№6 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Ақпаратты қорғау әдістері. Цезарь шифрі

САБАҚ МАҚСАТЫ: Excel ортасында Цезарь шифрін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Ақпаратты қорғау әдістері
- Цезарь шифрі

НЕГІЗГІ МАҒЛҰМАТТАР:

Цезарь шифрі қарапайым ауыстыру әдісіне жатады. Рим императоры Гай Юлий Цезарь осы әдісті пайдаланғандықтан әдіс осылай аталады. Бастапқы мәтінді шифрлеу үшін мәтіннің әр әріпі алфавиттың басқа арпіне келесі ережемен аустырылады.

Мысалы: айталық, А - қолданылатын алфавит:

$A=\{a1, a_2,\ldots,a_m,\ldots,a_N\}$, мұнда $a_1,a_2,\ldots,a_m,\ldots,a_N$ - алфавит символдары; N алфавит ұзындығы.

Айталық, k – шифрлеу кезіндегі алфавит символдарының ығыстыру позициясының саны, $0<k<N$. Шифрлеу кезінде алфавиттың кодталатын мәтіннің әр нөмері m символы осы алфавиттың $m+k$ символына ауыстырылады. Егер $m+k>N$, онда А алфавиттегі символ нөмері $m+k-N$ өрнек арқылы анықталады.

ЖҰМЫСТЫ ОРЫНДАУҒА ӘДІСТЕМЕЛІК НҰСҚАУЛАР:

1. Excelді қосыңыз. Жаңа құжатты құрып, екінші бетіне өтіңіз. А1 бастап А40 дейін 1"а" суреттегідей алфавитті теріңіз. Алфавит диапазонын ерекшелеп оған «ЗЕРТ1» атты меншіктеңіз.
2. Құжаттың бірінші бетіне В1 ұяшығына шифрленетін мәтінді теріңіз, мысалы: **Гай Юлий Цезарь:"Пришел, увидел, победил!"** Мәтінді теру барысында тек қана алфатитте бар символдарды пайдалану қажет.
3. В3 ұяшығына В1 ұяшығындағы мәлеметтерді көшіріп, символдарды үлкен әріптерге аустырыңыз.
4. D3 ұяшығына =ДЛСТР(В3) формуласын енгізіңіз, ДЛСТР функциясы шифрленетін символдар санын есептейді.
5. D4 ұяшығына k мәнін енгізіңіз, *мысалы*, 5-ті.
6. А бағанасының, А6 ұяшығынан бастап 1 ден Nге дейін нөмірлеңіз, мұнда N – мәтіндегі символдар саны (пробелді қосқанда).

N мәні D3 ұяшығында есептелген.

7. В6 ұяшығына =ПСТР(В$3;А6;1) формуласын енгізіңіз, бұл формула шифрленетін мәтінді жеке символдарға бөледі. Бұл формуланы В7- В47 ұяшықтарға көшіріңіз.
8. С6 ұяшығына =ПОИСКПОЗ(В6; ЗЕРТ1;0)" формуласын енгізіңіз. ПОИСКПОЗ функциясы ЗЕРТ1 массивтегі символдың индексін 2 – беттен іздейді. С6 ұяшығының мәнін С7-С47 ұяшықтарға көшіріңіз.
9. ЗЕРТ1 алфавитінен символ нөмерін алып кодталатын мәтіннің символдарын ығыстырыңыз. Ол үшін D6 ұяшығына келесі формуланы енгізіңіз:

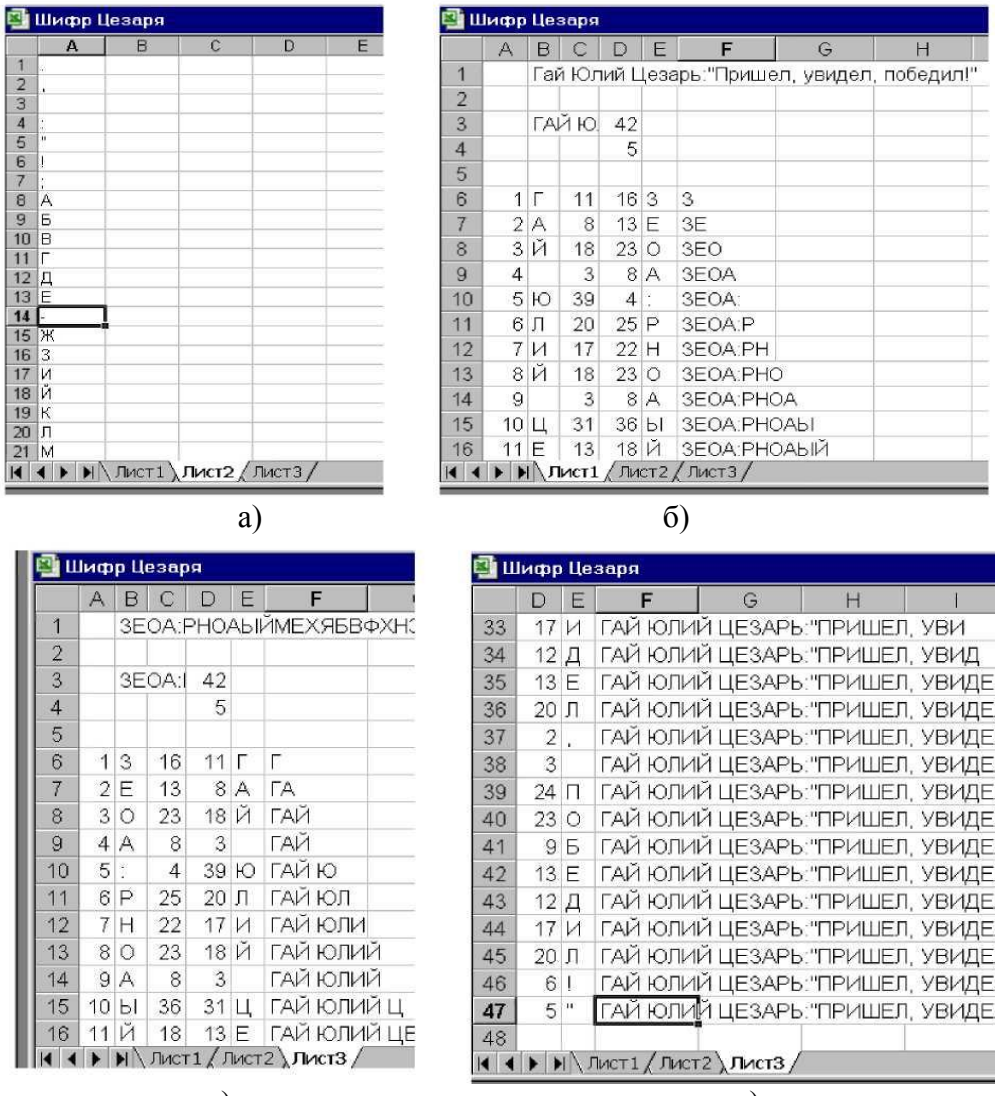
=ЕСЛИ(ПОИСКПОЗ(В6; ЗЕРТ1;0)+$D$4>38;ПОИСКПОЗ(В6; ЗЕРТ1;0)+$D$4-40;ПОИСКПОЗ(В6; ЗЕРТ1;0)+$D$4) (1)

Бұл формулаға түсініктеме беріңіз. D6 ұшығының мазмұнын D7-D47 ұяшықтар диапазонына көшіріңіз.

10. ЗЕРТ1 алфавитінен жаңа нөмерлеріне сәйкес символдарды таңдап алу. Е6 ұяшығына =ИНДЕКС(ЗЕРТ1;D6) формуласын еңгізіңіз. Е6 ұшығының мазмұнын Е7-Е47 ұяшықтар диапазонына көшіріңіз.
11. Кодталған мәтінді алу үшін F6 ұяшығына =Е6 формуланы, ал F7 ұяшығына =F6&E7 формуланы енгізіңіз. F7 ұшығының мазмұнын F8-F47 ұяшықтар диапазонына көшіріңіз. F47 ұшығынан шифрленген мәтінді оқи аласыз.
12. Шифрлеуді тексеру үшін шифирленген мәтінді (F47 ұшығында) кері шифрлеу керек

және оларды салыстыру қажет. 3 – бетте зертханалық жұмыстың 2-11пунктерін орындау керек. Мұнда келесіні ескеру қажет:
2 – пункті орындағанда шифрленген мәтінді теру қажет; ал 9 – пункті орындағанда D6 ұяшығына мына формуланы енгізіңіз:

=ЕСЛИ(ПОИСКПОЗ(B6; ЗЕРТ1;0)-$D$4<0;ПОИСКПОЗ(B6; ЗЕРТ1;0)-$D$4+40; ПОИСКПОЗ (B6; ЗЕРТ1;0)-$D$4). (2)



а) б)

в) г)

сурет.1. – № 6 зертханалық жұмыстың Excelдегі құжаттардың фрагменттері:
а) Цезарь шифрінің символдар алфавиті; б) шифрлеу құжаттың бастапқы бөлігі; в) және г) кері шифрленген құжаттың бастапқы және соңғы бөлігі

Тапсырмалар:

1. Осы мысалды пайдалана отырып қазақ алфавитін құрастырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді шифрлеу және кері шифрлеуді орындаңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.