

Лабораториялық жұмыс нұсқаулығы
"Дешифрлеу тренажері" қолданбасымен жұмыс істеу

1. Жұмыс тақырыбы

Моноалфавитті алмастыру шифрын криптоанализдеу - жиілік талдау әдісі арқылы дешифрлеу

2. Жұмыс мақсаты

- Алмастыру шифрының жұмыс принципін үйрену
- Жиілік талдау әдісін практикалық қолдану
- Криптоанализдің негізгі кезеңдерін меңгеру

3. Қажетті құрал-жабдықтар

- Компьютер
- Интернет браузері (Chrome, Firefox, Edge)
- "Дешифрлеу тренажері" қолданбасы

4. Жұмыс барысы

4.1. Алғышарттарды дайындау

1. Браузерді ашыңыз
2. Тренажер файлын (index.html) ашыңыз
3. Интерфейс тілін қазақшаға орнатыңыз (ҚАЗ түймесі)

4.2. Тәжірибелік тапсырмалар

Тапсырма 1: Мәтінді жүктеу және шифрлау

1. "Ашық мәтінді жүктеу" түймесін басыңыз
2. Қазақша мәтінді таңдаңыз (қалыпты мәтін, эссе, мақала)
3. "Шифрлау" түймесін басыңыз
4. Шифрланған мәтінді бақылаңыз

Тапсырма 2: Жиілік талдау

1. "Талдау" түймесін басыңыз
2. Бір әріптердің жиіліктерін салыстырыңыз
3. Мәтін тілін қазақша деп орнатыңыз
4. Эталондық жиіліктермен шифртекст жиіліктерін салыстырыңыз

Тапсырма 3: Алмастырулар жасау

1. Шифртексттегі ең жиі кездесетін әріпті таңдаңыз
2. Эталондық жиіліктердегі сәйкес әріпті анықтаңыз
3. Алмастыруды енгізіп, "Алмастыру" түймесін басыңыз
4. Процесті қайталаңыз (5-7 алмастыру)

Тапсырма 4: Мәтінді толық дешифрлау

1. Барлық әріптерді дұрыс тапқанша алмастыруларды жасаңыз
2. "Тексеру" түймесін басыңыз
3. Нәтижелерді талдаңыз

Тапсырма 5: Түрлі параметрлермен жұмыс

1. Мәтін тілін өзгертіңіз (орыс, ағылшын)
2. Талдау параметрлерін өзгертіңіз
3. Шифрлау параметрлерін өзгертіңіз

5. Есептер мен талдау

5.1. Бақылау сұрақтары:

1. Қандай әріптер ең жиі кездеседі?

2. Эталондық жиіліктер қалай анықталады?
3. Алғашқы алмастырулар қандай әрекеттерге негізделген?
4. Қандай қиындықтар туындады?

5.2. Есептер:

1. Өзіңіздің шифрлау кестеңізді құрастырыңыз
2. Берілген шифртекстті дешифрлаңыз
3. Өз мәтініңізді шифрлап, сыныптастарыңызға дешифрлеуге беріңіз

6. Нәтижелерді тіркеу

Кесте 1 - Жиілік талдау нәтижелері

№	Шифр символы	Шифртексттегі жиілігі (%)	Эталондық символ	Эталондық жиілік (%)	Алмастыру
1					
2					
...					

Кесте 2 - Дешифрлау статистикасы

Параметр	Мән
Барлық символдар	
Шифрланған символдар	
Дешифрланған символдар	
Дәлдік (%)	
Уақыт (минут)	

7. Қорытынды жасау

Төмендегі тармақтар бойынша қорытынды жазыңыз:

1. Моноалфавитті алмастыру шифрының артықшылықтары мен кемшіліктері
2. Жиілік талдау әдісінің тиімділігі
3. Қазақ тіліндегі мәтіндерді талдаудың ерекшеліктері
4. Қиындықтар және оларды шешу жолдары
5. Шифрдың қауіпсіздігін арттыру әдістері

8. Қауіпсіздік ережелері

1. Файлдарды сақтағанда вирустық сканерлеуді өткізіңіз
2. Жеке деректерді шифрламаңыз
3. Жүйені зақымдайтын әрекеттерден аулақ болыңыз

9. Өздік жұмыс тапсырмалары

1. Өртүрлі ұзындықтағы мәтіндермен жұмыс жасаңыз
2. Өртүрлі тілдегі мәтіндерді салыстырыңыз
3. Өз шифрлау алгоритміңізді құрастырыңыз

10. Әдебиеттер тізімі

1. Криптография негіздері
2. Ақпарат қауіпсіздігі
3. Алгоритмдер және деректер құрылымдары

Ескерту: Бұл нұсқаулық студенттерге "Дешифрлеу тренажері" қолданбасымен жұмыс істеуге арналған. Әрбір тапсырманы орындағаннан кейін нәтижелерді тіркеп, талдау жасау қажет.