառագայթման վտանգավորության աստիճանի.

1-ին կարգին պատկանում են այն լազերները, որոնց ճառագայթումը վտանգավորություն չի ներկայացնում մարդու ո՛չ մաշկի և ո՛չ աչքերի համար:

2-րդ կարգին պատկանում են այն լազերները, որոնց ճառագայթումը վտանգավորություն է ներկայացնում աչքերի և մաշկի համար ուղիղ կամ հայելիով անդրադարձած ճառագայթով ճառագայթահարման ժամանակ:

3-րդ կարգին պատկանում են այն լազերները, որոնց ճառագայթումը վտանգավորություն է ներկայացնում աչքերի համար ցրված, անդրադարձած ճառագայթով ճառագայթահարման ժամանակ անդրադարձնող մակերևույթից 10սմ-ից ավել հեռավորության վրա:

4-րդ կարգին պատկանում են այն լազերները, որոնց ճառագայթումը վտանգավորություն է ներկայացնում մաշկի և աչքերի համար ցրված, անդրադարձած ճառագայթով ճառագայթահարման ժամանակ անդրադարձնող մակերևույթից 10սմ ավել հեռավորության վրա:

Լազերի կարգը սահմանվում է արտադրող ձեռնարկության կողմից: լազերների բաժանումը կարգերի թույլ է տալիս տարբեր տեսակի լազերներով աշխատելու ժամանակ հստակ որոշել անվտանգության միջոցառումները:

Լազերային ճառագայթումը միակ վտանգավորությունը չի: Տեխնիկական պարամետրերից և շահագործման պայմաներից կախված՝ սպասարկող անձնակազմի վրա կարող են ազդել նաև հետևյալ կողմնակի և վնասակար արտադրական գործոնները՝

* Լազերային սարքավորումներում բարձր լարման էլեկտրասնուցումը,
* Մղման իմպուլսային լամպերի շատ բարձր պայծառությունը, որոնց էներգիան իր հերթին բարձրացնում է լազերի ճառագայթման էներգիան,
* Աշխատանքային գոտում օդի բարձր փոշոտվածությունը,խոնավապարունակությունը, լազերային ճառագայթներ, կլանող նյութերի առկայությունը:
* Իոնացնող ճառագայթումը,
* Ուլտրամանուշակագույն ճառագայթումն, մղման իմպուլսային լամպերից կամ քվանտային գազապարպող խողովակներից,
* Բարձր հաճախականության և ՀԹՃ գերբարձր հաճախականության միջակայքերի էլեկտրամագնիսական ճառագայթումը,
* Սարքավորումների մակերևույթների բարձր ջերմաստիճանը և ինֆրակարմիր ճառագայթումը,
* Աշխատանքային վայրում աղմուկի և վիբրացիայի բարձր մակարդակը, որն առաջանում է լազերային սարքավորմներով աշխատելիս,
* Հրդեհի և պայթյունավտանգավորության բարձրացումը, որը պայմանավորված է վառվող նյութերի լազերային ճառագայթի հարվածելու հնարավորությունից:

Բոլոր թվարկված կողմնակի գործոններն առավել ուժգին են արտահայտվում 4-րդ կարգի լազերային սարքավորումների աշխատանքի ժամանակ, բայց կարող են հանդիպել նաև 3-րդ կարգի սարքավորումների ժամանակ:

«Լազերներին օկտագործման և սարքավորումների առողջապահական չափորոշիչները և կանոնները» հանդիսանում է լազերային ճառագայթի հաստատված սահմանային թույատրելի մակարդակի հիմնական փաստաթուղթ: Համաձայն այս փաստաթղթի՝ ներգործության սահմաների թույլատրելի մակարդակը որոշելու համար օգտագործում են ճառագայթման հետևյալ պարամետրերը.

Իմպուլսային կամ կարճատև ներգործության ժամանակ, երբ գումարային կենսաբանական էֆեկտը որոշվում է ճառագայթման հիմնական ընդհանուր էներգիայով, նորմավորվում է ըստ ճառագայթման էներգիա հոսքի խտության:

Տեսանելի լույսով աչքի կարճատև ճառագայթահարման ժամանակ նորմավորվում է W լազերային էներգիան, Ջ, որը 7մմ տրամագծով բացվածքի վրա ընկնող էներգիան է: Երկարատև ճառագայթման ժամանակ երբ օրգանիզմը հարմարվում է լազերային ճառագյթման ազդեցությանը, նորմավորվում է ճառագայթման հոսքի խտությունը:

Տեսանելի լույսով աչքի երկարատև ճառագայթահարման ժամանակ նորմավորվում է ճառագայթան հզորությունը P (7մմ տրամագծով բացվացքի վրա ընկնող ճառագայթման հզորությունը):

**Գլուխ 5**

**Աշխատանքի պայմաններում դժբախտ պատահարների հետազոտումը**

Ամեն մարդու համար շատ կարևոր է իմանալ, որ այն վայրը, որտեղ նա աշխատում է համապատասխանում է բոլոր ստանդարտներին: Քանի որ ցանկացած աշխատատեղում կարող են լինել դժբախտ պատահարներ,մենք պարտավոր ենք իմանալ բոլոր վնասակար գործոնները և դրանցից պաշտպանվելու միջոցները:

Դժբախտ պատահարները տեղի են ունենում աշխատանքի պայմաններում, երբ ստեղծվում են մարդկանց կյանքի կամ տեխնոլոգիական սարքավորումների համար վտանգավոր իրադարձություններ: Դրանց պատճառը կարող է հանդիսանալ մեքենաների անսարքությունը, տեխնոլոգիական պրոցեսների խախտումները, աշխատանքային սխալ գործողությունները կամ անբարենպաստ պայմանները, աշխատանքային կարգապահության խախտումները և այլն:

Հաճախ վտանգավոր պահեր կարող են ստեղծվել սարքավորումների կոնստրուկտիվ թերությունների, աշխատանքի սխալ կազմակերպման, մարդկանց հոգնածության և այլ պատճառներով: Նշված վտանգավոր իրադրությունները կարող են հանգեցնել դժբախտ պատահարների:

Պատահարներ են կոչվում այն դեպքերը, որոնց ընթացքում արտաքին գործոնների անսպասելի ներգործությամբ վնասվում է մարդու օրգանիզմը կամ խախտվում առողջությունը:

Պատահարի հետևանքով առաջացած այն վնասվածքները, որոնք ստանում է մարդը իր աշխատանքային պարտականությունները կատարելիս, անկախ նրանից, թե դա տեղի է ունեցել աշխատավայրում, և թե դրանից դուրս, կոչվում են արտադրական:

Վնասվածքները կարող են լինել կոտրվածքների, վերքերի, ջերմային կամ քիմիական այրվածքների, ցրտահարման, էլեկտրական վնասվածքների, ճառագայթման ազդեցության և այլ ձևերով:

Վնասվածքները լինում են.

* թեթևակի, երբ աշխատողը չի կորցնում աշխատունակությունը և չի թողնում աշխատանքը,
* թեթև` աշխատունակության ժամանակավոր կորստով,
* ծանր` աշխատունակության մասնակի կամ լրիվ անվերադարձ կորստով
* մահացու:

Հնարավոր են ինչպես անհատական, այնպես էլ խմբային վնասվածքներ:  
 Արտադրական վնասվածքները կարող են հանգեցնել նաև համակարգիչների, տեխնիկայի, և այլ սարքավորումների խափանման մասնակի և նույնիսկ լրիվ կործանման` առանց մարդկային զոհերի: Նման դեպքերը դիտվում են որպես վթարներ: Պետք է նկատել, որ վթարների մեծ մասը սպառնալից վտանգ են ներկայացնում մարդկանց կյանքին, ուստի դրանց կանխումը աշխատանքի պահպանության առաջնահերթ խնդիրներից մեկն է: Հնարավոր են նաև այնպիսի իրադրություններ, երբ տեխնոլոգիական պրոցեսները կամ աշխատանքի անբարենպաստ պայմանները ստեղծում են մարդկանց առողջության վրա բացասաբար ազդող երկարատև գործոններ, որոնց հետևանքով կարող են առաջանալ որոշակի հիվանդություններ:

Քիչ չեն դեպքերը, երբ պատահարների ու հիվանդությունների պատճառ են դառնում կազմակերպչական բնույթի թերությունները, ինչպես օրինակ աշխատասենյակի սխալ ընտրությունը, տեխնիկայի սխալ միացումները և նրանց սխալ օգտագործումը, սանիտարահիգենիկ միջոցառումների անբավարարությունը և այլն:

Աշխատասենյակում, որտեղ կատարվում է աշխատանքը, պետք է ապահովել անհրաժեշտ սանիտարահիգենիկ պայմաններ:

Պատահարների հաշվառման ու հետաքննման կարգը պարտադիր է բոլոր կազմակերպությունների համար: Հետաքննման ենթակա են բոլոր այն պատահարները, որոնց հետևանքով աշխատողը կորցնում է աշխատունակությունը ոչ պակաս մեկ օրից և եթե դրանք տեղի են ունեցել.

* Կազմակերպության տարածքում
* Կազմակերպության տարածքից դուրս, կազմակերպության կողմից տրված առաջադրանքը կատարելիս, ինչպես նաև կազմակերպության կողմից հատկացված փոխադրամիջոցներով աշխատանքի գալիս կամ վերադառնալիս:

Պատահարը ենթակա է հետաքննության, եթե այն տեղի է ունեցել տոնական կամ հանգստյան օրերին կատարված աշխատանքի ընթացքում:

Յուրաքանչյուր պատահարի դեպքում տուժողը կամ մոտիկ ականատեսը պարտավոր է կատարվածի մասին անմիջապես հաղորդել աշխատանքի ղեկավարին:

Եթե պատահարը տեղի է ունեցել աշխատանքի վայրում, ղեկավարը ստանալով պատահարի լուրը, պարտավոր է անմիջապես կազմակերպել տուժածին ցույց տրվող առաջին օգնությունը, հնարավորին չափ կարգավորելով աշխատատեղում ստեղծված իրավիճակը: Միաժամանակ նա պարտավոր է պատահարի մասին անմիջապես հաղորդել աշխատանքի համապատասխան ղեկավարին, ով և պարտավոր է`

* Պատահարի մասին անմիջապես հաղորդել կազմակերպության ղեկավարին,
* Աշխատանքի պաշտպանության հասարակական հսկչի ու կազմակերպության անվտանգության ինժեների հետ միասին 24 ժամվա ընթացքում հետաքննել պատահարը, կազմել սահմանված ձևի ակտ և ուղարկել ձեռնարկության ղեկավարին, նա հաստատում է հիշյալ ակտը և համապատասխան կարգադրություններ է անում պատահարի պատճառները վերացնելու վերաբերյալ: Տուժածի աշխատունակության ժամկետը ավարտվելուց հետո ղեկավարը վերոհիշյալ հասցեներով տեղեկություններ է ուղարկում պատահարի պատճառած նյութատեխնիկական վնասների մասին:

Եթե պատահարի հետևանքով տուժել են երկու կամ ավել աշխատողներ, մարդկային զոհի կամ ծանր վնասվածքի դեպք է եղել, ապա ձեռնարկության ղեկավարը պարտավոր է անմիջապես հայտնել վերադաս ղեկավարությանը, կենտրոնական խորհրդին, տեղի դատախազությանը:

Կատարվում է հետաքննություն, կազմված ակտը, տեխնիկական վերահսկիչի եզրակացության և հետաքննության մյուս նյութերի հետ յոթ օրվա ընթացքում ուղարկվում են տեղի դատախազություն և վերադաս ղեկավար կազմակերպություն:

Համապատասխան մարմինները սահմանված ձևի հաշվառման մատյաններում գրանցում են բոլոր ծանր, մահացու և խմբակային պատահարները:

Վթարների հետևանքով տեղի ունեցած բոլոր դժբախտ պատահարները, անկախ նրանց ծանրության աստիճանից, պետք է քննարկվեն համապատասխան ատյանների նիստերում:

Վերլուծելով ծանր, մահացու և խմբակային պատահարների հետաքննման նյութերը համապատասխան նախարարությունը ցուցումներ է տալիս ստորադաս կազմակերպություններին հետագայում պատճառները կանխելու համար:

Անկախ պատահարի ծանրության աստիճանից և տուժածների թվից, յուրաքանչյուր տուժածի համար կազմվում է առանձին ակտ:

Պատահարները և հիվանդությունները կանխելու համար անհրաժեշտ է բազմակողմանի ուսումնասիրության միջոցով պարզել դրանց առաջացման պատճառները և վերացման հնարավորությունները: Այդ ուսումնասիրությունների համար ընդունված է կիրառել հետևյալ մեթոդները.

1. Վիճակագրական մեթոդ, որով կատարվող հետազոտությունների համար հիմք են հանդիսանում տեղի ունեցած պատահարների վիճակագրական տվյալները, որոնք վերցվում են ակտերից: Հետևաբար վիճակագրական մեթոդներից կարող են օգտվել խոշոր կազմակերպություններն ու անվտանգության տեխնիկայի ինժեները, պետական վերահսկողության մարմինները և այլն:

Հետազոտությունները կատարվում են հետևյալ հաջորդականությամբ .

* Անհրաժեշտ տվյալների հավաքում,
* Դրանց մաթեմատիկական վերամշակում
* Ստացած արդյունքների վերլուծում:

Վիճակագրական մեթոդներով կարող են ճիշտ եզրակացությունների հանգել միայն նախնական ստույգ տվյալների առկայության դեպքում, ուստի այդ տվյալները պետք է մանրազնին ստուգվեն:

Վիճակագրական տվյալների մշակման էությունն այն է, որ ակտավորված պատահարները խմբավորվում են ըստ որևէ հատկանիշի. Օրինակ` ըստ տուժածների սեռի, մասնագիտության, տարիքի, աշխատանքային ստաժի, աշխատանքի բնույթի կամ ըստ պատահարի պատճառի, տեղի և այլն: Այնուհետև այդ խմբերի վերաբերյալ ստացված տվյալները գրանցվում են համապատասխան աղյուսակներում:

Համեմատելով և վերլուծելով աղյուսակներում նշված վիճակագրական տվյալները, պարզվում են պատահարների առաջացման պատճառները և դրանց օրինաչափությունները:

1. Մոնոգրաֆիկ մեթոդ, որի դեպքում մանրակրկիտ հետազոտվում է որևէ կազմակերպության գործընթացը, տեղակայքը, աշխատանքային տեղը, աշխատանքային միջավայրը, փոխադրական միջոցը, մարդկանց հանգստի կազմակերպման պայմանները և այլն: Հետազոտումը կատարվում է ոչ միայն եղած, այլ սպասվելիք հնարավոր պատահարների կամ վթարների պատճառները հայտնաբերելու և վերացնելու նպատակով: Այս մեթոդը մոնոգրաֆիկ է կոչվում, որովհետև ուսումնասիրվում և մանրամասն պարզաբանվում է որևէ մեկ կոնկրետ պատճառ, որը առիթ է հանդիսացել բազմաթիվ դժբախտ դեպքերի:
2. Տեղագրական մեթոդ, որի առանձնահատկությունն այն է, որ պատահարները հետազոտվում են ըստ առաջացման տեղի: Եթե պատահարները կրկնվում են համակարգչային սրահներում, լաբորատորիաներում, նշանակում է դրանց պատճառը պետք է փնտրել այդտեղ եղած սարքավորումների անսարքության, աշխատանքային մեթոդների կամ պաշտպանական միջոցների անբավարարության մեջ:
3. Տեխնիկական մեթոդը կիրառվում է այն դեպքում, երբ պատահարների, հիվանդությունների ու վթարների առաջացումը անմիջականորեն կախված է տեխնիկական սարքավորումների հուսալիության, որակի և անխափան աշխատանքի ապահովման մեջ:

Սարքավորումների այդ հատկությունները ստուգվում են ինժեներական հաշվարկների և փորձարկումների միջոցով:

**Գրականություն ցանկ**

* *Баричев С.Г., Гончаров В.В., Серов Р.Е.* 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — С. 30—35. — (Специальность. Для высших учебных заведений). — 3000 экз. — [ISBN 5-93517-075-2](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/5935170752)
* ***Шнайер Б.*** [Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си](http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm) = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: [Триумф](http://ru.wikipedia.org/w/index.php?title=%D0%A2%D1%80%D0%B8%D1%83%D0%BC%D1%84_(%D0%B8%D0%B7%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE)&action=edit&redlink=1), 2002. — 816 с. — 3000 экз. — [ISBN 5-89392-055-4](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/5893920554)
* *Мэтью Мак-Дональд* WPF: Windows Presentation Foundation в .NET 3.5 с примерами на C# 2008 для профессионалов = Pro WPF in C# 2008: Windows Presentation Foundation with .NET 3.5. — 2-ое. — М.: [«Вильямс»](http://ru.wikipedia.org/w/index.php?title=%D0%92%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC%D1%81_(%D0%B8%D0%B7%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE)&action=edit&redlink=1), 2008. — С. 25. — 928 с. — [ISBN 978-5-8459-1429-3](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/9785845914293)
* Andrew Troelsen. Pro C# 5.0 and the .NET 4.5 Framework
* SQL в примерах и задачах; Учеб. пособие / И.Ф. Астахова, А.П. Тол-стобров,В.М. Мельников.— Мн.: Новое знание, 2002. — 176 с.
* Шилдт, Герберт. Ш57 С# 4.0: полное руководство. : Пер. с англ. — М. : ООО "И.Д. Вильяме", 2011. — 1056 с.: ил. — Парал. тит. англ. ISBN 978-5-8459-1684-6 (рус.)