



Мэдээллийн сүлжээ,  
аюулгүй байдлын салбар



Кибер аюулгүй байдал  
мэргэжил

# Прокси дахин шифрлэх схемд суурилсан туршилтын систем хөгжүүлэх нь

Гүйцэтгэсэн: А.Мягмарцэрэн (B190970106)

Удирдагч: В.Нямсүрэн (Доктор Ph.D)

Зөвлөх багш: В.Нямсүрэн (Доктор Ph.D)

Ц.Манлайбаатар (Магистр)

MUST, SICT

Мэдээлэл, Холбооны Технологийн Сургууль



## Агуулга

1. Зорилго

2. Судалгааны хэсэг

3. Хөгжүүлэлт системийн ажиллагаа

4. Туршилт, Хэрэгжүүлэлт

5. Дүгнэлт



MUST, SICT





# Зорилго

Прокси дахин шифрлэх схемийг ашиглан шифрлэсэн файл хуваалцах туршилтын системийн систем хөгжүүлэх.



3



MUST, SICT

Мэдээлэл, Холбооны Технологийн Сургууль



## Файл хуваалцахад учрах аюулгүйн байдлын эрсдэл



4



MUST, SICT

Мэдээлэл, Холбооны Технологийн Сургууль



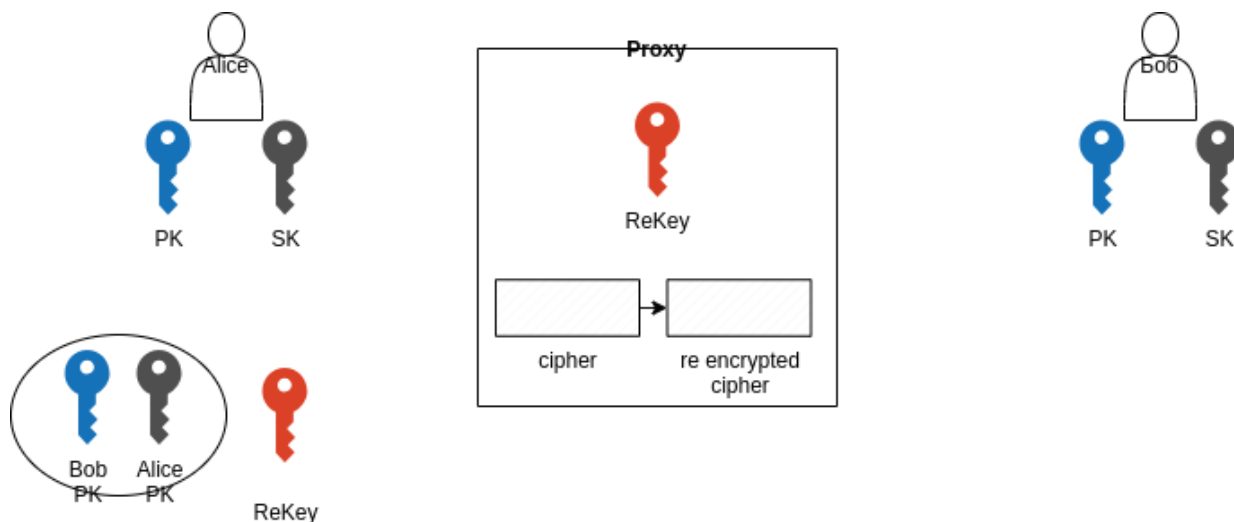
# Шифрлэх схемүүд

- Танилтад суурилсан шифрлэлт
- Шинж чанарт суурилсан шифрлэлт
- Гомоморф шифрлэлт
- Прокси дахин шифрлэлт



## Прокси дахин шифрлэх схем

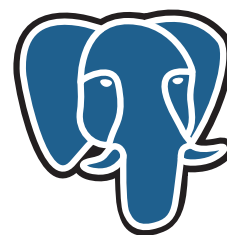
1. Алис өөрийн PK -ээр шифрлэнэ.
2. Боб-ын PK болон өөрийн SK-г ашиглан ReKey үүсгэнэ.
3. Прокси Алис-ын шифрийг ReKey-р дахин шифрлэнэ
4. Боб шифрийг өөрийн SK-г тайлна.





# Ашигласан технологи

- Flask
- Tkinter
- PyUmbrel
- PostgreSQL



Flask



MUST, SICT

7



Мэдээлэл, Холбооны Технологийн Сургууль



# Ерөнхий загвар



## Desktop program

Файл шифрлэх

ReKey үүсгэх

Шифрийг тайлах

Хувийн түлхүүр хадгалах



## API server

Түлхүүр үүсгэх

Дахин шифрлэх

Өгөгдлийн сан руу хадгалах

Шифрлэсэн файл хадгалах



## Database



MUST, SICT

8

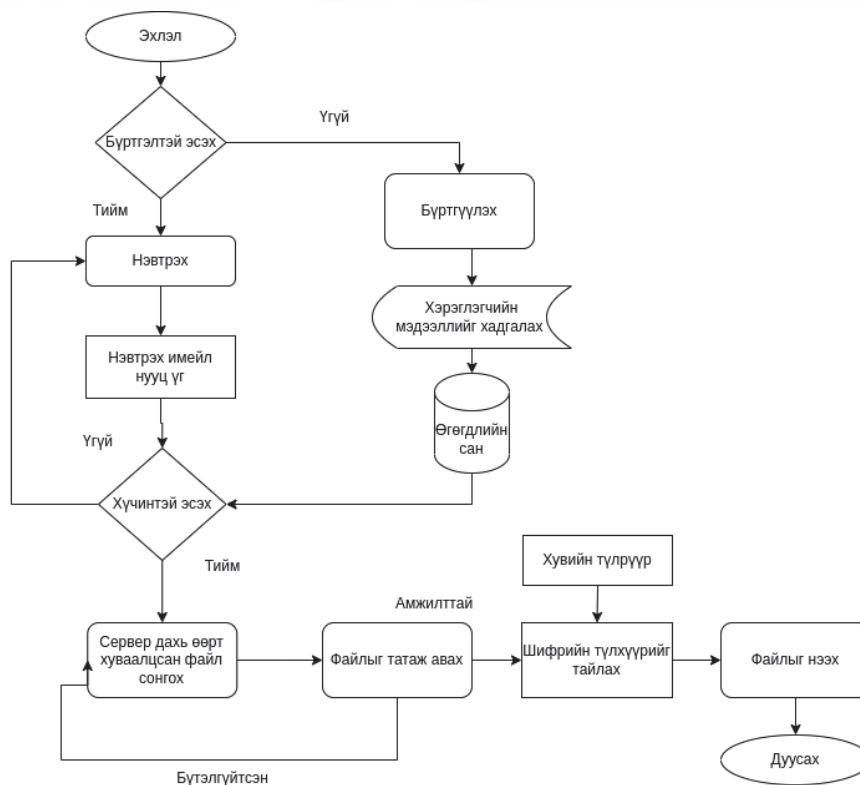


Мэдээлэл, Холбооны Технологийн Сургууль





# Үйл ажиллагааны диаграмм



11



## ДҮГНЭЛТ

- Прокси дахин шифрлэхийн схемийг талаар ойлголт авч түүнийгээ практик байдлаар өөрийн файл хуваалцах туршилтын системийг хөгжүүллээ. Бүрэн гүйцэд сайн систем болоогүй ч үргэлжлүүлэн хөгжүүлэх боломжтой.

12



**Анхаарал хандуулсанд  
баярлалаа.**

