ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТІРЛІГІ
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
МЕХАНИКО-МАТЕМАТИКА ФАКУЛЬТЕТІ
АҚПАРАТТЫҚ ЖҮЙЕЛЕР КАФЕДРАСЫ

ДИПЛОМДЫҚ ЖҰМЫС

ТАҚЫРЫБЫ:

Жылжымалы шабуылын блоктік шифрлау алгоритмдеріне қатысты қолдану және талдау

Орындаған: Турғамбаева Ж.Б.
Топ: АЖ-13-4 курс
Ғылыми жетекшісі: Мусиралиева Ш.Ж.

МАҚСАТЫ

1)Жылжымалы шабуылын блоктік шифрлау алгоритмдеріне қатысты қолданып, талдау жасау;

2)Слайд шабуыл әдісі арқылы шабуыл жасап, слайд жұптарын табу;

3)Слайд шабуылдарын қолданып криптографиялық талдау жасау.

Ғылыми жаңалығы

- блоктық шифрлау алгоритмдерінің құрамына кіретін криптографиялық әдістер қарастырылды;
- ықтималдық теориясы, ақпаратты кодтау теориясы мен криптоталдаудың математикалық негіздеріндегі әдістер мен жүйелерді құру әдістеріне негізделген слайд жұптарын табатын программаны жүзеге асырылды;

Слайд шабуылы

Слайд шабуыл – бұл криптографиялық шабуыл. Оның жетістігінің бірі - ең мықты деп саналатын блоктік шифрды бұза алатындығында болды. Дегенмен, бұның басым идеясы, тіпті, әлсіз шифрлардың раундтар санын арттыру арқылы өте мықты бола алуында және ол әртүрлі шабуылдардан қорғау үшін пайдаланылады.

ПРОГРАММА БЛОК СХЕМАСЫ

Дипломдық жұмысымда слайд шабуылдарын пайдаланып, криптографиялық талдау жасау барысында мәтіндерді Раунды функция ашық Sbox және жабық рекурсивті екілік раунд түрінде алдым.

Раунды функция. Ашық Sbox мәтінін жариялау

4 қадам жылжи отырып, К0 және К1 кілттерін табу арқылы слайд жұптарын анықтаймыз.

Слайд жұптардың табылуы

Нәтижесінде слайд жұптарының табылған пайызы анықталады.