Батлав. Мэдээллийн сүлжээ, аюулгүй байдлын салбарын эрхлэгч:

..... /доктор (Ph.D) Б.Мөнхбаяр/

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

Дипломын төсөл гүйцэтгэх төлөвлөгөө

Дипломын төслийн сэдэв:
Монгол: " Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь"
Англи: " Developing Prototype System of Proxy Re-Encryption Scheme"

Төслийн зорилго: Proxy Re-Encryption схемийн хэрэглээнүүдийг судалж, нэгэн хэрэглээг хэрэгжүүлэх туршилтын систем хөгжүүлэх

Гүйцэтгэх оюутны овог нэр: А.Мягмарцэрэн/B190970106/
Холбоо барих утас: 99754252

№	Ажлын бүлэг, хэсгийн нэр	эзлэх хувь	дуусах хугацаа
Бүлэг №1. Өгөгдөл хуваалцах үйлчилгээний тухай			
1	1.1 Өгөгдөл хуваалцах үйлчилгээний тухай 1.2 Өгөгдлийн аюулгүй байдал 1.3 Шифрлэх схемүүд 1.4 Файл шифрлэх аргууд	20%	
Бүлэг №2. Прокси дахин шифрлэлтэд суурилсан файл хуваалцах систем			
2	2.1 Прокси дахин шифрлэлт 2.2 Хөгжүүлэх технологи, хэл сонгох 2.3 Хөгжүүлэлтийн орчин бэлдэх	40%	
Бүлэг №3. Прокси дахин шифрлэлтэд суурилсан файл хуваалцах систем хөгжүүлэх			
3	3.1 Системийн шаардлага 3.2 Системийн загвар 3.3 Системийн хөгжүүлэх 3.4 Файл хуваалцах системийг турших	40%	
Бүлэг №4. Ерөнхий дүгнэлт			

Төлөвлөгөөг боловсруулсан оюутан: ..... /А.Мягмарцэрэн/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 30% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-1		IV/03-IV/07	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-1 хийсэн багш: ..... /доктор (Ph.D) В.Нямсүрэн/

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 50% -с багагүй байна.	Огноо	доктор (Ph.D), Ц.Энхтөр багшийн гарын үсэг
1	Үзлэг-2			IV/17-IV/21	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-2 хийсэн багш: ..... /доктор (Ph.D), Ц.Энхтөр/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 70% -с багагүй байна.	Огноо	магистр Ц.Манлайбаатар багшийн гарын үсэг
1	Үзлэг-3			V/08-V/12	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-3 хийсэн багш: ..... /магистр Ц.Манлайбаатар/

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 90% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-4		V/15-V/19	

№	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн үнэлгээ (30 оноо)	Огноо	Удирдагч багшийн гарын үсэг
1		V/17	

Удирдагч багш: ..... /доктор (Ph.D) В.Нямсүрэн/

Жич: Удирдагч багш өөрийн үнэлгээгээ 30 хүртэл оноогоор өгөх ба үнэлгээ тавьсан хуудсыг оюутанд буцааж өгөлгүй төгсөлтийн нарийн бичгийн даргад хураалгана уу.

ТӨГСӨЛТИЙН АЖЛЫН ЯВЦ

№	Хийж гүйцэтгэсэн ажил	Биелсэн хугацаа	Удирдагчийн гарын үсэг
1	Бүлэг №1. Proxy Re-Encryption схемийн онолын хэсэг	2023-4-28	
2	Бүлэг №2. Серверт шифрлэгдсэн файл хуваалцах судалгаа	2023-4-21	
3	Бүлэг №3. Proxy re-encryption систем хөгжүүлэх	2023-5-18	
4	Бүлэг №4. Ерөнхий дүгнэлт	2023-5-25	

Ажлын товч дүгнэлт

.....
.....
.....
.....
.....
.....
.....

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

ЗӨВШӨӨРӨЛ

Оюутан А.Мягмарцэрэн–н бичсэн төгсөлтийн ажлыг УШК-д хамгаалуулахаар тодорхойлов.

Салбарын эрхлэгч: ..... /доктор (Ph.D) Б.Мөнхбаяр/

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

ШҮҮМЖИЙН ХУУДАС

Мэдээллийн сүлжээ, аюулгүй байдлын салбар–н салбарын төгсөх курсийн оюутан А.Мягмарцэрэн-н "Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь" сэдэвт төгсөлтийн ажлын шүүмж.

1. Төслөөр дэвшүүлсэн асуудал, үүнтэй холбоотой онолын материал уншиж судалсан байдал. Энэ талаар хүмүүсийн хийсэн судалгаа, түүний үр дүнг уншиж тусгасан эсэх.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

2. Төслийн ерөнхий агуулга. Шийдсэн зүйлүүд, хүрсэн үр дүн. Өөрийн санааг гарган, харьцуулалт хийн, дүгнэж байгаа чадвар.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

3. Эмх цэгцтэй, стандарт хангасан өөрөөр хэлбэл диплом бичих шаардлагуудыг биелүүлсэн эсэх. Төсөлд анзаарагдсан алдаанууд, зөв бичгийн болон өгүүлбэр зүйн гэх мэт /Хуудас дугаарлагдаагүй, зураг хүснэгтийн дугаар болон тайлбар байхгүй, шрифт хольсон, хувилсан зүйл ихээр оруулсан/.

   .....
   .....
   .....
   .....
   .....

4. Төслөөр орхигдуулсан болон дутуу болсон зүйлүүд. Цаашид анхаарах хэрэгтэй зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

5. Төслийн талаар онцолж тэмдэглэх зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

6. Ерөнхий оноо. (30 оноо)

   .....

Шүүмж бичсэн: ..... /магистр Г.Баяр/

Ажлын газар: .....

Хаяг (Утас) .....

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Хураангуй

Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь

А.Мягмарцэрэн
b190970106@must.edu.com

Түлхүүр үгс: мэдээллийн аюулгүй байдал, прокси дахин шифрлэлт

Товчилсон үгс

PRE **P**roxy **R**e-**E**ncryption
BBS **B**laze **B**leumer **S**trauss

БҮЛЭГ 1

Proxy Re-Encryption схемийн онолын хэсэг

1.1 Өгөгдөл хуваалцах үйлчилгээ

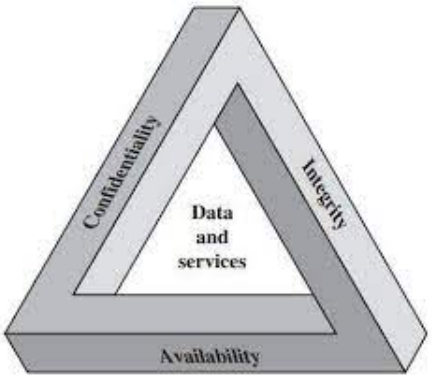
Өгөгдөл хуваалцах гэдэг нь өгөгдлийг программ болон хэрэглэгчид эсвэл байгуулгууд хоорондоо ашиглах боломжтой болдог. Хамтын ажиллагааг сайжруулаж хоорондын харилцаа холбоог хөнгөвчлдөг.

1.2 Өгөгдөл аюулгүй байдал

1.3 Шифрлэлт, түүний ач холбогдол, ангилал, хэрэглээ

Мэдээллийн аюулгүй байдал үндсэн гурван зарчимыг тэнцвэртэй хангахыг зоридог.

- **Нууцлаг байдал (Confidentiality)**: Мэдээлэлийг нууц хэвээр нь хамгаалж үлдэх. Санаатай болон санамсаргүй мэдээллийг зөвшөөрөлгүй хуваалцах тараахаас сэргийлэх.
  - Өгөгдлийн нууцлал (Data1 confidentiality)
  - хувийн нууц (Privacy)
- **Бүрэн бүтэн байдал (Integrity)**: Өгөгдөлд үнэн зөв найдвартай гадны нөлөө ороогүйг шалгах, бүрэн бүтэн хадаглах.
  - Өгөгдлийн бүрэн бүтэн байдал (Data integrity)
  - Системийн бүрэн бүтэн байдал (System integrity)
- **Хүртээмжтэй байдал (Availability):** Тухайн системийн хэрэглэгчид хүртээмжтэй байх.



Зураг 1.1: CIA гурвалжин

Криптографд шифрлэлт нь энгийн текстийг (жишээ нь, эх мессеж) шифр текст (жишээ нь, шифрлэгдсэн эсвэл кодлогдсон мессеж) болгон хувиргахад ашигладаг алгоритм юм. Шифрлэлтийн зорилго нь мессежийг түлхүүргүй хүн унших боломжгүй болгох явдал юм.

Мэдээлэл болон өгөгдлийг шифрлэлт хийснээр нууцлаг байдлыг хангах хамгийн том давуу тал юм. Бүрэн бүтэн байдал болон хүртээмжтэй байдлыг ч шифрлэлт нь хангах боломжтой. Шифрлэлт ерөнхийд нь гурав ангилна.

- **Тэгш хэмт шифрлэлт (symmetric)** нь шифрийг тайлах болон шифрлэхдээ нэг түлхүүр ашигладаг. Уламжлалт шифрлэлт гэх нь бий. Уламжлалт

(компьютероос өмнөх үе) тэгш хэмтэй шифрүүд нь орлуулах эсвэл шилжүүлэх аргыг ашигладаг. Орлуулах арга нь энгийн текстийн элементүүд (тэмдэгтүүд, битүүд) шифр текстийн элементүүдэд солино оруулж тавина. Шилжүүлэх техник нь энгийн текстийн элементүүдийн байрлалыг системтэйгээр шилжүүлдэг. Тэгш хэмт шифрлэлт нь хоёр төрөлтэй.

  - Урсгал шифрлэлт (Stream шифрлэлт) RC4 болон ChaCha20 гэх мэт.
  - Блок шифрлэлт (Block шифрлэлт) AES, DES, болон 3DES гэх мэт.

- **Тэгш бус шифрлэлт (asymmetric)** нь нийтийн болон хувийн хоёр түлхүүртэй. Нийтийн түлхүүр нь нийтэд нээлтэй байдаг. Хувийн түлхүүрийг эмзэгшигч нь нууцалж алдахгүй байх ёстой.

- **Хэш (Hash)** функц нь хувьсах урттай мессежийг тогтмол урттай хэш утга шифрлэдэг. Ихэнх хэш функц нь шахалтын алгоритм ашигладаг.

Криптограф нь дамжуулалтын явцад мессежийг хөндлөнгөөс өөрчлөлт ороогүй эсэхийг шалгаж бүрэн бүтэн байдлыг хангадаг. Хэш, мессежийг баталгаажуулалтын код (MACs), тоон гарын үсэг (Digital Signatures) ашигладаг байдаг.

Мессежийн баталгаажуулалтын код (MACs) нь авсан өгөгдөл нь илгээсэнтэй яг таарч (өөрчлөлт оруулах, устгах) мөн илгээгчийн баталгаажуулдаг. Нууц түлхүүр ашигдаг. MAC нь хувьсах урттай мессежийг нууц түлхүүр болгон авч, баталгаажуулах код үүсгэдэг. MAC нь хэш функц болон тэгш хэмт блок шифрлэлтийг ашиглдаг.

Тоон гарын үсэг (Digital Signatures)

Ихэвчлэн шифрлэгдсэн мессэж, энгийн мессежийн хэшийг бүтээгчийн хувийн түлхүүрийн хэшийг авч харьцуулж баталгаажуулдаг.

1.4 Орчин үеийн ширфлэлтийн схемүүд

Өгөгдлийг хэрхэн найдвартай нууцлаж хамгаалах нь чухал болсон. Зөвхөн шифрлэхээс гадна үүнийг схемчилж илүү хурдан өөр өөрсдийн давуу талтай схемүүдмйг хөгжүүлж гаргаж ирсэн.

Танилтад суурилсан шифрлэлт (IBE)

Нийтийн түлхүүрийн оронд өөрийн хувийн мэдээллийг ашиглан өгөгдлийг шифрлэх, тайлах боломжийг олгодог нийтийн түлхүүрийн шифрлэлтийн нэг төрөл юм. IBE-ийг хэрэглэгчдийг таних тэмдэгээр нь мэддэг тохиолдолд аюулгүй өгөгдөл хуваалцахад ашиглаж болно.

Шинж чанарт суурилсан шифрлэлэт (ABE)

Энэ нь нас, албан тушаал, байгууллагын үүрэг зэрэг урьдчилан тодорхойлсон шинж чанарт үндэслэн өгөгдөлд хандах боломжийг олгодог шифрлэлтийн төрөл юм. ABE нь өгөгдөлд хандах хандалтыг нарийн хянахад ашиглагдаж болох ба зарим шинж чанарууд дээр үндэслэн хандалт олгосон хувилбаруудад ашиглаж болно.

Гомоморф шифрлэлт (HE)

Энэ нь шифрлэгдсэн өгөгдлийг эхлээд тайлахгүйгээр тооцоолол хийх боломжийг олгодог шифрлэлтийн төрөл юм. Тооцоолол хийх боломжийг олгохын зэрэгцээ өгөгдлийг нууцлах шаардлагатай тохиолдолд HE-г аюулгүй өгөгдөл боловсруулахад ашиглаж болно.

Secure multiparty computation (MPC)

Энэ талууд өөрсдийн оролтыг бие биедээ ил гаргахгүйгээр хувийн оролт дээрээ функцийг хамтран тооцоолох боломжийг олгодог криптографийн арга юм. Мэдээллийн нууцлалыг хадгалах, олон тал хамтран ажиллах шаардлагатай тохиолдолд MPC-ийг аюулгүй өгөгдөл боловсруулахад ашиглаж болно.

1.5 Proxy Re-Encryption схем

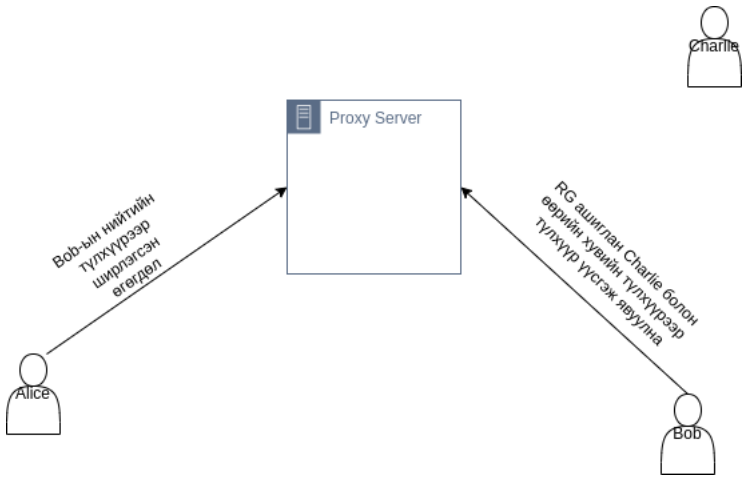
Прокси дахин шифрлэлт нь нийтийн түлхүүрээр шифрлсэн өгөгдөлийг дахин ширфлэж өөр хувийн түлхүүрээр тайлах боломжийг олгодог.

Үндсэн хоёр төрөлтэй.

- Нэг чиглэлт (Unidirectional PRE)
- Хоёр чиглэлт (Bidirectional PRE)

Нэг чиглэлт PRE (KE, RG, E, R, D) хэсгүүдээс тогтоно.

1. Алис, Боб болон Чарли хувийн болон нийтийн түлхүүрийг үүсгэнэ. (KE)
2. Алис Боб-д зориулж өгөгдлөө шифрлэж серверт байршуулна.
3. Боб Алис-ын өгөгдлийг Чарли-тай хуваацлахын тулд RE(pkB,skB,pkC,skC) шифрлэж серверт байршуулна. Чарлигийн хувийн заавал шаардахгүй үүсгэж болно.
4. Боб RE-г ашиглаж үүсэгсэн түлхүүрийг серверт явуулж Алисын файлыг дахин шифрлэж Чарли тайлах боломжтой болно.



Зураг 1.2: Proxy Re-encryption scheme

Давуу талууд:

- Нууцлалыг сайжруулна: PRE нь оролцогч талуудын хувийн мэдээллийг задруулахгүйгээр өгөгдлийг хуваалцахыг зөвшөөрснөөр нууцлалыг сайжруулахад тусална. Энэ нь талууд нууцаар эсвэл хувийн нууц мэдээллийг задруулахгүйгээр мэдээллээ хуваалцахыг хүссэн тохиолдолд хэрэг болно.

- Нарийн төвөгтэй байдлыг багасгасан: PRE нь итгэмжлэгдсэн гуравдагч этгээдэд шифрлэлт болон шифрийг тайлах үйл явцыг удирдах боломжийг олгосноор шифрлэлт болон түлхүүрийн удирдлагын нарийн төвөгтэй байдлыг багасгахад тусална. Энэ нь ялангуяа олон талын оролцоотой, гол менежмент нь төвөгтэй, удирдахад хэцүү болж болзошгүй тохиолдолд хэрэг болно.

Сул талууд:

- Проксид итгэх: PRE нь дахин шифрлэлтийг гүйцэтгхэд гуравдагч талын прокси дээр тулгуурладаг ба схемийн аюулгүй байдал нь прокси талаас хамаарна.

- Хязгаарлагдмал өргөтгөх чадвар: PRE нь өргөтгөх чадварын хувьд хязгаарлагдмал байж болно. Учир нь хэрэглэчдийн тоо нэмэгдэхийн хэрээр олон талыг дэмжихэд шаардлагатай дахин шифрлэлтийн түлхүүрүүдийн тоо хурдацтай өсөх болно. Энэ нь гол менежментийг төвөгтэй болгож, удирдахад хэцүү болгодог.

- Potential for replay attacks: PRE нь халдагч хариуг зогсоож хандах эрхийг өөрт ашигтай солих боломжтой.

- Хүчингүй болгоход хүндрэлтэй байдал: PRE дахь өгөгдөлд хандах эрхийг цуцлах нь ялангуяа олон тал оролцсон тохиолдолд хэцүү байж болно. Хэрэв аль нэг талын дахин шифрлэлтийн түлхүүр алдагдсан бол бусад талуудын мэдээлэлд хандах эрхэд нөлөөлөхгүйгээр өгөгдөлд хандах эрхийг цуцлах нь хэцүү байж болно.

- Хязгаарлагдмал хэрэглээ: PRE нь харьцангуй шинэ бөгөөд шинээр гарч ирж буй технологи хэвээр байгаа бөгөөд илүү уламжлалт шифрлэлтийн схемүүдтэй харьцуулахад хэрэглээ нь хязгаарлагдмал байдаг. Энэ нь технологийг хэрэгжүүлэх, удирдах туршлагатай мэргэжилтнүүд бага байдаг.

1.6 Бүлгийн Дүгнэлт

Энэ бүлэгт орчин үеийн шифрлэлтийн схеммүүдмйг судалж прокси дахин шифрлэлэт нь бусад схеммүүдээс ямар давуу тал сул талыг судалж харицуулсан. Системийн хөгжүүлэлт ерөнхий загварийг гаргаж юу хэрэгтэй сангуудыг ашиглан системийн хөгжүүлэлтыг хийж элсэн.

БҮЛЭГ 2

Серверт шифрлэгдсэн файл хуваалцах судалгаа

2.1 Файл шифрлэх аргуудыг судлах

2.2 Сервер талын шифрлэлт болон клиент талын шифрлэлт судлах

2.3 Proxy-encryption ашиглсан системүүд

БҮЛЭГ 3

Proxy re-encryption систем хөгжүүлэх

3.1 Системийн үйл ажилгааны загвар

3.2 Хөгжүүлэх технологи, хэл сонгох

3.3 Системийн хөгжүүлэх