МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ
ХЭРЭГЛЭЭНИЙ ШИНЖЛЭХ УХААН, ИНЖЕНЕРЧЛЭЛИЙН СУРГУУЛЬ
МЭДЭЭЛЭЛ, КОМПЬЮТЕРИЙН УХААНЫ ТЭНХИМ

Даянгийн Балжинням

Криптографын зарим алгоритм, программ

(Some algorithms and programs for cryptography)

Програм хангамж(D061302)
Бакалаврын судалгааны ажил

Улаанбаатар

2023 оны 11 сар

МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ
ХЭРЭГЛЭЭНИЙ ШИНЖЛЭХ УХААН, ИНЖЕНЕРЧЛЭЛИЙН СУРГУУЛЬ
МЭДЭЭЛЭЛ, КОМПЬЮТЕРИЙН УХААНЫ ТЭНХИМ

Криптографын зарим алгоритм, программ
(Some algorithms and programs for cryptography)

Програм хангамж(D061302)
Баклаврын судалгааны ажил

Удирдагч: _____ Д. Гармаа

Хамтран удирдагч: _____ Н. Оюун-Эрдэнэ

Гүйцэтгэсэн: _____ Д. Балжинням (20B1NUM0563)

Улаанбаатар

2023 оны 11 сар

Зохиогчийн баталгаа

Миний бие Даянгийн Балжинням ”Криптографын зарим алгоритм, программ” сэдэвтэй судалгааны ажлыг гүйцэтгэсэн болохыг зарлаж дараах зүйлсийг баталж байна:

- Ажил нь бүхэлдээ эсвэл ихэнхдээ Монгол Улсын Их Сургуулийн зэрэг горилохоор дэвшүүлсэн болно.
- Энэ ажлын аль нэг хэсгийг эсвэл бүхлээр нь ямар нэг их, дээд сургуулийн зэрэг горилохоор оруулж байгаагүй.
- Бусдын хийсэн ажлаас хуулбарлаагүй, ашигласан бол ишлэл, зүүлт хийсэн.
- Ажлыг би өөрөө (хамтарч) хийсэн ба миний хийсэн ажил, үзүүлсэн дэмжлэгийг дипломын ажилд тодорхой тусгасан.
- Ажилд тусалсан бүх эх сурвалжид талархаж байна.

Гарын үсэг: _____

Огноо: _____

ГАРЧИГ

ЗУРГИЙН ЖАГСААЛТ

ХҮСНЭГТИЙН ЖАГСААЛТ

Кодын жагсаалт

УДИРТГАЛ

Энэхүү дипломын ажилд криптографийн янз бүрийн алгоритм, программуудыг системтэйгээр судалсан бөгөөд үндсэн зорилго нь тэдгээрийн үндсэн бүтэц, үйл ажиллагааны механизм, практик хэрэглээг ойлгох явдал юм. Энэхүү судалгааны ажилд уламжлалт болон шинээр гарч ирж буй криптографийн алгоритмуудыг судалж, гүйцэтгэл, аюулгүй байдал, үр ашигтай байдалд үндэслэн харьцуулсан судалгааг хийв.

Энэхүү судалгаанд өгөгдлийн шифрлэлтийн стандарт (DES), дэвшилтэт шифрлэлтийн стандарт (AES), Ривест-Шамир-Адлеман (RSA), эллиптик муруй криптографи (ECC) зэрэг тэгш хэмтэй болон тэгш бус криптограф алгоритмуудыг нарийвчлан судалсан.

Төгсөлтийн ажлын практик хэсэгт хэд хэдэн криптографийн програмуудыг боловсруулж, харьцуулсан ба орчин үеийн стандартыг хангасан тоон гарын үсгийн системийг үүлэн технологид суурилан бүтээсэн.

Зорилго

Үүлэн технологид суурилсан тоон гарын үсгийн системийг бүтээснээр хэрэглэгчид өөрсдийн цахим гарын үсгээр баталгаажсан файлуудыг интернет хуваалцах боломжийг бүрдүүлэх гол зорилготой юм.

Зорилт

Бүрэн бүтэн байдал нь хөндөгдөөгүй, эх сурвалж нь тодорхой файлыг хуваалцах боломжийг бүрдүүлэх.

Үндэслэл

Монголд одоогийн байдлаар үүлэн технологид суурилсан тоон гарын үсгийн систем байхгүй байгаа нь хэрэглэгчид энэхүү технологийг ашиглахад төвөгтэй болгож байна. Ихэнх клайнт програмуудууд нь зөвхөн Windows үйлдлийн систем дээр ажиллахаар хийгдсэн нь нийцтэй байдлыг хангахгүй байна.

1. ОНОЛЫН СУДАЛГАА

1.1 Тэгш хэмт крифтограф

Тэгш хэмт крифтографт шифрлэлт болон шифр тайлах түлхүүрүүд адил байна. Тэгш хэмт алгоритм нь Тэгш бус хэмт шифрлэлтээс харьцангуй хурдан ажилдаг. Гэвч нууцалсан мэдээллийг тайлж унших түлхүүр болон нууцлах түлхүүр адилхан байх нь харилцагч талууд урьдчилан түлхүүрээ хоорондоо тохиролцох шаардлагыг гаргаж ирдэг. Энэ нь сул тал болох эрсдэлтэй. Хэрвээ гуравдагч этгээд түлхүүрийг олж авбал бүх нууцалсан мэдээллийг үзэх боломжтой болох юм.

Хамгийн түгээмэл хэрэглэгддэг тэгш хэмт шифрлэлтийн алгоритм бол Бельгийн криптографич Жоан Даемен, Винсент Рижмен нарын боловсруулсан Advanced Encryption Standard (AES) юм. AES нь хуучин Data Encryption Standard (DES)-ийг сольсон бөгөөд одоо дэлхий даяар ашиглагдаж байна.[1]

1.1.1 Блокон шифрлэлт

Хэрвээ эх ба шифрлэгдсэн тексүүдийн огторгуй нь ямар нэг $\sum^n$ олонлог байвал тухайн криптографыг блокон шифрлэлт гэнэ. Блокон шифрлэлтэнд өгсөн мэдээг тэнцүү *n* урттай хэсгүүдэд хуваан шифрлэдэг.[3]

Блок шифрт энгийн текстийн блокийг бүхэлд нь авч, шифрлэгдсэн текстийн блокыг үүсгэхэд ашигладаг. Блокийн хэмжээг ерөнхийдөө шифрийн алгоритмаар тодорхойлно. Ихэнх блок шифрүүдийн хувьд энэ нь ихэвчлэн 64 эсвэл 128 бит байдаг ба зарим тохиолдолд нууцлалыг нэмэх зорилгоор 256, 512 бит ч байж болдог.

Хоёр төрлийн алгоритм ашиглах ба нэг нь шифр хийхэд нөгөө нь тайлахад ашиглагддаг. Эдгээр нь *n* урттай бит болон *k* бит урттай түлхүүрийг авч *n* бит урттай блок үүсгэнэ. $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. Тайлах алгоритм *D*-г нууцлах функцын урвуу гэж тодорхойлж

болно.

$D : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

$\forall k \in \{0,1\}^k, \forall m \in \{0,1\}^n, D(k, E(k,m)) = m$

[4]

1.1.2 Урсгалын шифрлэлт

Урсгалын шифрлэлт гэдэг нь өгөгдлийг урсгал маягаар нэг дор нэг битийг Криптографын алгоритм болон түлхүүрээ ашиглан шифрлэх арга юм. Урсгалын шифрын давуу тал нь блок шифрлэлтээс харьцангуй хурдан ажиллахаас гадна, хэрэгжүүлэлтэнд бага код ордог билээ. Гэсэн хэдий ч орчин үед түгээмэл ашиглагдахаа больсон ба элдэв халдагад түгээмэл өртдөг нь үүнтэй холбоотой. Жишээ нь RC4 гэх Урсгалын шифрлэлтийн алгоритм нь WEB болон WPA хамгаалалтад ашиглагддаг байсан хэдий ч хангалттай сайн хамгаалалт болж чадахгүй байгаа тул, хэрэглээнээс халагдаж байна.

1.2 Өгөгдөл шифрлэлтийн стандарт

1.2.1 DES алгоритм

DES (Data Encryption Standard) нь 1970-аад онд хөгжүүлэгдсэн тэгш хэмт блок шифрлэлтийн алгоритм юм. DES нь 64 бит урттай блок дээр ажиллах ба үүнийг 32-бит урттай хоёр хэсэг L_0, R_0 болгон хувааж, баруун талын 32-бит урттай хэсгийг олон янзын аргаар хувиргаж эцэст нь L_0-тэй XOR үйлдэл хийнэ. Арван зургаан үе хувиргалтын дараагаар L_0, R_0 нийлүүлж 64 бит шифрлэгдсэн блокыг үүснэ.

Шинжүүд

1. Түлхүүрийн урт: DES нь 56 битийн түлхүүрийг ашигладаг бөгөөд анхандаа хангалттай аюулгүй байдлыг хангадаг гэж бодож байсан ч одоо Brute Force халдлагад маш эмзэгт тооцогддог.

2. Symmetric Encryption: DES нь шифрлэлт болон шифрийг тайлахад ижил түлхүүр ашигладаг. Тиймээс түлхүүрийг илгээгч, хүлээн авагч хоёулаа мэдэж, нууцлах ёстой.

3. Блок шифр: DES нь тусдаа бит биш харин өгөгдлийн блокууд дээр ажилладаг. Энэ нь их хэмжээний өгөгдлийг шифрлэх шаардлагатай програмуудад тохиромжтой.

4. DES үйлдлүүд: DES нь Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) зэрэг хэд хэдэн үйлдлийн горимыг дэмждэг.

5. DES нь детерминистик: ижил текст болон ижил түлхүүрийн хувьд шифрлэгдсэн текст үргэлж ижил байх болно.

хэдийгээр 3-DES гэж байдаг хэдий ч энэ нь тооцоолол ихээр шаарддаг тул цаашид ашиглагдах нь зогссон.

1.2.2 AES

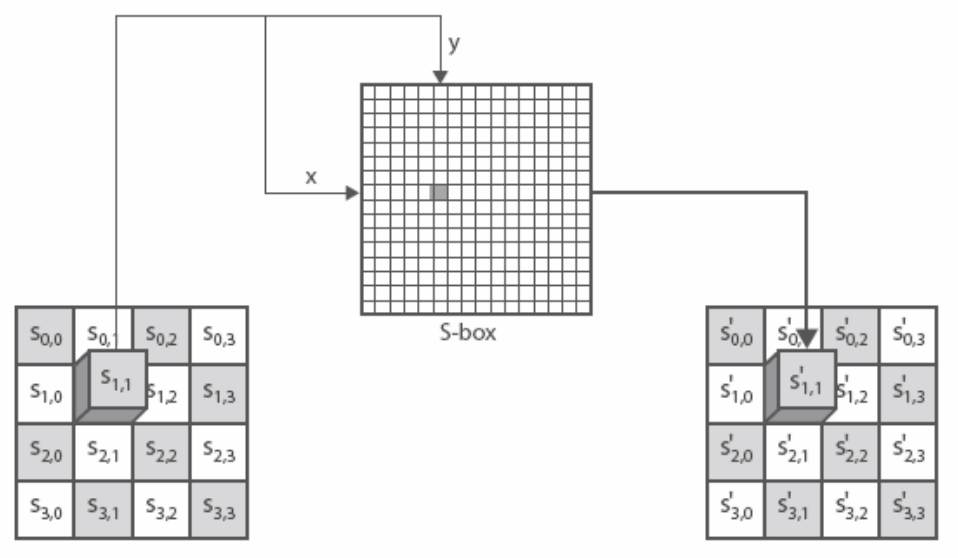
АНУ-ын Стандарт, Технологийн үндэсний хүрээлэн (VIST) 1997 онд өгөгдөл нууцаллын стандарт (DES)-ыг сайжруулах ажлыг эхлүүлж 2001 онд В.Рижмень, Д.Дэймен нарын блокон шифрлэлтийн схемийг дэвшилтэт нууцлалаын стандартаар зарласан.[3]

AES нь орлуулах сэлгэлт (substitution-permutation) гэж нэрлэгддэг зарчим дээр суурилдаг бөгөөд програм хангамж болон техник хангамжийн аль алин дээр нь хурдан ажилдаг. Орчин үед шифрлэлтийг хурдан хийх зорилгоор техник хангамж дээр зөвхөн энэ алгоритмд зориулсан хэсэг хүртэл байдаг билээ.

Үндсэн үйлдэл

1. **SubBytes:**

    - Байт болгоны байрлалыг солино

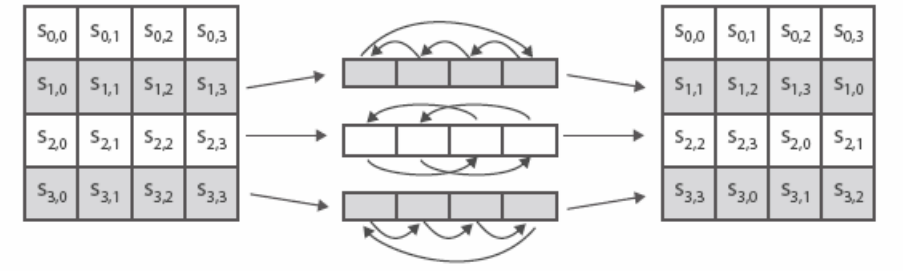


Зураг 1.1: SubBytes үйлдэл

- Тухайн мөр баганын мэдээлэл солигдоно

2. **ShiftRows:**

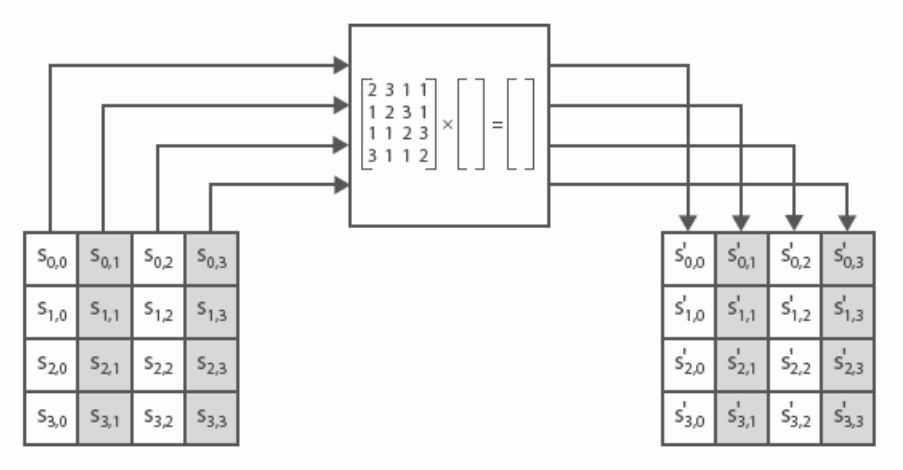
- 1-р мөрийг шилжүүлэхгүй
- 2–р мөрийн байтуудыг зүүн тийш 1 байт шилжүүлнэ
- 3–р мөрийн байтуудыг зүүн тийш 2 байт шилжүүлнэ
- 4–р мөрийн байтуудыг зүүн тийш 3 байт шилжүүлнэ
- Тайлах үйлдлийг хийхдээ баруун тийш шилжүүлэх үйлдлийг хийнэ



Зураг 1.2: ShiftRows үйлдэл

3. **MixColumns:**

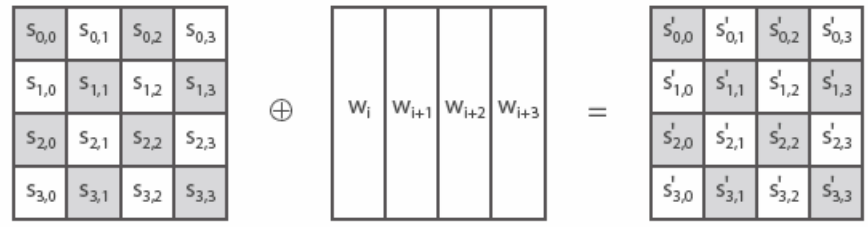
   - Багана бүр тус тусдаа холигдоно
   - Багана болгоны харгалзаа байтууд хоорондоо солигдоно



Зураг 1.3: MixColumns үйлдэл

4. **AddRoundKey:**

   - 128 бит XOR үйлдлийг циклийн түлхүүрт ашиглана
   - Тайлах үйлдэл хийх бол эсрэгээр гүйцэтгэнэ



Зураг 1.4: AddRoundKey үйлдэл

AES-ын нууцлалт, нууцын тайлалт

1. шифрлэх блок ба түлхүүрийн урт, мөчлөгийн тоог сонгох. Шифрлэх блок ба түлхүүрийн урт нь 128, 192, 256 байт байж болох бөгөөд мөчлөгийн тоо нь харгалзан 10, 12, 14 байна.

2. Шифрлэх текст, түлхүүрийн матриц *T, W, K*-г үүсгэнэ.

3. Эцсийн мөчлөгөөс бусад мөчлөгийн *T, W, K* матрицуудад **AES**-н үндсэн үйлдлүүдийг дэс дараалан хийнэ. Харин эцсийн мөчлөгт Mix Columns үйлдлийг хйихгүй.

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

2. СИСТЕМИЙН ЗОХИОМЖ

3. ТАЙЛАН БОЛОВСРУУЛАХ ЗӨВЛӨМЖ

Бакалаврын судалгааны тайлан бол шинжлэх ухаан, инженерчлэлийн бүтээлийг тайлагнах баримт бичиг юм. Мэдээлэл, компьютерийн ухааны тэнхимд хийгддэг ажлууд нь гол төлөв судалгаа, эрдэм шинжилгээний ажил эсвэл мэдээллийн технологийн инженерчлэлийн чиглэлийнх байдаг. Эрдэм шинжилгээний ажил бичиж байгаа бол судалгааг хийх сэдвийн судлагдсан байдал, боловсруулсан шийдэл, арга аргачлал, туршилт, үр дүнгийн боловсруулалт зэрэг агуулга зонхилно. Харин инженерчлэлийн чиглэлийн ажлын хувьд хэрэглэгчийн шаардлага, шинжилгээ, зохиомж, хэрэгжүүлэлт гэсэн агуулгыг голлож бичдэг.

3.1 Тайлангийн бүтэц ба төлөвлөлт

Тайланг бичиж эхлэхээс өмнө тайлангийн бүтцийг тодорхойлж төлөвлөх хэрэгтэй. Тайлан хэдэн бүлгээс тогтох, аль бүлэгт ажлын аль хэсгийг харуулах, хоорондоо хэрхэн уялдаатай байх, бүлгийн дэд гарчиг, дэд гарчиг доторх цогцолбороор юу өгүүлэх зэргийг урьдчилж боловсруулвал тайлан бичихэд илүү хялбар болдог. Энэ нь тайланг бичиж эхлэхээс өмнө ямар баримт бичиг болохыг бүхэлд нь харах боломжийг олгох бөгөөд тайлангийн цар хүрээг тодорхойлж буй хэрэг юм. Доорх жишээнд бүлгийг нэрлэж, бүлэг болон дэд бүлэг ямар агуулга байгааг хэрхэн төлөвлөж байгааг харуулав.

- Бүлэг 1. Үгийн утга зүйн цахим сан *[Үгийн утга зүй, цахим сангийн хэрэглээ, бүтэц, агуулга зэргийг товч бичих]*
  - 1.1 Нутгийн мэдлэгийн цөм *[НМЦ гэж юу болох, бүрэлдэхүүн хэсэг, ойлголтын цөм, хэлний цөмийн бүтэц, түүнд агуулагдах элементүүдийг тайлбарлах]*
  - 1.2 Холбоотой ажлууд *[Үгийн утга зүйн цахим сангийн талаарх бидний ажилтай нягт холбоотой ажлуудыг товч танилцуулж бичих, мөн бидний ажилтай холбоотой онцлог шинж, ялгарах талуудыг дурдах]*
  - 1.3 Цахим сан үүсгэх асуудлууд *[Дээрх холбоотой ажлуудад тулгарч байгаа нийтлэг*

асуудлууд, тэдгээр ажлуудад авч үзээгүй зүйлс зэргийг бичих]

- Бүлэг 2. Нутагшуулах аргачлал
- ...

3.1.1 Тайлангийн гарчиг

Тайлангийн гарчиг нь илүү явцуу, тухайн ажлыг бүхэлд нь илэрхийлж чадахуйц байхаар өгдөг. Эрдэм шинжилгээ судалгааны ажлын хувьд [Асуудал][Арга/Шийдэл][Ай/Сэдэв] гэсэн хэсгүүдийг агуулсан байвал илүү тодорхой болдог. Жишээ нь, *"Нутгийн Мэдлэгийн Цөмийг хамтын ажиллагаат олны хүчээр үүсгэх аргачлал ба хэрэгжүүлэлт"* сэдвийн хувьд *"үүсгэх аргачлал ба хэрэгжүүлэлт"* гэдэг нь асуудал, *"олны хүчээр"* гэдэг нь арга, шийдэл, *"Мэдлэгийн цөм"* гэдэг нь хэдий оноосон нэр боловч knowledge base, knowledge core гэх англи утгыг агуулж байгаа тул ай (domain) буюу сэдвийг тодорхой хэмжээнд илэрхийлж байна. Дээрх гурван хэсгийн дарааллын хувьд сэдвийн нэрийн найруулгаас хамаарах биз ээ.
Програм хангамж хөгжүүлэлтийн ажлын хувьд [програмын нэр][төрөл][гүйцэтгэсэн ажил] зэрэг агуулгыг тайлангийн гарчигтаа оруулвал илүү тодорхой болж бусад ажлуудаас ялгарч өгдөг. Програмын нэр нь ерийн эсвэл оноосон нэртэй байж болох юм. Англи нэрээ ч мөн адил удирдагч багштайгаа сайтар ярилцаж зөвлөсний үр дүнд өгөх нь зүйтэй. Дипломын ажлын нэр сургууль төгссөнийг гэрчлэх дипломын хавсралт дээр бичигддэг учир тун ач холбогдолтой хандах хэрэгтэй.

3.1.2 Бүлэг нэрлэх

Бүлгийг нэрлэхдээ аль болох тухайн ажилтай холбоотой нэр томъёо, үгийг ашиглах нь оновчтой байдаг. Энэ нь тухайн ажлыг бусад ажлаас ялгах, тайлангийн агуулгыг ерөнхийд нь ойлгох боломжийг уншигчдад олгодог. Сэдвийн судалгаа, шинжилгээ ба зохиомж, хэрэгжүүлэлт гэх мэтээр ерөнхий нэрлэснээс илүү ойлгомжтой болгодог тул аль болох бүлгийн нэрийг оновчтой, бүлэг доторх агуулгадаа тохирсон байдлаар өгөх нь зүйтэй байна. Мөн бүлгийн

нэр нь нэр үгээр байвал зохимжтой байдаг. Эсвэл үйлт нэрээр бичдэг.

3.2 Удирдтгал бичих

Удиртгал буюу оршил хэсэгт ажлыг хийх хэрэгцээ, шаардлага, үндэслэл, ажлын зорилго, зорилгод хүрэх зорилтуудыг бичдэг. Мөн тайлангийн бүтэц буюу аль бүлэгт юуны талаар өгүүлснийг бичнэ. Удиртгалыг хэсэг нэгээс хоёр нүүрт багтаан цогцолборууд хооронд оо нягт уялдаатай бичсэн байдаг.

3.3 Дүгнэлт бичих

Дүгнэлт нь бүхэлдээ юу хийж гүйцэтгэж ямар үр дүнд хүрсэн. Энд ажлын онцлог, давуу тал, шинэлэг байдал зэрэг бусад ажлаас ялгарах гол шинжүүдийг бичвэл илүү оновчтой байдаг. Түүнчлэн цаашид хэрэгжүүлэх ажил, нэмж гүйцэтгэх саналыг мөн оруулдаг. Ийм саналыг тухайн ажлыг гүйцэтгэсэн хүн илүү тодорхой хэлж чаддаг бөгөөд ажлын сул тал, гүйцээгүй зүйлсийг зөв тодорхойлж буйг илэрхийлэх юм.

4. БИЧВЭР БОЛОВСРУУЛАЛТ

Бүлгийн гарчгийн дор тухайн бүлэгт юу агуулж байгаа, юуны талаар өгүүлэхийг товч бичих нь баримт бичгийг уншигчдад илүү ойлгомжтой болгодог.

4.1 Шинэ мөр ба цогцолбор

Латекс бичих явцад олон хоосон зай, шинэ мөр авахад гаралтын файлд ганцхан хоосон зайгаар дүрсэлж харуулдгаараа бусад засварлагчаас ялгаатай юм.

Шинэ мөр буюу цогцолбор (paragraph) авахдаа хоёр удаа enter товч дарах буюу нэг хоосон мөр үлдээж бичнэ.

Эсвэл par командыг бичнэ.

Харин шинэ мөр авахдаа хоёр ширхэг ургашаа налуу зураас дарааллуулан бичнэ. Дэлгэрэнгүйг [2]-с унш.

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of ”de Finibus Bonorum et Malorum” (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, ”Lorem ipsum dolor sit amet..”, comes from a line in section 1.10.32.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from ”de Finibus Bonorum et Malorum” by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

4.2 Бичвэр зэрэгцүүлэх

4.2.1 Зүүн тийш зэрэгцүүлэх

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of ”de Finibus Bonorum et Malorum” (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, ”Lorem ipsum dolor sit amet..”, comes from a line in section 1.10.32. The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from ”de Finibus Bonorum et Malorum” by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

4.2.2 Баруун тийш зэрэгцүүлэх

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of ”de Finibus Bonorum et Malorum” (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, ”Lorem ipsum dolor sit amet..”, comes from a line in section 1.10.32. The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from ”de Finibus Bonorum et Malorum” by Cicero are

also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

4.3 Хэлбэржилт

Энэ бүлэгт бичвэрийг хэлбэржүүлэх (format) командуудын талаар дурьдана. Илүү дэлгэрэнгүйг [**?**]-с хар.

4.3.1 Тодруулах

`\textbf` командаар бичвэрийг **тодруулах буюу болд** болгоно.

4.3.2 Налуулах

`\textit` командаар бичвэрийг *бичмэл буюу италик* болгоно.

4.3.3 Доогуур зураас

`\underline` командаар бичвэрийг **тодруулах буюу болд** болгоно.

4.4 URL оруулах

`\url` команд дотор холбоосыг бичнэ. `http://milab.num.edu.mn`

4.5 Жагсаалт

4.5.1 Энгийн жагсаалт

`\begin{itemize}` командын дотор энгийн жагсаалтыг бичнэ [**?**].

- Жагсаалтын эхний элемент
- Жагсаалтын хоёрдугаар элемент
- Жагсаалтын гуравдугаар элемент

- Жагсаалтын дөрөвдүгээр элемент

4.5.2 Дугаартай жагсаалт

`\begin{enumerate}` командын дотор энгийн жагсаалтыг бичнэ [**?**].

1. Жагсаалтын эхний элемент
2. Жагсаалтын хоёрдугаар элемент
3. Жагсаалтын гуравдугаар элемент
4. Жагсаалтын дөрөвдүгээр элемент

5. ИШЛЭЛ, ЗҮҮЛТ

5.1 Ишлэл

Ашигласан материал эсвэл номзүйг бичвэр тодор ишлэхдээ cite командаар заалтыг нь оруулна. Үүний тулд энэ хуудасны хамгийн доор байгаа *Ашигласан материал, ном зүй* хэсэгт bibitem командыг нэмнэ.

Жишээ нь: bibitem{image1} Гарчиг, Зохиогчдын нэр, хэвлэсэн он, хэвлэсэн газар

Дээрх жишээнд image1 гэдэг нь ишлэх нэр. Доод талын мөрөнд нь байгаа дарааллын дагуу ашигласан материалыг бичнэ.

Ишлэхдээ cite командад ишлэх нэрийг дамжуулж өгнө. Жишээ нь cite{image1}.

5.2 Зүүлт

Зүүлтийг footnote командаар оруулна [1] .

[1] Энэ холбоосоос зүүлтийн талаар дэлгэрэнгүй унш: `https://www.sharelatex.com/learn/Footnotes`

6. ЗУРАГ

Зураг оруулахдаа includegraphics командыг ашиглана. Доорх жишээнд figure01.png гэдэг нь зургийн файлын нэр бөгөөд өргөтгөлийг заавал бичих шаардлагагүй. Зургийн файл нь main.tex файлтай нэг фолдерт байх шаардлагатайг анхаарна уу! Дэлгэрэнгүйг [**?**]-с үз.

6.1 Зургийн хэмжээ өөрчлөх

Хэмжээг томруулахдаа 0-1 хооронд утга ашиглана. Хэрэв 2 гэвэл 2 дахин томроно.

includegraphics[scale=0.5]{figure01}

Өндөр өргөнийг шууд зааж өгч болох бөгөөд дөрвөлжин хаалтан дотор доорх байдлаар бичнэ.

includegraphics[width=3cm, height=4cm]{figure01}

6.2 Зураг эргүүлэх

Зургийн эргүүлэхдээ angle параметрт эргүүлэх өнцгийн хэмжээг өгнө.

includegraphics[width=3cm, height=4cm, angle=45]{figure01}

6.3 Зургийн нэр

Зургын нэрийг begin{figure} хооронд includegraphics командтай хамт оруулна Зураг 6.1-ыг хар.

Энд зургийн нэрээс гадна label-ийг давхар бичиж өгөх шаардлагатай ба энэ нь зургийн дугаараар заалт хийхэд ашиглана. Жишээ нь: Зураг 6.2

Зураг 6.1: Зураг голлуулах

6.4 Зураг голлуулах

Зургийг голлуулахдаа includegraphics командын өмнө centering командыг бичээд reflectbox командыг includegraphics болон caption командуудад үйлчлэхээр оруулна.

Зураг 6.2: Зургийн нэрийг энд бичнэ

6.5 Зургийн чанар

LaTex-т зургийг вектор форматаар (svg, eps) оруулбал хэвлэх болон томруулж харахад зургийн чанар алдагдахгүй. Тиймээс аль болох вектор зураг оруулж өгвөл зүгээр.

7. ХҮСНЭГТ ОРУУЛАХ

Хүснэгт оруулахад tabular командыг ашигладаг [**?**].

Table 7.1: Хүснэгтийн нэр. Хүснэгтийн нэр хүснэгтийн дээд талд байрлана.

Багана1	**Багана2**	**Багана3**	**Багана4**	**Багана5**
өгөгдөл	*өгөгдөл1*			

7.1 Хүснэгт зурах хэрэгсэл

Цэвэр LaTex кодоор Хүснэгт үүсгэхэд харьцангуй төвөгтэй байдаг учир хялбар хэрэгслийг ашиглаж болно.

Тухайлбал `https://www.tablesgenerator.com/` холбоосруу орж хүснэгтийг визуал орчинд зураад үүсгэж өгсөн LaTex кодыг энд хуулж оруулна.

8. КОД БА АЛГОРИТМ ОРУУЛАХ

Код оруулахдаа begin{lstlisting} ... end{lstlisting} командын хооронд бичнэ.

```c
#include <stdio.h>
#define N 10
/* Block
 * comment */
int main()
{
    int i;
    // Line comment.
    puts("Hello␣world!");
    for (i = 0; i < N; i++)
    {
        puts("LaTeX␣is␣also␣great␣for␣␣programmers!");
    }
    return 0;
}
```

Код 8.1: C хэлний кодын жишээ

Мөн кодын эх файлыг шууд оруулж ирж болох бөгөөд доорх командыг бичнэ.

```c
    puts("Hello␣world!");

    for (i = 0; i < N; i++)
    {
        puts("LaTeX␣is␣also␣great␣for␣programmers!");
    }
```

Код 8.2: Кодын файлаас хэсэгчилж оруулах

Мэдээллийн технологи, програм хангамжийн ажлын тайланд алгоритмыг хийсвэр кодын бичиглэлээр оруулах шаардлага гардаг. Дараах жишээгээр (Алгоритм 1) хийсвэр кодоор хэрхэн бичиж болохыг харуулав. Мөн бичвэр дотроо алгоритмд ашиглаж байгаа $parentId$ хувьсагчийг дурдаж бичиж болдог.

Алгоритм 1 Даалгавар үүсгэх алгоритм

```
1:  function traverse(parentId)                    ▷ parentId–эцэг ойлголтын дугаар
2:      children ← getChildConceptIds(parentId)
3:      childCount ← children.count
4:      if childCount == 0 then
5:          return
6:      end if
7:      for i = 0 to childCount do
8:          generateTask(children_i)               ▷ Орчуулгын даалгавар үүсгэх
9:      end for
10:     for i = 0 to childCount do
11:         traverse(children_i)
12:     end for
13: end function
```

Дүгнэлт

сольсонДүгнэлтийг энд бич

Bibliography

[1] Daemen, J., & Rijmen, V. (2002). ”The Design of Rijndael: AES - The Advanced Encryption Standard.” Springer. p.1-2.

[2] Paragraphs and new lines, Share LaTex, `https://www.sharelatex.com/learn/Paragraphs_and_new_lines`

[3] Д. Гармаа (2022). ”Криптографын үндэс.” Улаанбаатар хот.

[4] Bellare, Mihir; Rogaway, Phillip (11 May 2005), Introduction to Modern Cryptography (Lecture notes), archived (PDF) from the original on 2023-10-30, chapter 3.

А. ШИНЖИЛГЭЭ ЗОХИОМЖ

Хавсралтын агуулга

В. КОДЫН ХЭРЭГЖҮҮЛЭЛТ

```
import numpy as np

def incmatrix(genl1,genl2):
    m = len(genl1)
    n = len(genl2)
    M = None #to become the incidence matrix
    VT = np.zeros((n*m,1), int)  #dummy variable

    #compute the bitwise xor matrix
    M1 = bitxormatrix(genl1)
    M2 = np.triu(bitxormatrix(genl2),1)

    for i in range(m-1):
        for j in range(i+1, m):
            [r,c] = np.where(M2 == M1[i,j])
            for k in range(len(r)):
                VT[(i)*n + r[k]] = 1;
                VT[(i)*n + c[k]] = 1;
                VT[(j)*n + r[k]] = 1;
                VT[(j)*n + c[k]] = 1;

                if M is None:
                    M = np.copy(VT)
                else:
                    M = np.concatenate((M, VT), 1)

                VT = np.zeros((n*m,1), int)

    return M
```