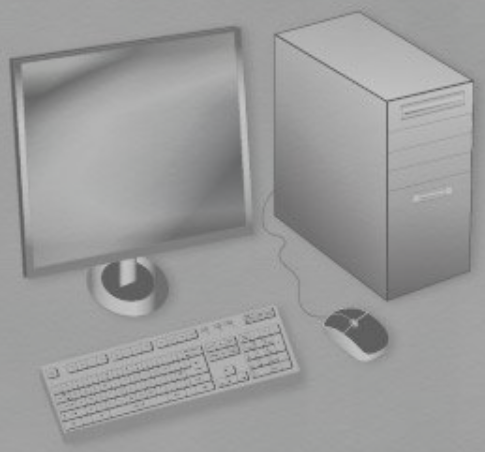
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
МЕХАНИКА-МАТЕМАТИКА ФАКУЛЬТЕТІ
АҚПАРАТТЫҚ ЖҮЙЕЛЕР КАФЕДРАСЫ

Дипломалды тәжірибе есебі

Тақырыбы: “Блоктік шифр үшін кеңейтілген дифференциалдық криптоталдау жасау”

Орындаған: Жарқымбек Н.Б.



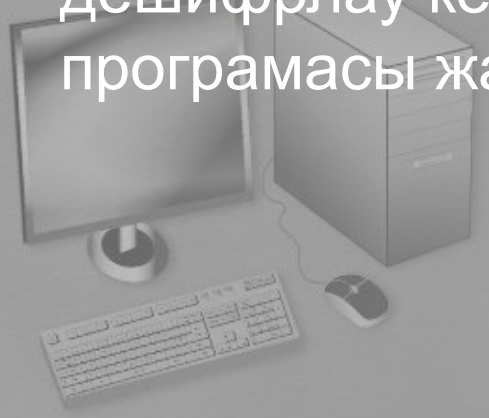
Алматы – 2016

Дипломдық жұмыс мақсаты:

- Блоктік шифрлеу алгоритмі үшін дифференциалдық криптоталдау жүргізу.

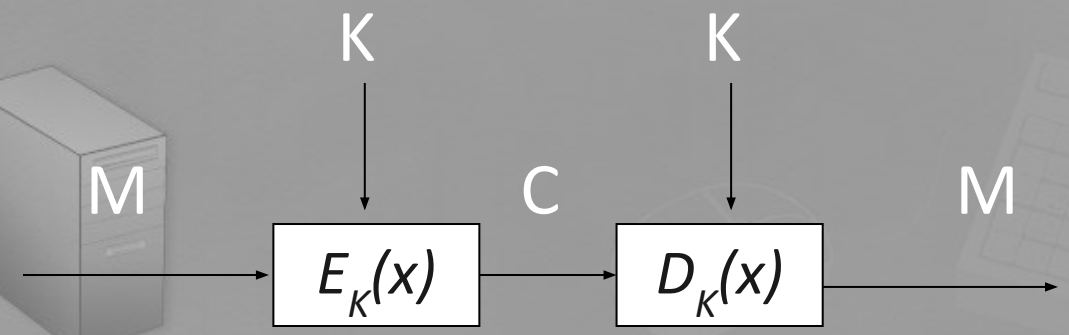
Зерттеудің практикалық маңыздылығы:

- S-DES шифрлау алгоритміне негізделген берілген мәнді шифрлау мен дешифрлау программасы жасалды.
- Дифференциалдық криптоанализ әдісіне негізделген S-DES шифрлау алгоритмінің мәтінді шифрлау мен дешифрлау кезінде қолданылатын кілтті іздеу програмасы жасалды.



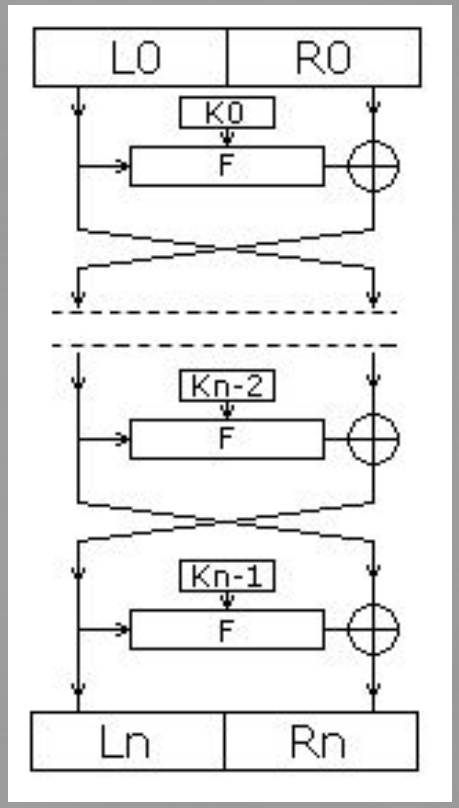
Кіріспе

- Компьютерлік жүйелерде ақпаратты қорғау бүгін ғылымның ерекше саласы болып табылады.
- Криптография – бұл мәліметтер мен деректердің әлдеқайда қауіпсіз сақталуы мен таратылуы үшін осы ақпараттарды шифрлейтін стандарттар мен хаттамалар жиынтығы.



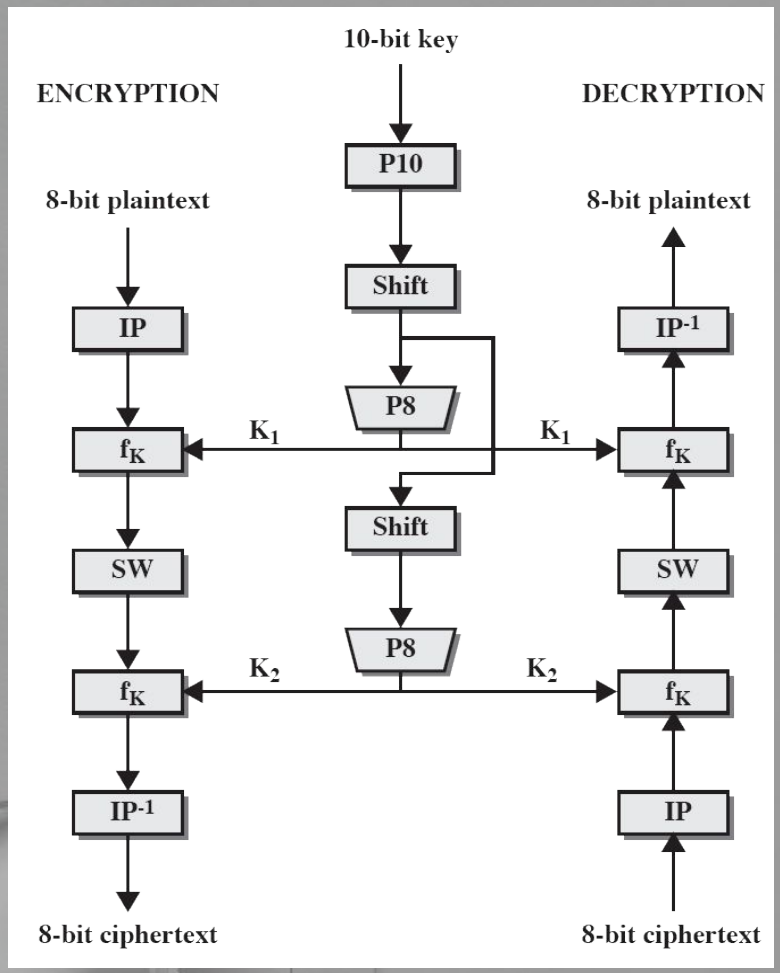
1-сурет. Криптографияның негізгі моделі

Блоктық шифрлер
Фейстель желісі



2-сурет. Фейстель тораптары (желілері)

S-DES



3-сурет. FEAL-6 алгоритмінің сызбасы

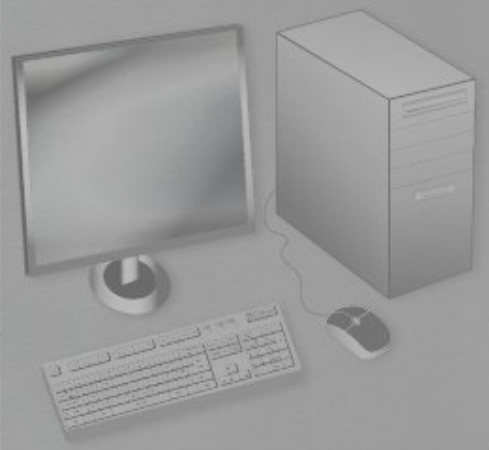
- **Қарапайым DES** – практикалық мәніне қарағанда, оқытушылық мәні жоғарырақ болатын шифрлеу алгоритмі. Қасиеттері мен құрылымы бойынша ол DES-ке ұқсайды, алайдаоның параметрлерінің саны салыстырмалы түрде азырақ болады.

S-DES-тың шифрлау және дешифрлау программасының нәтижесі.

```
================================S-DES================================

 Aldyn ala berilip koigan kiltti koldanasyz ba (y/n) ?y
 Ashyk matindi korsetiniz (8 BITS) ?101010101
 Ashyk matin = 10101010 [170 Ondyk sanau zhuesinde]
 Kilt = 0000100000 [ 32 Ondyk sanau zhuesinde]

 ========================== Shifrlau ============================
 Shifrmatin = 01111010 [122 Ondyk sanau zhuesinde]

 ========================== Deshifrlau ==========================
 Deshifrlangan shifrmatin = 10101010 [170 Ondyk sanau zhuesinde]

Shifrlauga zhane deshifrlauga ketken uakyt - 0 secund
```

Криптоталдау
Дифференциалды криптоталдау

- Криптоталдау – криптожүйенің сенімділігін бағалау және алгоритмдерге қол сұғу.
- Дифференциалды криптоталдаудың соңғы тапсырмасы - алгоритмнің негізгі құрылымын S-box негізгі құрылымында пайдалана отырып, раундтың кілтін тауып алу.
- Дифференциалды криптоталдауды қолдданып S-DES-ке жасалған шабуылдың программасы жазылды.



НАЗАРЛАРЫҢЫЗҒА РАХМЕТ!