

Сериал түлхүүрийн судалгаа

Гүйцэтгэсэн: Э. Сарангэрэл
Оюутны код: 16b1seas0696

Улаанбаатар хот 2020 он

Гарчиг

1. Ерөнхий хэсэг

1.1 Удиртгал

1.2 Зорилго

2. Сериал түлхүүрийн тухай

2.1 Сериал түлхүүрийн тухай

2.2 Ашиглагддаг алгоритм

2.3 Програм хангамжийн лицензийн тухай

2.4 Лицензийн загвар

2.5 Лицензийн төрөл

3. Судалгааны хэсэг

3.1 Цуваа түлхүүр үүсгэх болон Java-ийн баталгаажуулалт

3.2 Шилдэг үйлдвэрлэгч

3.3 Сериал түлхүүр үүсгэгч вэбсайт

4. Ерөнхий дүгнэлт

5. Ашигласан материал

Зургийн жагсаалт

- 2.1 Шифрлэлт хийх үйл явц
- 2.2 Google сайтын Windows 8.1 програмын хайлтын үр
- 3.1 Санамсаргүйгээр цуваа түлхүүрийг үүсгэх
- 3.2 MD2,MD5,SHA1 тулгуурлан хэш үүсгэх
- 3.3 Төрлөөс хамааран оролтын тэмдэгт мөрийг хэш үүсгэх
- 3.4 Цуваа түлхүүрийн 18 хэш сонгож авах
- 3.5 Хэрэглэгчийн нэрээр цуваа түлхүүр үүсгэх
- 3.6 Хэрэглэгчийн нэрээр цуваа түлхүүр үүсгэсэн үр дүн
- 3.7 serials.ws сайтын бүтэц
- 3.8 serialbay.com сайтын бүтэц
- 3.9 keygenninja.com сайтын бүтэц
- 3.10 smartserials.com сайтын бүтэц

I. Ерөнхий хэсэг

1.1 Удиртгал

Орчин үед лицензтэй програм нь нэр хүнд болон найдвартай ажиллагаа нь ихээхэн чухал билээ. Энэ бие даалтын ажлаар сериал түлхүүрийн судалгааг хийсэн ба сериал түлхүүр ашигласнаар зөв хүнд албан ёсны лицензтэй аюулгүй найдвартай ажиллах програмыг санал болгож байна. Лицензийн үйлдвэрлэгч болгон өөр өөр сериал түлхүүрийг ашигладаг ба үүсгэхдээ криптографийн хэш функцуудыг ашигладаг учраас тайлж уншихад төвөгтэй юм.

1.2 Зорилго

Бие даалтын хүрээнд лицензийн сериал түлхүүр бүтэц, ашигладаг алгоритм болон төрөл, үйл ажиллагааг судлах зорилготой.

II. Сериал түлхүүрийн тухай

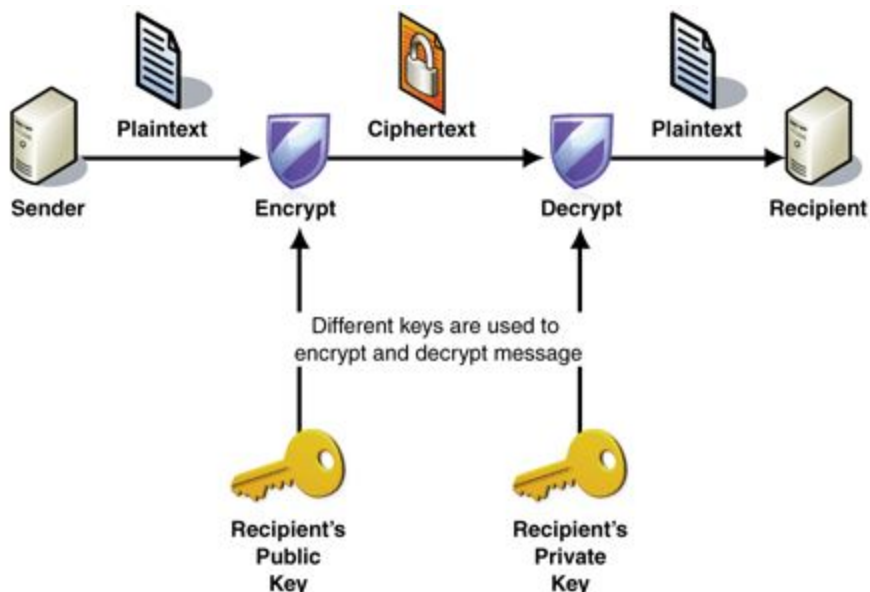
2.1 Сериал түлхүүрийн тухай

Сериал түлхүүр нь компьютерийн тусгай програм хангамжийн түлхүүр юм. Компьютерийн програм хангамж болон тоглоомууд нь зөвшөөрөлгүйгээр хуулбарлахгүй байхын тулд цуваа түлхүүрийг ашигладаг. Цуваа түлхүүр нь тоонууд болон / эсвэл үсгийн дарааллаас бүрдэнэ. Энэ дараалал нь ихэвчлэн компьютерийн програм хангамжийг суурилуулах явцад хэрэглэгчийн оруулсан бөгөөд дараа нь програмын баталгаажуулалтын функцруу шилждэг. Энэ функц нь түлхүүр дарааллыг математикийн алгоритмтай нийцүүлэн хянадаг бөгөөд үр дүнг харьцуулдаг. Интернетийн өсөлтөөс үүсэх халдлагууд (түлхүүрийн хэрэгцээг багасгах) нийтлэг болжээ. Үүний улмаас програм хангамжаа зохиогч нь түлхүүрүүд нь үнэн зөв, найдвартай гэдгийг баталгаажуулах өөр аргуудыг улам ихэсгэж байна. Нэг арга, бүтээгдэхүүний баталгаажуулалт нь хэрэглэгчийн компьютерийн техник хангамжийн (түүний MAC хаяг гэх мэт) өвөрмөц онцлог дээр үндэслэсэн цуваа түлхүүрийг үүсгэдэг бөгөөд энэ нь хэрэглэгчийн тоног төхөөрөмжөөс шалтгаалан хялбархан давтагдах боломжгүй байдаг. Бусад шинэ аргууд нь CD түлхүүрийг интернетийн сервертэй тогтмол хугацаанд баталгаажуулахыг шаарддаг (интернетийн бүрэлдэхүүн хэсэгтэй тоглоомуудын хувьд энэ нь хэрэглэгч нэвтрэх бүртээ хийгддэг). Баталгаажуулалтыг серверийн тал дээр гүйцэтгэж, халдлага үүсэхээс сэргийлж (хэрэглэгч талдаа хийж байх үед) тэдгээрийг хандалтыг хаах болно.

2.2 Ашиглагддаг алгоритм

Криптографийн хувьд шифрлэлт нь зөвхөн эрх бүхий талуудад хандах боломжтой мессеж, мэдээллийг кодлох үйл явц юм. Шифрлэлт нь мэдээллийг нууцлах тусгай түлхүүртэй бол нууц мэдээллийг задлах боломжгүй болгодог. Шифрлэх нь таны мэдээллийг хамгаалах арга юм. Шифрлэлтийн үндсэн зорилго нь: Компьютерын системд хадгалагдаж буй интернэт эсвэл бусад компьютерын сүлжээгээр дамжуулагдсан дижитал мэдээллийн нууцлалыг хамгаалахад оршино. Шифрлэлтийн схемд, төлөвлөсөн мэдээлэл буюу мессеж нь plaintext (ил бичвэр) гэж нэрлэгддэг шифрлэлтийн алгоритмаар шифрлэлтийг бий болгох шифрлэгдсэн кодыг ашиглан уншигдах боломжтой. Техникийн шалтгаанаар шифрлэлтийн схем нь ихэвчлэн алгоритмаас үүссэн псевдо-санамсаргүй шифрлэлтийн түлхүүрийг ашигладаг. Түлхүүр эзэмшихгүйгээр мессежийг код тайлах аргын зарчмаар хэрэглэх боломжтой боловч сайн боловсруулсан шифрлэлтийн

схемийн хувьд тооцооллын нөөц, ур чадвар шаардагдаж байна. Криптографийн хэш функцууд нь тоон гарын үсэг,цуваа түлхүүрд өгөгдлийн бүрэн бүтэн байдлыг шалгах гэх мэт аюулгүй байдлын олон асуудлаар өргөн хэрэглэгддэг.



Аюулгүй криптографын хэш функцийн гол шинж чанарууд нь:

- Түлхүүрийн урт нь оролттой харьцуулахад бага байдаг.
- Тооцоолол нь хурдан, үр ашигтай байдаг.
- Оролтын аливаа өөрчлөлт нь гаралтын битүүдийн олонхид нөлөөлдөг.
- Оролтыг гаралтаас тодорхойлж болохгүй.
- Хоёр янзын оролт нь ижил гаралт үүсгэж чадахгүй гэх мэт чанарууд багтана.

Мессеж болон файлуудын бүрэн бүтэн байдлыг шалгах

Аюулгүй байдал нь өгөгдлийн бүрэн бүтэн байдлыг шалгах явдал юм. Урьдчилан тооцоолох мессежийг (мессежийн хэшийг боловсруулсан) харьцуулж, дараа нь дамжуулалт нь мессеж эсвэл файлд ямар нэгэн өөрчлөлт хийгдсэн эсэхийг тодорхойлох боломжтой. MD5, SHA1, эсвэл SHA2 хэш боловсруулалт нь татаж авсан файлуудад бүрэн бүтэн байдлыг шалгах боломжийг вэбсайт эсвэл форумд илгээдэг. Криптографын хэш, найдвартай сүлжээ ашиглан файлын хортой өөрчлөлтөөс сэргийлдэг.

Зурвасын баталгаажуулалт

Шифрлэлт нь мессежийн нууцыг хамгаалах боломжтой боловч мессежийн бүрэн бүтэн байдал, үнэн зөв байдлыг хамгаалахын тулд бусад арга техник хэрэгтэй хэвээр байна. Жишээлбэл, мессежийг таних код (MAC) буюу тоон гарын үсгийн баталгаажуулалт. Шифрлэлтийн төхөөрөмж зөвхөн өөрөө өөрчлөгдөөгүй бол үүсгэх үед шифрлэх нь аюулгүй байдаг.

Криптографийн хэш функцийн төрөл

MD5

MD5-ийг 1991 онд Ronald Rivest-ээр боловсруулсан бөгөөд MD4 хэш функцыг 1992 онд RFC 1321 гэж тодорхойлсон. MD5-тай мөргөлдөөнийг хэдхэн секундын дотор тооцоолж болох бөгөөд энэ нь криптографын хэш шаардагдах ихэнх тохиолдолд алгоритмыг ашиглахад тохиромжтой. MD5 нь 128 бит (16 байт) -г боловсруулдаг.

SHA-1

160 бит хэш функц. NSA-с тоон гарын үсгийн алгоритмын хэсэг болгож загварчилсан. Оролт нь 264 битээс бага мессеж, гаралтанд нь 160 битийн мессежгарна. Энэхүү стандартын хүрээнд аюулгүй байдлыг нээж илгээх турш SHA-384 ба SHA-512 алгоритмууд нь аюулгүй байдлын хамгаалалтаар хамгийн өндөрт байдаг.

SHA-2:

Өөр өөр блокуудтай 2 ижил хаш функцийн бүлэг юм. SHA-256, SHA-512 SHA-256 нь SHA-1 ба MD4, MD5-н аргаар үйл ажиллагаа явуулдаг. SHA-256 шахалтын функц нь 256 битийн завсрын хэш утга ба 512 битийн мессежийн блок дээр ажилладаг. Энэ нь үндсэндээ 256 битийн блок шифрлэлтийн алгоритм юм. SHA-224, SHA-384, SHA-512/224 ба SHA-512/256 гэсэн тус бүрийн стандарт байдаг. Эдгээрийг NSA зохион бүтээсэн. 2 гол бүрэлдэхүүн хэсэгтэй. 1. SHA-256 шахалтын функц 2. SHA-256 мессежний хуваарь SHA-256 нь 32 битийн үсэгт ашиглагдана.

SHA-3

Одоо ажиллаж буй NIST hash competition функцийн хувилбарт санал болгосон хэш функцийн стандарт. 2012 оны 10 сард SHA-3 гэсэн шинэ стандартыг бий болгосон. Тоон гарын үсэг болон хэш дээр суурилсан MACs, PRFs, RNGs, KDFs-г дэмждэг. Аюулгүй байдлын хувьд маш өндөр нарийвчлалтай. SHA-3 нь SHA3-224, SHA3-256, SHA3-384 ба SHA3-512

гэсэн 4 криптографын хэш функцээс бүрдэнэ. SHA-512 шахалтын функц ба SHA-512 мессежийн хуваарьтай.

Криптографийн хэш функцийн үйл ажиллагааны харьцуулалт

Хүснэгт 2.1. Хэш алгоритмуудын харьцуулалт

Алгоритм болон вариант	Гаралтын хэмжээ (bits)	Дотоод байдлын хэмжээ (bits)	Блокын хэмжээ (bits)	Хамгийн их мессежийн хэмжээ (bits)	Үгийн хэмжээ (bits)	Rounds	Үйл ажиллагаа	Онолын дүгнэлт
MD5	128	128	512	$2^{64} - 1$	32	64	+, and, or, xor, rot	yes
SHA 0	160	160	512	$2^{64} - 1$	32	80	+, and, or, xor, rot	yes
SHA 1	160	160	512	$2^{64} - 1$	32	80	+, and, or, xor, rot	Theoretical халдлага (2^{60})
SHA 2 -> SHA224 SHA256	224, 256	256	512	$2^{64} - 1$	32	64	+, and, or, xor, rot	Дурын
SHA 2 -> SHA384, SHA512, SHA512/224, SHA521/256	384, 512, 224, 256	512	1024	$2^{128} - 1$	64	80	+, and, or, xor, rot	Дурын
SHA3	224/256/384/ 512	1600			64	24	and, or, xor, rot	Дурын

2.3 Програм хангамжийн лицензийн тухай

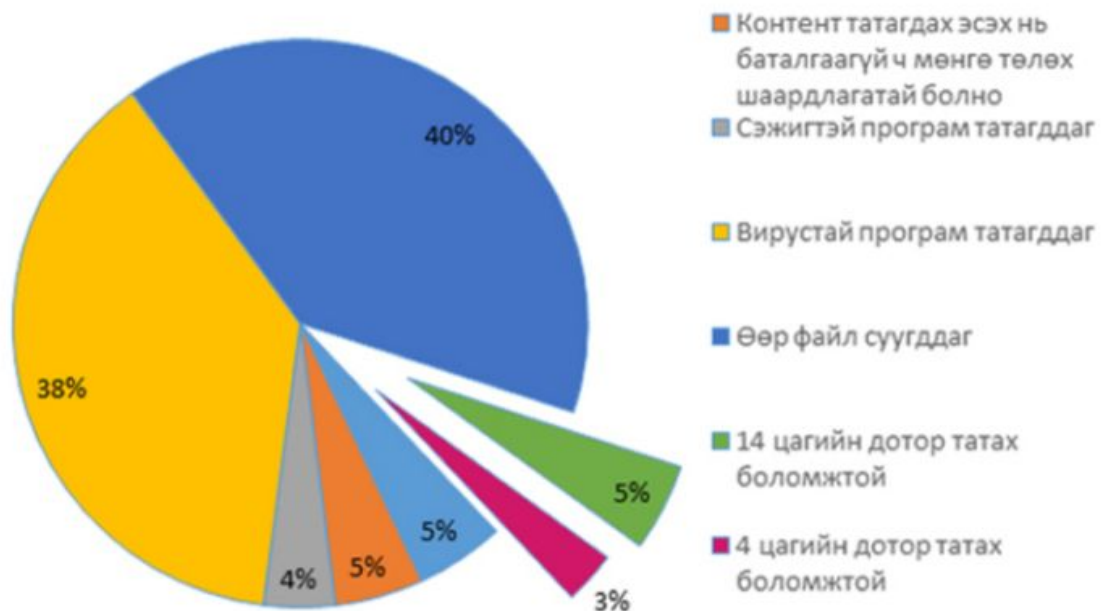
Програмхангам(ПХ) лиценз гэдэг нь зохион бүтээгчийн програмыг албан ёсоор хэрэглэнэ гэсэн үг бөгөөд хэрэглэгч ба програм хангамж үйлдвэрлэгч нарын хооронд үүссэн гэрээний тусгай нэг хэлбэр юм. Програм хангамж худалдан авснаар зохиогчийн эрх програм хангамжийг хэрэглэх үед байх ёстой хязгаарлалтуудыг лицензийн гэрээнд тусгасан байдаг. Жишээ нь өөр хүнд дамжуулахыг хориглох, суулгах төхөөрөмжийн тооны хязгаарлалт, хэрэглэх хугацаа гэх мэт. Албан ёсны лицензтэй програм хангамж ашиглах нь мэдээллийн сан болон хувь хүний мэдээллийн аюулгүй байдлын баталгаа болдог. Програм хангамж үйлдвэрлэгчид албан ёсны лицензтэй програм хангамж нь бүх төрлийн компьютер дээр доголдолгүй ажиллах, ямар нэг гацалт, хортон вирусгүй гэдэгт чанарын баталгаа өгдөг.

Лицензгүй програм хангамж ашиглах нь ямар эрсдэлтэй вэ?

Хуурамч програм хангамж ашиглах нь дараах ноцтой эрсдэлүүдийг дагуулдаг: техникийн, санхүүгийн, зохиогчийн эрхийн тухай хуулийг зөрчсөнөөс үүдэн иргэний эрхийн болон эрүүгийн хариуцлага хүлээх. Ихэнх хулгайн програм хангамж хэрэглэгчид албан ёсны бус програм суулгасанаар зохиогчийн эрх болон түүнд хамаарах эрхийн тухай хуулийг зөрчиж байгаагаа мэддэггүй бөгөөд ямар хор уршиг араасаа дагуулдагыг мэддэггүй. Судалгаанаас үзэхэд хуурамч програм хангамж хэрэглэгчдийн 92 хувь нь өөрийн компьютерийг болон хувийн мэдээллээ ямар нэг хэмжээгээр эрсдэлд оруулж байна.

Хуурамч програм хангамж хайж татан авч,суулгадаг хэрэглэгчдийн компьютер хортон програмын халдлагад өртөх магадлал - 92 хувь
Хулгайн програм хангамж хайхад ямар нэг эрсдэлгүйгээр програмыг татах боломж - 3 хувь
Хэрэглэгчдийн 5хувь нь эрсдэлгүйгээр програмыг татах боломжтой ч үүнд 14 цаг шаардлагатай болно.

Зураг 2.2: Google сайтын Windows 8.1 програмын хайлтын үр



2.4 Лицензийн загвар

Програм хангамжийн борлуулагчид (ISVs) нь лицензийн хэрэглээг тоогоор хэмжиж, бүтээгдэхүүнийхээ орлогыг нэмэгдүүлэх лицензийн олон загвар, хэмжүүрүүдийг ашигладаг. Програм хангамжийн борлуулагч бүр өөрсдийн хэмжүүр гэж нэрлэдэг өөр нэр томъёо байдаг боловч лицензийг тоолох хязгаарлагдмал тооны аргууд байдаг. Програм хангамжийн борлуулагчаас үл хамааран лиценз олгох загварууд нь ерөнхий ангилалд хуваагдана:

Лицензийн хэмжүүр

1. үйлчлүүлэгч / хэрэглэгч

ширээний компьютерийн лиценз

- хэрэглэгчийн тоо эсвэл төхөөрөмжүүдийн тоо
- төхөөрөмж
- хэрэглэгч

2. хүчин чадал / дэд бүтэц хүчин чадал / мэдээллийн төвийн лиценз

- Машины хэмжээ (цөм, процессор, залгуур)
- машинуудын төрөл

3. Зэрэгцээ явагдах

- нэгэн зэрэг хандах
- нэгдмэл хэрэглэгч
- өөрчлөгддөг хэрэглэгч

4. компанийн хэмжүүр

- ажилтан
- үйл ажиллагаа
- орлого

2.5 Лицензийн төрөл

Нэг хэрэглэгчийн лиценз

Нэг хэрэглэгчийн: Энэ төрлийн лиценз нь бусад хэрэглэгчид сүлжээнд нэвтрэх эрхгүй ганц процессор дээр програм суулгах, ашиглах боломжийг олгоно. Програм хангамжийг зөвхөн нэг компьютер дээр ашиглах бөгөөд бусад хэрэглэгчид програм хангамжид хандах эсвэл компьютерт холбогдсон үед ажиллуулах боломжгүй болно.

Лицензийн төрөл:

1. Тогтвортой лиценз: Хэрэглэгч програм хангамжийг хязгааргүйгээр суулгах, ашиглах боломжийг олгодог. Техникийн туслалцааг хязгаарлагдмал хугацаанд, ихэвчлэн 90 хоног багтаана.

2. Захиалгын лиценз: Хэрэглэгч тодорхой хугацаанд програм хангамжийг ашиглахыг зөвшөөрдөг. Энэ лиценз нь ихэвчлэн техникийн дэмжлэг, захиалгын хугацаанд гарсан шинэчлэлтүүд болон засварууд багтна. Энэ нь хугацааны төгсгөлд хэрэглэгч дараах хэд хэдэн сонголттой байна: захиалгыг шинэчлэх эсвэл байнгын лицензийг бууруулсан үнээр худалдан авах эсвэл програмыг компьютерээс устгах сонголтоос сонгох боломжтой.

3. Үнэгүй лиценз : Энэ төрлийн лицензийг зохиогч санал болгодог бөгөөд ашиглалтын төлбөрийг шаарддаггүй.

4.Shareware лиценз: Энэ нь програм хангамжийг туршилтын хугацаанд ашиглах лиценз юм. Хэрэв програм хангамжийг үргэлжлүүлэн ашиглавал shareware төлбөр төлөх эсвэл програм хангамжийг ашиглахаа болих хэрэгтэй.

Тусгай сувгийн лиценз

1. OEM (тоног төхөөрөмж үйлдвэрлэгч): Эдгээр лицензүүд нь дангаараа PC болон зөөврийн компьютерт зориулсан програм хангамжийг хамрах бөгөөд компьютерын системтэй цуг байх ёстой бөгөөд тусдаа (эсвэл дангаараа) бүтээгдэхүүн болгон түгээхгүй байх ёстой. Энэ програмыг "Компьютерийн техник хангамжийн шинэ хувилбараар түгээлтийн хувьд"гэж нэрлэнэ.

2.Боловсрол ба эрдэм шинжилгээний програм хангамж лиценз: Боловсролын байгууллага, оюутнуудад хөнгөлөлттэй үнээр тараах програм хангамж. Энэ програм хангамжийг ихэвчлэн академик бүтээгдэхүүн гэж нэрлэдэг бөгөөд зөвхөн эрдэм шинжилгээний болон боловсролын байгууллагуудад ашигладаг.

3. Баталгаат бус програм хангамжийн лиценз (NFR): Програм хангамжийн борлуулагчид шууд өгч буй тусгай болон хязгаарлагдмал лицензүүд бөгөөд ихэвчлэн NFR гэж тодорхойгүй нөхцөлд тэмдэглэдэг. NFR програм хангамж нь арилжааны ердийн хуваарилалтанд тусгай зөвшөөрөлтэй байдаггүй.

Бие даасан / Олон хэрэглэгчийн лиценз

1. Эзлэхүүний лицензүүд: Лиценз эзэмшигчид тодорхой тооны компьютер дээр програм хангамжийг суулгахыг зөвшөөрдөг. Лиценз эзэмшигч нь хамгийн бага худалдан авалтын шаардлагыг хангаж, үнийг бууруулсан үнээр худалдан авдаг. Лиценз худалдан авахдаа ихэвчлэн хэвлэл мэдээллийн хэрэгсэл, бичиг баримтыг илүү их худалдан авалт хийх боломжтой байдаг.

2. Сайт / Аж ахуйн нэгж: Энэ лиценз нь ганц байршилд програм хангамжид хандах боломжийг олгодог. Дүрмээр бол эдгээр лицензийг нийтлэгчтэй нэг бүрчлэн хэлэлцэж, тэдгээрийн нэр томъёо нь өөр байдаг.

Сүлжээ / Олон хэрэглэгчийн лиценз

1. Сервер (сүлжээ): Сервер лиценз. Энэ төрлийн лиценз нь файлын серверт байрлах програмын нэг хувийг шаарддаг. Серверт тусгай зөвшөөрөл олгох үед тодорхой нэг үйлчлүүлэгчийн лиценз тодорхой сервертэй холбоотой байдаг. Энэ серверт зориулж худалдан авсан клиент лицензийн тоогоор энэ серверийг нэг серверт нэг лицензээр зэрэг нэвтрүүлэх боломжтой төхөөрөмжийн тоог хязгаарладаг.

2. Нэг суудал (машин): Машин / суудал бүрт лицензтэй - Энэ лиценз нь үйлчилгээ авахад шаардлагатай клиент компьютер, төхөөрөмж бүрт лицензийг худалдан авахыг шаарддаг. Энэ лицензийг сүлжээний лицензтэй хамт ашигладаг.

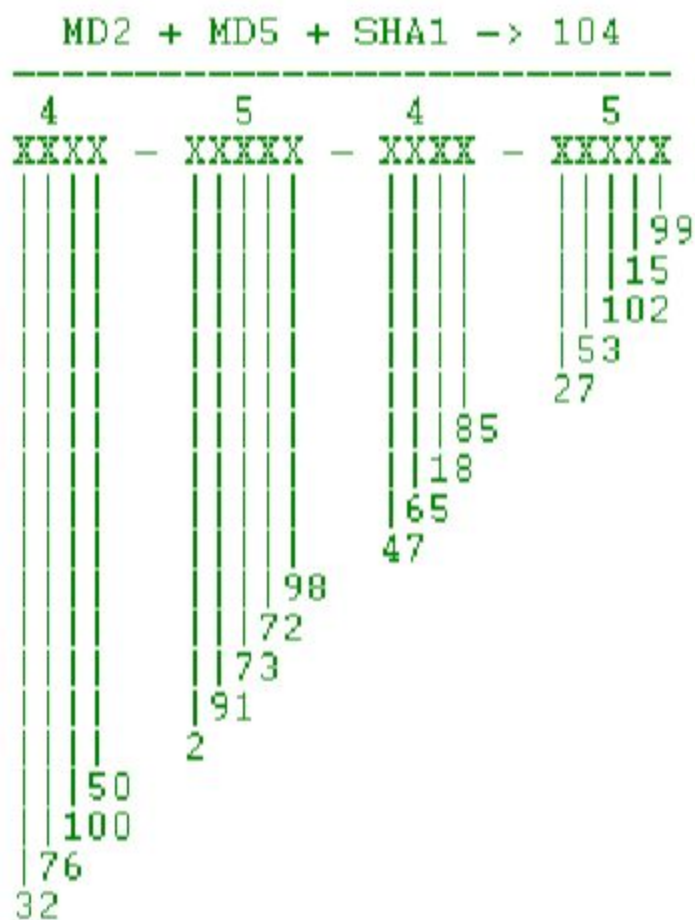
3. Процессор бүрийн хувьд: Процессор бүрийн загварт нийцүүлэн програм хангамжийг ажиллуулж буй сервер дээр процессорын зөвшөөрөл авдаг. Процессорын тусгай зөвшөөрөл нь ихэвчлэн хязгааргүй тооны хэрэглэгчидтэй холбох хандалттай байдаг. Та нэмэлт серверийн лиценз, клиентийн лиценз, интернет холболтын лиценз худалдан авах шаардлагагүй.

4. Нэг шуудангийн хайрцаг (Боловсролын хэрэглэгчдэд зөвхөн): Хэрэв та Exchange Server ашиглан боловсролын хэрэглэгч бол танд лицензийг шуудангийн хайрцагт горимд байрлуулах нэмэлт сонголт байна. Энэ загвараар та Exchange Server серверт хандах өвөрмөц мэйлийн хайрцаг бүрт нэг CAL олж авна.

Одоо байгаа болон шинээр олгогдсон лицензүүд

- Шинэчлэлт: Хэрэглэгч өмнө нь олж авсан програмын лицензтэй байсан бөгөөд шинэ хувилбар руу шинэчлэхийг хүссэн тохиолдолд лицензийг худалдан авдаг. Өмнөх хувилбар хүчин төгөлдөр бус бөгөөд өмнөх хувилбарыг өөр хэрэглэгч рүү шилжүүлж болохгүй.
- Оюутнуудын хэрэглээ: Энэ нь оюутнууд програм хангамжийг ашиглахыг зөвшөөрдөг. Оюутнууд төгссөний дараа програм хангамжийг устгах шаардлагатай байдаг.
- Хоёрдогч хэрэглээ: лицензтэй эцсийн хэрэглэгчид програмыг хоёр компьютер дээр ашиглахыг зөвшөөрдөг.
- Гэрийн ажлын эрх: Факультет / ажилтнууд гэртээ програм хангамж ашиглах боломжтой. Энэ нь анхдагч ажлын компьютер лицензтэй бөгөөд тухайн хүн ажилтан бол үр дүнтэй байдаг. Хөдөлмөр эрхлэлтийг дуусгавар болгохоор нь энэхүү лицензийг цуцална.
- Захиалга / үйлчилгээ. Энэ нь лиценз эзэмшигч болон програм хангамжийн хөгжүүлэгчийн хооронд байгуулсан гэрээний хугацаа бөгөөд гэрээний хугацааны туршид бүх програм хангамж шинэчлэлт эсвэл шинэчлэлийг хүлээн авахыг зөвшөөрдөг. Энэ нь ихэвчлэн лицензийн гадна болон лицензийн хамт худалдан авдаг. Subscription / Service нь гэрээний төгсгөлд ихэвчлэн шинэчлэгддэг. Одоогийн лиценз дээр нэмсэн захиалга / үйлчилгээ нь анхны лицензийг өөрчилж болно.

III. Судалгааны хэсэг



Зураг 3.1: Санамсаргүйгээр цуваа түлхүүрийг үүсгэх

3.1 Цуваа түлхүүр үүсгэх болон Java-ийн баталгаажуулалт

Модуль нь гурван хэсгээс бүрдэнэ.

- Цуваа үеийн алгоритм
- Цуваа үүсгэх
- Цуваа шалгах

1.Цуваа үеийн алгоритм

Цуваа түлхүүрийн хувьд 18 оронтой тоо. Энэ нь хэрэглэгч хэрэглэгчийн нэр өгдөг юм. Энэ нь дахин давтагдашгүй байх болно (оролт дээр тулгуурлан). Хэрэглэгчийн нэрийг оролт болгон аваад MD2, MD5 SHA1 алгоритмд

зориулан бэлтгэж нийлүүлнэ. Энэ нь нийтдээ 104 оронтой тоо бий болно. Учир нь 18 тоог сонгохын тулд урьдчилан тодорхойлогдсон тоонуудыг ашиглаж болно. Доорх зурагт алгоритмыг тайлбарласан болно. 104 тооны хэшээс 18 тоог сонгохын тулд санамсаргүй тоонуудыг сонгож авсан бөгөөд та цуваа түлхүүрийг үүсгэдэг дурын тоог ашигладаг.

2.Цуваа үүсгэх нь

```
String serialNumberEncoded = calculateSecurityHash(fullNameString,"MD2") +  
    calculateSecurityHash(fullNameString,"MD5") +  
    calculateSecurityHash(fullNameString,"SHA1");
```

Зураг 3.2: MD2, MD5, SHA1 тулгуурлан хэш үүсгэх

```
private String calculateSecurityHash(String stringInput, String algorithmName)  
    throws java.security.NoSuchAlgorithmException {  
    String hexMessageEncode = "";  
    byte[] buffer = stringInput.getBytes();  
    java.security.MessageDigest messageDigest =  
        java.security.MessageDigest.getInstance(algorithmName);  
    messageDigest.update(buffer);  
    byte[] messageDigestBytes = messageDigest.digest();  
    for (int index=0; index < messageDigestBytes.length ; index ++){  
        int countEncode = messageDigestBytes[index] & 0xff;  
        if (Integer.toHexString(countEncode).length() == 1)  
            hexMessageEncode = hexMessageEncode + "0";  
        hexMessageEncode = hexMessageEncode + Integer.toHexString(countEncode);  
    }  
    return hexMessageEncode;  
}
```

Activate
Go to Settings

Зураг 3.3: Төрлөөс хамааран оролтын тэмдэгт мөрийг хэш үүсгэх

Цуваа үүсгэхийн тулд оролтын тэмдэгт мөрөнд MD2, MD5, SHA1 ашиглан мөрүүдийг оролтын хэсэгт үүсгэнэ. Calculate Security Hash нь оролтын тэмдэгт мөр ба хэш утгыг оролтоор авч, энэ арга дээр тулгуурласан хэш үүсгэдэг.

Гурван төрлийн хэшийг нэгтгэсний дараа 104 тэмдэгттэй болно. Цуваа түлхүүрийнхээ хувьд 18 холимог хэшээс санамсаргүй 18 тооноос

сонгож болно. Түлхүүрийг баталгаажуулахын тулд 18 тоог авахад санамсаргүй тоо үүсгэх боломжгүй болно.0-ээс 103 хоорондох тоонуудыг сольж өгч болно. Түлхүүр нь өөр өөр байх бөгөөд оролтын хэсгээс хамаарч болно.

3. Цуваа шалгах

Хэрэглэгчийн нэр, цуваа түлхүүрийг авах бүртээ баталгаажуулах боломжтой байх ёстой. Цуваа түлхүүр болон хэрэглэгчийн нэрийг баталгаажуулахын тул алгоритм нь тус бүрээр хэрэглэгчийн нэрийг авч цуваа түлхүүр үүсгэх болно. Цуваа түлхүүртэй бол үүнийг баталгаажуулах зорилгоор авсан түлхүүртэй нь харьцуулах юм бол хоёулаа таарч байвал зөв түлхүүр байна.

```
String serialNumber = ""
+ serialNumberEncoded.charAt(32) + serialNumberEncoded.charAt(76)
+ serialNumberEncoded.charAt(100) + serialNumberEncoded.charAt(50) + "-"
+ serialNumberEncoded.charAt(2) + serialNumberEncoded.charAt(91)
+ serialNumberEncoded.charAt(73) + serialNumberEncoded.charAt(72)
+ serialNumberEncoded.charAt(98) + "-"
+ serialNumberEncoded.charAt(47) + serialNumberEncoded.charAt(65)
+ serialNumberEncoded.charAt(18) + serialNumberEncoded.charAt(85) + "-"
+ serialNumberEncoded.charAt(27) + serialNumberEncoded.charAt(53)
+ serialNumberEncoded.charAt(102) + serialNumberEncoded.charAt(15)
+ serialNumberEncoded.charAt(99);
```

Зураг 3.4: Цуваа түлхүүрийн 18 хэш сонгож авах


```
String serialNumberEncoded =
    registrationAppSerialGenerationReversal.calculateSecurityHash(fullNameString,"MD2")
    + registrationAppSerialGenerationReversal.calculateSecurityHash(fullNameString,"MD5")
    + registrationAppSerialGenerationReversal.calculateSecurityHash(fullNameString,"SHA1");

String serialNumberCalc = ""
    + serialNumberEncoded.charAt(32) + serialNumberEncoded.charAt(76)
    + serialNumberEncoded.charAt(100) + serialNumberEncoded.charAt(50) + "-"
    + serialNumberEncoded.charAt(2) + serialNumberEncoded.charAt(91)
    + serialNumberEncoded.charAt(73) + serialNumberEncoded.charAt(72)
    + serialNumberEncoded.charAt(98) + "-" + serialNumberEncoded.charAt(47)
    + serialNumberEncoded.charAt(65) + serialNumberEncoded.charAt(18)
    + serialNumberEncoded.charAt(85) + "-" + serialNumberEncoded.charAt(27)
    + serialNumberEncoded.charAt(53) + serialNumberEncoded.charAt(102)
    + serialNumberEncoded.charAt(15) + serialNumberEncoded.charAt(99);

if (serialNumber.equals(serialNumberCalc))
    System.out.println("Serial MATCH");
else
    System.out.println("Serial MIS-MATCH");
```

Зураг 3.5: Хэрэглэгчийн нэрээр цуваа түлхүүр үүсгэх

```
D:\temp>java RegistrationAppSerialGeneration
Starting Serial Generation Algorithm
Enter Full Name: Joey
Serial Number f55d-967fa-44cf-ca24f

D:\temp>java RegistrationAppSerialGenerationReversal
Enter Full Name: Joey

Enter the Serial Number: f55d-967fa-44cf-ca24f
Serial MATCH

D:\temp>java RegistrationAppSerialGenerationReversal
Enter Full Name: Joey

Enter the Serial Number: f25d-d67fa-4dcf-3ae4f
Serial MIS-MATCH
```

Зураг 3.6: Хэрэглэгчийн нэрээр цуваа түлхүүр үүсгэсэн үр дүн

3.2 Шилдэг үйлдвэрлэгч

Одоогийн байдлаар үйлдвэрлэгчдийн санал болгодог лицензийн төрлүүд

1. Төхөөрөмж - 'машин дээр суурилсан' гэж бас нэрлэдэг.

2. Хэрэглэгч - Лицензийн гэрээг баталгаажуулахын тулд л хэрэглэгчдэд лиценз олгогддог ба лицензийн нөхцөлийг мөрддөг.
3. Сүлжээ (WAN LAN) - Сүлжээний ижил дэд бүтэцтэй машинуудыг хамарсан лиценз. Энэ нь олон сүлжээнд эсвэл жижиг хэмжээний сүлжээний форматтай. 'Нэмэлт лиценз' гэж тодорхойлдог.
4. Захиалга (хэрэглэгчийн эсвэл төхөөрөмж) - Лиценз зөвхөн захиалга өгөх үед гарах боломжтой. Гэрээг ашиглахын өмнө болон дараа нь ашиглах эрхгүй (гэрээ сунгагдаагүй бол).
5. 'Cloud based credits' захиалга – Үүлэн технологид суурилсан кредит нь үйлдвэрлэгчээс олгож байгаа тодорхой програмуудыг ажиллуулах эрхтэй нэгж юм. Үүл дээр зохион байгуулагддаг бөгөөд ихэвчлэн захиалгын загвар байдаг.
6. Нийтийн лиценз (GPL) - Лиценз, програм хангамж үнэгүй байдаг. Хэрэглэгчид програм хангамжийг ашиглах, хуваалцах, хуулбарлах, өөрчлөх боломжтой. 'төлбөргүй програм' гэж тодорхойлогддог.
7. Клиент хандах лиценз (CAL, төхөөрөмжийн болон хэрэглэгчийн хэмжүүрийг хоёуланг нь агуулдаг) - Хэрэглэгчид програм хангамжийн функц / функцийг ашиглахын тулд серверийн програм хангамжид холбогдохыг зөвшөөрдөг.
8. Чадавхийг үндэслэсэн лиценз - Лиценз нь CPU / Хатуу диск эсвэл бусад тоног төхөөрөмжийн хүчин чадал дээр суурилдаг.
9. Фонтын лиценз - Фонт тодорхой лиценз.
Байгууллагын онлайн эсвэл дотроо ашигладаг фонтуудтай холбоотой.
10. Freeware-Лиценз нь худалдан авалт хийхийг шаарддаггүй боловч зохиогчийн эрх хуулиар хамгаалагдсан байна. Хөгжүүлэгч нь програм хангамжийг зарж борлуулж, эх кодыг тараахгүй.

Шилдэг 10 үйлдвэрлэгч, тэдний лиценз

Санхүүгийн жилийн орлогынхоороо тэргүүлэгч 10 компани дээр тулгуурлан лицензийн загварыг тэдний өгөгдлийн маягтаар авч үзье.

Хүснэгт 3.1 Шилдэг үйлдвэрлэгч, тэдний лиценз

	Microsoft	Oracle	IBM	SAP	Symantec	EMC	HP	VMWare	CA	Salesforce
Device	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗
User	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Core/ Processor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Networked	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗
Subs	✓	✓**	✓	✓	✓	✓	✓	✗	✓	✓
Cloud credits	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗
GPL	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
CAL	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Font	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
Freeware	✓	✓*	✗	✓	✗	✗	✗	✗	✗	✗

* Oracle-ийн хөгжүүлэгчийн лиценз

** Oracle-ийн 'Update subscription service'. Лиценз гэж тооцогддог.

+ Үйлдвэрлэгчид захиалгын тусгай зөвшөөрөл олгохгүй байж болох боловч засвар үйлчилгээ болон бусад үйлчилгээнд захиалга өгдөг.

3.3 Сериал түлхүүр үүсгэгч вэбсайт

Програмын цуваа түлхүүр өгөх боломжийг олгодог сайтууд:

Програм хангамжийг худалдан авч, бүх боломжид хандах боломжийг танд олгож буй програм хангамж түлхүүртэй байдаг. Тиймээс хамгийн их ашиглагддаг програмын цуваа түлхүүрийг олох боломжтой вэбсайтууд.

1. Serials.ws: Serials.ws бол програм хангамжийн цуваа түлхүүрүүдийг олох боломжтой хамгийн сайн вэбсайт юм. Цуваа түлхүүр бүхий олон вэбсайт дээр олон холбоосоор дамжих хэрэгтэй болно. Энэ нь зөвхөн нэг холбоос дээр дарж, програм хангамжийн цуваа түлхүүрийг авах болно. Энэ вэбсайтад 125544 програм хангамж ажиллаж байгаа цуваа түлхүүрүүд байна. Вэбсайт нь хугацаа дууссаны дараа шимтгэлийн програм бүр өөрсдийн цуваа түлхүүрийг өөрчилдөг тул дууссан цуваа түлхүүрүүдээс байнгын цуваа түлхүүрүүдийг авахын тулд долоо хоног бүр шинэчлэгддэг.

SERIALS.WS
UNLOCKED THE WORLD

DAILY UPDATING!!!

Unlocking the world since 2001

Serials in the database: **128544**

Added today: **0**

Added within the last week: **0**

Top uploaders are:

[Ghosty]
[fox]
[Gips]
[Ahmed]

Recent serials rating is: **0%**

Overall average rating is: **42.63%**

Last added

	Date
iobit Advanced SystemCare 11.3 key	2018-05-08
Windows 10Professional [08 May 2018]	2018-05-07
Magik Photostory deluxe	2018-05-07
IObit Uninstaller 7.4 PRO	2018-05-06
IObit Malware Fighter 6	2018-05-06
Battleground	2018-05-06
Driver Booster 5.4	2018-05-06
Freemake video converter [08 May 2018]	2018-05-05
Advanced SystemCare 11.3 Pro key	2018-05-05
Advanced SystemCare 11.3 Pro key [08 May 2018]	2018-05-05
Advanced SystemCare 11.3 Pro NEW	2018-05-05
Trainz simulator a new era	2018-05-05
Star Trek Voyager Elite Force	2018-05-05
WinToUSB	2018-05-05
AVG 2018 [08 May 2018]	2018-05-03

Top 25 serials

	date	rating
iobit Advanced SystemCare 11.3 key	2018-05-08	60%
IObit Malware Fighter 6	2018-05-06	35%
Windows 10Professional [08 May 2018]	2018-05-07	49%
Driver Booster 5.4	2018-05-06	70%
Advanced SystemCare 11.3 Pro key	2018-05-05	85%
ByteFence Anti-Malware Pro 2017	2017-05-24	92%
Advanced SystemCare 11.3 Pro key [08 May 2018]	2018-05-05	87%
ByteFence Anti-Malware 2017 free - Pro	2017-05-27	87%
Advanced SystemCare 11.3 Pro NEW	2018-05-05	70%
AVG 2018 [08 May 2018]	2018-05-03	33%
Microsoft Windows 10 Pro	2015-10-05	60%
ByteFence Anti-Malware Free Pro 2017	2017-07-10	49%
ByteFence Anti-Malware 2017	2017-09-07	66%
IObit Uninstaller 7.4 PRO	2018-05-06	89%
IObit Malware Fighter Pro 5.3	2017-11-30	90%
IObit Malware Fighter 5.1 PRO	2017-06-05	91%
Advanced SystemCare 11.2 PRO	2018-04-17	86%
IObit Malware Fighter WORKS 100% PROOF	2017-05-10	90%
Advanced SystemCare 11 Pro	2017-11-20	81%
Advanced SystemCare 11.2 PRO	2018-04-17	87%

Popular queries:

advanced system care
advanced systemcare
11
avast
iobit
office 2016
driver booster 5
driver booster
iobit malware fighter 6
bytefence
advanced systemcare
storyboard quick 6
ccleaner
windows 10
keygenerator adobe
mastercollection cs5
days gone keyfinder
real farm
keep vid pro 4.10.1
vshare identification
code
proshow gold v4.0.2549
ecrawl 2.41
softwarenetz rechnung
avance c video converter
php tools for visual
studio
hd tune pro
windows 8 activator

Recent queries:

key action minis 1.20
Adobe Photoshop
Elements 15 serial
GIMP 2.10
Droptube Magic
Vespa Rally Standard

Зураг 3.7: serials.ws сайтын бүтэц

736

Like

Navigation

- » Main Page
- » Add Serials

Browse

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

Search

Share

SHARE

Lastest Serials

- » FutureDecks DJ Pro v3.5.0
- » Tagtraum Industries beaTunes v3.5.11
- » Ocster Backup Pro v7.10
- » Breez LocalAPK v1.5.3
- » Ardfray PSD Codec v1.6.1.0
- » EASEUS Data Recovery Wizard Professional v5.8.0
- » Connectify Hotspot Pro v4.2.0.26.088
- » AVCWARE Video Converter Ultimate v7.7.2.20130122
- » Goldwave v5.68
- » KSSoft Advanced Host Monitor v9.38 Enterprise
- » ESComputing EditPlus v3.50.277
- » openCanvas v5.5.09
- » ChemTable Software Reg Organizer v6.0
- » ActiveFax v5.01.0232
- » Light Image Resizer v4.4.1.0
- » AD Sound Recorder v5.4.5
- » Drive SnapShot v1.42
- » Spectaculator v8.0
- » Okdo Document Converter Professional v4.8
- » Auslogics Disk Defrag Pro v4.2.2.0
- » Novosoft Handy Backup Home Standard v7.3.2.11853
- » PDF-XChange 2012 Pro v5.0.267.0
- » PDF-XChange Viewer Pro v2.5.208
- » Focus Photoeditor v6.5.1.0

Зураг 3.8: serialbay.com сайтын бүтэц

2.Serialbay.com - цувралын түлхүүрүүд болон серверт зориулсан өөр нэг том мэдээллийн бааз бөгөөд цогц холбоосуудтай өргөн хэрэглэгддэг вэбсайт бөгөөд

serials.ws нь маш сайн сонголт юм. Энэ нь компьютерийн програм хангамжийг төдийгүй бас тоглоомуудыг санал болгодог.

3.keygeninja.com-Цуваатүлхүүртомоохонплатформболононцлогбүхий мэдээллийн баазыг ашиглахад хялбар, ямар ч зар сурталчилгааг ашигладаг. Энд тоглоом, програмын түлхүүр, олох боломжтой. Сайтын хэрэглэгчийн интерфэйсүүд нь энгийн бөгөөд амархан ажиллах боломжтой байдаг. Та мөн өөрийн програм хангамжийн лицензийн түлхүүрийг хуваалцаж болно.



Зураг 3.9: keygeninja.com сайтын бүтэц



Зураг 3.10: smartserials.com сайтын бүтэц

4. Smartserials.com-Сайт нь хамгийн сүүлийн үеийн ажиллах цуваа түлхүүрүүдийн асар их цуглуулгатай. Энэ нь тодорхой програм хангамжийн цуваа түлхүүрийн

хүсэлт гаргаж болох форумын хэсэг байдаг. Энэ цуваа түлхүүрүүдийн сайт нь та хэрэгтэй файлыг авах болно (гуравдагч этгээдийн сайтаас татан авахад шаардлагатай гарын үсэг) болон сериал дугаарыг авах болно.

5. keygens.pro- Энэ вэбсайт мэдээллийн сан нь програм хангамж, цувааны түлхүүрүүдийг үнэ төлбөргүй авах боломжтой байдаг. Вэбсайтын хайлтын систем нь маш сайн ажилладаг бөгөөд ямар ч нэр томъёог хайж олоход бүх түлхүүр үгсийг харуулж, цагаан толгойн дарааллаар харуулдаг.

IV. Дүгнэлт

Энэхүү бие даалтын хүрээнд програм хангамжийн компанууд лиценздээ яагаад сериал түлхүүрийг ашиглах болсон гэвэл зохиогчийнхнийг дээдлэх, өөрсдийн бэлдсэн сайжруулсан зүйлийнхээ найдвартай ажиллагаа болон хэрэглэгчдэд сэтгэл ханамжтай үйлчилгээг бий болгох явдал юм. Сериал түлхүүр нь лицензтэй програм хангамж үйлдвэрлэгч болон хэрэглэгч хоорондын дахин давтагдашгүй баталгаажилтын түлхүүр юм. Лицензгүй програм ашигласнаар халдлагад өртөмтгий сул тал ихтэй. Иймд зүй зохистой хэрэглээг бий болгож лицензтэй програм хангамж ашигласах нь оновчтой.

V. Ашигласан материал

- Serial key available at
<https://www.goodtechtricks.com/software-serial-keys/>
- Serial key generation available at
<https://venishjoe.net/post/serial-key-generation-and-validation-in-java/>
- Top license type available at
<https://www.itassetmanagement.net/top-ten-licensing-types/>
- serial key sites available at
<https://www.jiho.com/en/free-utilities/free-serial-key-websites.h>