# JAVASCRIPT SӨCKET АЮУЛГҮЙ ЧАТ ӨРӨӨ

**Т.Булганмаа, Zhang Jiu Xing**

Өвөрмонголын их сургууль, Компьютерын сургууль

И-мэйл: yhoomsg@yahoo.com

## ХУРААНГУЙ

*Мэдээллийн эрин нь мэргэжлийн програмистийн криптогарф (нууц бичээс тайлалт)-ийг хэрэглэх шаардлагатай болдог тоон системийн сангийн эрин үе юм. Аюулгүй байх үүднээс, зөвшөөрөлгүй нэвтрэх хэрэглэгчдээс сэргийлэх хамгаалалттай байх хэрэгтэй бөгөөд ингэснээр хүсээгүй өөрчлөлт хийх шаардлагагүйгээс гадна зориулалтын хэрэглэгчид хэрэглэж чадах нөхцлийг бүрдүүлж өгдөг. Үүнийг шифрлэлт, тоон түлхүүр тэмдгүүд болон интерференц гэх мэтийн аюулгүйн элементүүдийн хэрэглээг бий болгодог протоколын утгуудаар баталгаажуулан хамгаалж болдог.*

*Интернетийн өргөн хэрэглээг дагаад виртуаль орчинд хүн бүр бие биентэйгээ сүлжээгээр холбогдож байна. Өдрөөс өдөрт нэмэгдэж байгаа онлайн худалдаа нь эдийн засаг, нийгэмд эерэг болон сөрөг үр дагаварыг авч ирж байна.*

*Интернет дамжуулалтын амин чухал асуудал бол мэдээллийн аюулгүй байдал түүнийг тойрсон асуудлууд юм.*

*Цахим харилцааны аюулгүй байдал нь Вэбд суурилсан үйл ажиллагаанууд, онлайн худалдаа, аюулгүй чат өрөө зэрэг олон талуудтай холбогдож байна. Интернетээр дамжин харилцаж байгаа талуудын хоорондох харилцааг хамгаалах, хувийн нууц, чухал мэдээллийг илүү найдвартай хамгаалах нь өнөөгийн байдлаар дутагдалтай байна. Криптограф бол компьютерийн системийн мэдээллийг хамгаалахад зориулагдсан чухал хэрэгтэй хэрэгсэл билээ. Криптосистем нь тэгш хэмт болон тэгш хэмт бус гэж хоёр хуваагддаг. Тэгш хэмт криптограф нь хоёр талууд нэгэн ижил түлхүүрийг хэрэглэн үйл ажиллагааг гүйцэтгэдэг бол тэгш хэмт бус криптограф нь нэг түлхүүр (нийтийн түлхүүр) хэрэглэн мессэжийг шифрлэх бөгөөд өөр нэг түлхүүр(хувийн түлхүүр) хэрэглэн шифрлэлтийг тайлдаг. Диффе Хэллмэн түлхүүрийн хэлэлцээр нь тэгш хэмт бус алгоритмуудаас хамгийн алдартай.*

*Sөket нь интернет сүлжээний програмчлалын API бөгөөд Unix, linux, windows зэрэг системийн хэрэглэгддэг интернет сүлжээний програмчлалын стандарт юм.*

*Сүлжээний програмчлалын явцад байнгын хэрэглэдэг аргачлал нь Client/Сервер юм. Энэхүү өгүүлэлд Client /Сервер хэлбэрийг Javascript Soket-г ашиглан Deffie Hellman түлхүүр солилцох аргаар аюулгүй мэдээлэл солилцох үүрэгтэй вэб сайт дээр суурилсан чат өрөө хийхийг зорилоо.*

**ТҮЛХҮҮР ҮГ**: javascript socket ю, Deffie hellman key exchange, security chatroom

## ОРШИЛ

**Socket-ийн тухай**

Socket нь компьютерийг нэг харилцаа холбооны портоор хангасан, компьютер нь энэ портоор бусад адилхан Socket интерфэйстэй дурын нэг компьютертэй харилцаа холбоо тогтоож болно. Мэдээлэл хүлээн авах нь бүгд Socket интерфэйсээр биелэгдэнэ. Бодит хэрэглээнд file handle ашиглаж байгаа шиг socket handle-ийг уншиж, бичиж болно. Socket залгуурыг заадаг /цахилгааны тэжээлийн залгуур шиг залгуурыг залгаж холболт үүсгэж цахилгаан тоног төхөөрөмжийг ажиллуулдагтай ижил.

Клиентүүд хоёр чиглэл бүхий интернет холболтыг үүсгэж сервер рүү холбогдож мэдээллийн эх үүсвэрүүдийг сонирхож холбогдох үйлчилгээг авах болно. Жишээлбэл сүлжээнд байнга ашигладаг telnet, ftp гэх мэт. Эдгээр нь socket-д суурилсан үйлчилгээний програм юм. Нэг хост компьютерээр олон төрлийн үйлчилгээ үзүүлж болох бөгөөд эдгээр үйчилгээ нь хоорондоо нөлөөлөхгүй зөвхөн тэдгээрийн харилцах порт нь өөр өөр байдаг. Жишээлбэл http үйлчилгээний порт нь 80 порт, telnet нь 23 порт, ftp нь 21 порт. Байнгын байдалд 0-1023 порт дугаарыг системд үлдээж 1023-с дээшийг хэрэглээний програмд өгч ажилуулдаг.

Мэдээллийн аюулгүй байдлыг хангахын тулд хууль бус хэрэглэгчид (нууцлалыг хадгалах зарчим), хүсээгүй өөрчлөлтүүдийг (бүрэн бүтэн халдашгүй байдал) хийхээс урьдчилан сэргийлэх, мөн хэрэглэгчдийн хүртээмжтэй, тохиромжтой байх нөхцлийг хангах ёстой. Энэ нь Шифрлэлт, тоон гарын үсэг, [1] хэш хийх гэх мэт аюулгүй байдлын команд ашиглах протокол аргаар баталгаажуулж болно.

Манай орны хувьд онлайн худалдаа нь хөгжих шатандаа явж байна. Нийт бүртгэлтай идэвхтэй үй ажиллагаатай 34 вэб сайтыг тандан судлахад (хувийн блог, фэйсбүүк сайтуудыг оруулаагүй) бүгд оператор хэрэглэгчтэй харилцах чат өрөөтэй байна.

Энэхүү чат өрөө нь Yahoo Messanger-ийг чатлах хэрэгслээ болгож байгаа нь дутагдалтай талтай бөгөөд хэрэглэгчдийн ярилцаж байгаа мессеж дээр хамгаалалт хийгдэггүй учраас дайрагчидад өртөг боломжтой. Тиймээс хэрэглэгчдийн дамжигдаж байгаа мессеж дээр хамгаалах технологийг судлаж аюулгүй чат өрөө бүтээв.

**Чат өрөөнд хэрэглэгдсэн технологиуд**

1. ***Javascript*** *JavaScrip нь динамик вэб хуудас бүтээхэд клиент серверийг холбодог хэрэглэхэд хялбар объект хандалтад скрипт хэл юм. Түүнчлэн бүх төрлийн үйлдлийн систем дээр ажилдагаараа давуу талтай. [3]*
2. ***Javascript socket. io*** *Node js /Socket.io,socks5,starttls,express/*
   Node.js [3] нь платформ хамааралгүй учраас аль нэг враузер дээр ажиллуулахад хурдан сүлжээний програм хангамжуудад хувиарлах боломжтой байдаг. Үүнийг хэрэглэхэд оролт/гаралт блоклогдохгүй хоцрогдлын хугацаа бага, бодит хугацаанд тархсан төхөөрөмжүүдээр ажилуулахад мэдээллийн боловсруулалт хийх нь төгс гүйцтгэлтэй юм. JavaScript дээр Node.js.-д зориулж SOCKS, HTTPS клиент талыг боловсруулна.
3. *JQuery* бол хурд өндөртэй, багахан хэмжээтэй, олон онцлогтой JavaScript-ийн сан юм. Энэ нь HTML баримтын хувиргал, шилжүүлэлт болон хувиргах оролдлого, үйлдлийг хянах, дүрсийг хөдөлгөөнд оруулах болон Ajax мэтийг ачаалагчийн олон үйлдлээр ажилладаг хэрэглэхэд хялбар API – аар амархан үйлддэг. [4]
4. *Git bash: Нээлттэй эхийн бүхий тархсан хувилбарт удирдлагын систем богоод Бүхий л жижиг, том тослүүд дээр хурдтай, бүтээмжтэй хэрэглэдэж байна.* [5]

## СУДЛАГДСАН БАЙДАЛ

Кикучиийн тодорхойлсноор Instant Messenger аюулгүй байдалд Deffie-Hellman протокол илүү тохиромжтой байдаг.Үндсэндээ Instant Messenger (IM) серверүүдийн хариуд мессежийн нууцлалыг хангахад чиглэгдсэн. Энэ нь Клиент-Сервер баталгаажуулалтын дүрмээр явдаггүй, Instant Messenger(IM) аюулгүй [6] шийдлийн энгийн хязгаарлалтаар хийгддэг. Олон төрлийн домэйн IM үйлчилгээ байдаг. Хамгийн түгээмэл нь AIM [7], ICQ [8], MSN Messenger (Windows Messenger in Windows XP) [9], and Yahoo! Messenger (YIM) [10] юм. Бид эдгээр мессенжер сүлжээ болон тэдний хэрэглгчдэд анхаарал тавин ажилладаг. Үүнээс гадна эдгээр сүлжээгээр харилцдаг олон тооны хэрэглэгчид байдаг. Бид гуравдагч тал болон үндсэн хэрэглэгчид, тэдгээрийн

мэдээллийн аюулгүй байдалтай холбоотой асуудалд санаа тавьдаг. Нийтийн IM-д одоогоор хэрэглэгдэж буй үндсэн протоколууд олон хамгаалалтын сүрдүүлэгт нээлттэй хэвээр байна.

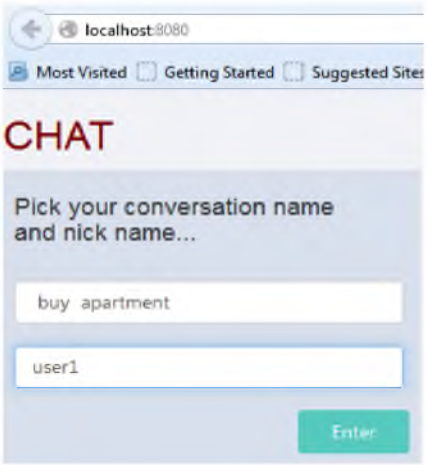
**Аюулгүй чат өрөөний бүтэц**

Чат өрөө нь хувийн болон нийтийн гэсэн хоёр хэсгээс бүрдэнэ.

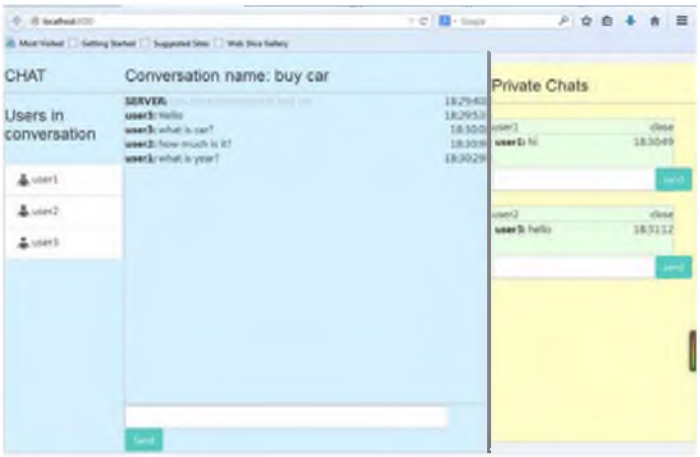
Хэрэглэгч заавал чатлах өрөөнийхөө нэрийг мэдсэн байх хэрэгтэй бөгөөд өөрийн хүссэн дурын нэрээр чатын өрөөнд орно.

Харилцагч хоёр талууд нь аюулгүй чатлах өрөөнд орохоосоо өмнө чатлах өрөөний нэрээ мэдсэн байна.

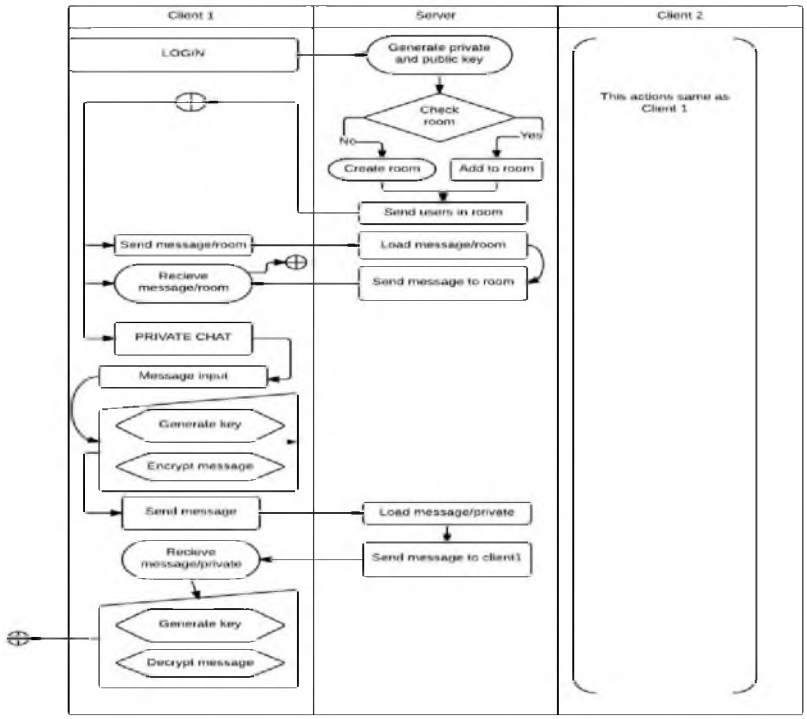
Жишээ нь Эрдний үнэт эдлэл дуудлага худалдаагаар зарах гэж байгаа бол Худалдагч этгээд харилцах өрөөний нэрийг "Үнэт эдлэл 2015:1:1" гэж нээсэн бол худалдан авагчид зөвхөн энэхүү нэрээр л чат өрөөнд орж худалдаа хийнэ. Харагдах байдал Зураг.1 Чат өрөөний нэрээр нэвтэрсэн тохиолдолд олон хэрэглэгчдтэй нэгэн зэрэг, эсвэл сонгосон хэдэн хэрэглэгчтэй харилцах боломжтой болно. Харагдах байдал зураг.2




Зураг.1 Чат өрөөнд нэвтрэх




Зураг.2 Чат өрөөнд нэг болон олон хэрэглэгчтэй ярилцах өрөө




Зураг.3 Чат өрөөний урсгалын диаграм

### *3.1 Чатын өрөөний үндсэн үйл ажиллага*

a. **Сервер порт:** Хэрэрэглэгч чатад ороход өөрийн портоороо серверт бүртгүүлж шинээр session үүсгээд бусад хэрэглэгчтэй холбогдоно.Хэрвээ групп чатад мэдээлэл солилцохоор хэрэглэгч орж ирвэл мессэжийг онлайнд байгаа хэрэглэгч болгонд харагдахаар сервер дамжуулна.Аль нэг хэрэглэгч чатаас гарах үед хоорондох яриа дуусгавар болж сервер портонд тус хэрэглэгчийг буцаана.

b. **Клиент порт:** Хэрэглэгч холбогдоход сервертэй холболт үүсгэж өөрийн хэрэглэгчийн нэрийг мэдүүлэхийн зэрэгцээ шинэ хэрэглэгч орж ирсэн болон гарсан тухай автоматаар серверт мэдэгдэнэ.

## СУДАЛГААНЫ АРГА ЗҮЙ

Шифрлэлт (cipher) нь мэдээг үсгээр кодлох арга юм. Өөрөөр хэлбэл мэдээний үсэг (тэмдэг) бүрийг өөр үсэг (тэмдэгт)-ээр өөрчлөж мэдээний утгыг нуух ерөнхий систем юм. Шифр бүр алгоритм болон түлхүүр гэж хоёр хуваагддаг.

*Диффе Хэллмэн түлхүүрийн хэлэлцээр* (D–H) [11] хийх арга нь нийтийн сувгаар криптографикийн түлхүүрийг аюулгүй байдалд солилцдог анхны криптографикийн нийтийн түлхүүр солилцох жишээ юм гэж Ралф Меркли нарийн тодорхойлжээ.

### *3.3 Диффе Хэллмэн түлхүүрийн хэлэлцээр хийх арга*

$F_q^*$ төгсөлөг талбарт $(F_q^*, 0)$ *цикл бүлгийг үүсгэгч* $g$ байг *Аливаа* $h \in F_q^*$ *элементийн хувьд* $g^x = h$ *байх* $0 \le x \le q-1$ *тоог бодлогыг өргөтгөсөн ерөнхий дүгнэлт гэнэ.[12]*

#### 3.1.1 Диффе Хэллмэн түлхүүрийн хэлэлцээр хийх

*Оролт: (p,g) p-том анхны тоо, g-* $F_q^*$ *төгсгөлөг талбарын үүсгэгч элемент*

*Гаралт: Хоёр талын хооронд илгээгдэх* $F_q^*$ *талбарын элемент*

a. *Alice* $a \in [1, p-1]$ *тоог нууцаар сонгоно*
$A \leftarrow g^a (mod\ p)$ *тооцно*
A тоог Bob илгээнэ

b. *Bob* $b \in [1, p-1]$ *тоог нууцаар сонгоно*
$B \leftarrow g^b (mod\ p)$ *тооцно*
$B$ тоог *Alice* илгээнэ

c. Alice $k \leftarrow B^a (mod\ p)$ утгыг тооцож нууц түлхүүрийг гарна

d. Bob $k \leftarrow A^b (mod\ p)$ утгыг тооцож нууц түлхүүрийг гарна

$g \in F^*p$ үүсгэгч элемент $0 < a, b < p$ тоонуудын хувьд $g^a (mod\ p), g^b\ (mod, p)$ утгууд мэдэгдэж байхад $g^{a,b} (mod, p)$ олох бодлого нь хүнд юм.

#### 3.1.2 Диффе Хэллмэн шифрлэлт

$\left(g^{ab}\right)^{-1}$ утгыг тооцох: $\left|F_p^*\right| = p-1, b, g^a|$ утгуудыг мэднэ. $F_p^*$ цикл бүлэг учир $\forall x \in .$ $F_p^*: x^{|F_p^*|} = x^{p-1} = 1 (mod\ p)$ байна. Эндээс $(g^a)^{p-1-b} = g^{a(p-1-b)} = g^{a(p-1)}\, g^{-ab} = (g^{p-1})^a\, g^{-ab} = 1^a \left(g^{ab}\right)^{-1} = (g^{ab})^{-1}$

*a.Оруулах* $m \in [0, p-1]$ *мэдээ, ил түлхүүр* $g^b \quad k = g^{ab} (mod\ p)$ *нууц түлхүүр*

*b.Гаралт* $c \leftarrow m g^{ab} (mod\ p)$ *шифр мэдээ*

#### 3.1.3 Диффе Хэллмэн код тайлалт

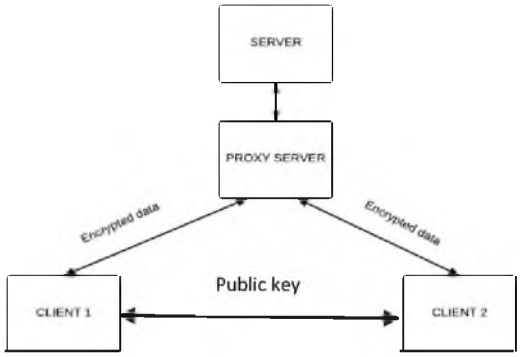
*a.Оруулах* $c \in [0, p-1]$ *шифр мэдээ,* $g^a$ *ил түлхүүр* $p, b$ *нууц тоонууд*

*b.Гаралт:* $m \leftarrow c(g^{ab})^{-1} \equiv c(g^a)^{p-1-b}\ mod (mod\ p)$

### *4. Чат өрөөний аюулгүй байдал*

#### 4.1 Socks5 хэрэглээ

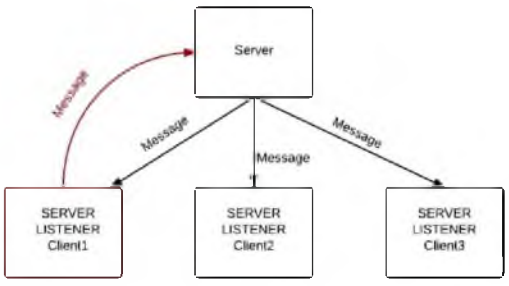
Socks5[13] энэ нь сервер дээр байрших бөгөөд хэрэглэгч серверлүү ямар нэгэн хүсэлт явуулахад тухайн хүсэлтийг барьж аваад өөрийн нууцлалтай "https" протоколоор дамжуулан тухайн хүсэлтийг үндсэн сервер рүү дамжуулна. Ингэснээр тухайн хэрэглэгчийн явуулсан хүсэлт Proxy сервер лүү хүсэлт илгээгдэж Proxy сервер нь жинхэнэ сервертэй харьцах юм. Ингэж Proxy сервер ашигласнаар тухайн клиентийн хүсэлтийг дундаас нь барьж авч серверлүү нэвтрэх гэсэн довтлогчоос хамгаалж байна. Хэрвээ довтлогч сервер рүү дайрвал тэнд ямар ч сервер байхгүй хоосон хүсэлтийн Proxy сервер байх учир аюулгүй байдал бүрэн хангагдаж байгаа юм.




Зураг.3 Proxy server

Хүснэгт1. Proxy server үйл ажиллагааны тайлбар

| Төлөв | | Үйл ажиллагаа | Тайлбар |
|---|---|---|---|
| Server | Proxy server | Хэрэглэгчээс ирсэн хүсэлтэнд тохирох хариуг Proxy сервер-лүү дамжуулна. | Proxy сервер нь үндсэн сервер-ийн хувьд цорын ганц харьцах клиент юм.Proxy Сервер болон үндсэн серверлүү хэрэглэгчээс ирсэн хүсэлтийг “https” портколоор шифрлээд серверийн порт руу дамжуулна. Сервер тухайн хүсэлтийг боловсруулаад тохирох хариу болон цаашид дамжих портуудыг proxy серверлүү буцааж дамжуулна. Тухайн сервэрээс ирсэн хариуг Proxy сервер тохирох портууд руу шууд дамжуулна. |
| Proxy server | Client1 | Encryption data | Үндсэн сервер Proxy Серверт дамжих портыг мэдэгдэнэ. Ингэснээр Proxy сервер үндсэн серверээс ирсэн портруу шууд дамжина. |
| | Client2 | Encryption data | |
| Client1 | Client2 | Public key | deffie hellman үүсгэсэн хувийн түлхүүрийг ашиглан нийтийн түлхүүр солилцоно. |




Зураг.4 Socket серверийн үйл ажиллагаа

| Төлөв | | Үйл ажиллагаа | Тайлбар |
|---|---|---|---|
| Server | Server listener client1,2,3 | message | Нийтийн чат дээр нэг хэрэглэгч мессэж бичихэд сервер бусад бүх идэвхитэй портууд руу тухайн мессежийг дамжуулна. |
| Server listener client1 | Server | message | Чатаар ярилцаж байгаа хэрэглэгчдийн мессэж серверт буцааж дамжигдана |

Хүснэгт.2 Socket серверийн үйл ажиллагааны тайлбар

**4.2 Чат өрөөнийн мессежийг Deffie hellman түлхүүр солилцох аргыг хэргэлэж Javascript дээр кодыг бичих**

A. Client холбогдонгуут хувийн болон нийтийн public түлхүүрүүд үүсгэх функцууд **(generatePrivateKey, generatePublicKey)**

Дараах функц нь deffie hellman хувийн түлхүүрийг дурын байдлаар үүсгэж үүсгэж байна.

```
var p=107, g=2;
var usernames=[];
function generatePrivateKey
{   return Math.fioor(Math.random() * 10) + 1;}
```

B. Чатлах үед нийтийн түлхүүрүүд солилцоно.
Харин дараах deffie hellman функц нь үүсгэсэн хувийн түлхүүрээ ашиглан нийтийн түлхүүр үүсгэх функц юм.

```
function generatePublicKey(privateKey)
{return ((Math.pow(g, privateKey))%p);}
```

C. Чатлаж байгаа хүнийхээ нийтийн түлхүүр болон өөрийн хувийн түлхүүрээс Diffie hellman алгоритмыг хэрэглэж мессеж шифрлэлт хийх түлхүүр гаргаж авах **(generateDecryptionKey функц)**

```
function generateDecryptionKey(privateKey, publicKey)
{return ((Math.pow(publicKey, privateKey))%p);}
```

D. **(encDecDataфункц)** энэ функц нь чатын мессежийг шифрлэх болон кодыг тайлалт хийнэ

```
function encDecData(str, k) {
        var encoded = "";
            for (i=0; i<str.length;i++) {
            var a = str.charCodeAt(i);
            var b = a ^ k;
            encoded = encoded+String.fromCharCode(b);
                    }
                return encoded;
                }function generateDecryptionKey(privateKey, publicKey)
{return ((Math.pow(publicKey, privateKey))%p);}
```

## ДҮГНЭЛТ

Энэхүү чат өрөөнд харилцах хэрэглэгчдийн дамжигдах мессэж нь Диффе Хеллман түлхүүрийн хэлэлцээрээр нууцлагдаж байна. Чатын давуу тал нь мессэжийг баазад хадгалахгүй шууд socket-ээр бодит хугацаанд явагдахаар хийсэн тул хэрэглэгч цонхоо хаах үед тухайн хэрэглэгчийн чаталсан бүх түүх устана.

Тухайн чатын серверийг localhost дээр ажиллуулахдаа GITBASH-ийг нээгээд 1. Cd Desktop/chatex， 2.Node app.js Энэ 2 командыг ажиллуулснаар сервер ажиллаж эхэлнэ. Эцсийн үр дүн нийтийн чат болон хувийн чат өрөөний мессэж шифрлэлт нь сервер дээр дараах байдалтай харагдаж байна.


Зураг.5 Сервер дээрх шифрлэлт

**АШИГЛАСАН ХЭВЛЭЛ**

[1] [6] Kahate, A. (2008) Cryptography and Network Security. McGraw-Hill.
[2] about javascript http://ecomputernotes.com/js/javascript-tutorial/what-is-javascript
[3] http://en.wikipedia.org/wiki/Node.js
[4] http://jquery.com/
[5] gitbash: http://msysgit.github.io/
[6] H. Kikuchi, M. Tada, and S. Nakanishi. Secure Instant Messaging protocol preserving confidentiality against administrator. In 18th International Conference on Advanced Information Networking and Applications, AINA 2004, volume 2, pages 27–30, Fukuoka, Japan, Mar. 2004.
[7] America Online, Inc. AOL Instant Messenger. http://www.aim.com
[8] ICQ Inc. ICQ Pro 2003b. http://www.icq.com
[9] Microsoft. MSN Messenger. http://messenger.msn.com
[10] Yahoo! Inc. Yahoo! Messenger. http://messenger.yahoo.com
[11] Merkle, Ralph C (April 1978). "Secure Communications Over Insecure Channels". *Communications of the ACM* **21** (4): 294–299. doi:10.1145/359460.359473. "Received August, 1975; revised September 1977"
[12] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory* **22** (6): 644–654. doi:10.1109/TIT.1976.1055638.
[13] Socks5 тухай http://en.wikipedia.org/wiki/SOCKS#SOCKS5

## *JAVASCRIPT SOCKET SECURITY CHATROOM*

***Bulganmaa.T, Zhang Jiu Xing***

*College of computer science, Inner Mongolian University, Hohhot*

*With the wide use of the Internet, virtually everyone is now connected to each other through their computers. This has led to a positive impact in the human environment socially, economically and in their day-to-day transactions. This being a security issue, information security therefore plays a vital role in Internet transactions. It can be deduced that secure digital communication is necessary for many aspects relating to web based activities, e-commerce, and secured instant messaging. More so for private, confidential, and vital information, the reality that safe, secure communication between parties communicating over the Internet is now a necessity cannot be overstated. Cryptography is an indispensable tool for protecting information in computer systems. Today's cryptosystems are divided into two categories: symmetric and asymmetric. The difference lies in the keys used in decryption and encryption—symmetric cryptography uses the same key for both of these processes, whereas asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. The Diffie-Hellman key exchange is one of the more well-known asymmetric Soket is API of internet programming and also standard of internet programming which is used for Unix, Linux and Windows systems. Client is the regular technique. That is used with the internet programming. In this article I have tried to create the Chat room based on a website which deals with exchanging the information securely with Deffie Hellman exchanging key method using the Javascript Soket.*