№ 10 Лекция тақырыбы: Уитстонның «қосарланған квадрат» шифры және қосарланған орналастыру әдісі

Лекцияның оқыту нәтижиелері: Уитстон шифрының шығу тарихы және қолданылуы, «Қосарланған квадрат» шифрының құрылысы және шифрлау ережелері мен Қосарланған орналастыру (Double Transposition) әдісін біледі.

Лекция мазмұны:

1. Уитстонның «қосарланған квадрат» шифры

Уитстонның «қосарланған квадрат» шифры (көбіне Плейфер шифры деп аталады) – полиалфавиттік шифрлаудың классикалық әдісі. Бұл шифр 1854 жылы ағылшын физигі Чарльз Уитстонмен ұсынылған, алайда оны қолданысқа енгізуде лорд Плейфер үлкен үлес қосқан. Сондықтан криптографияда бұл әдіс көбіне «Плейфер шифры» деп аталады.

Чарльз Уитстон (1802-1875) - XIX ғасырдың ағылшын ғалымы, физик және өнертапқышы. Ол телеграфты дамытуға қосқан үлесімен және электрлік өлшеулерде қолданылатын "Уитстон көпірі" деп аталатын құралды ойлап табуымен әлемге танымал. Алайда оның криптография саласына қосқан үлесі де кем емес. Уитстон 1854 жылы "қосарланған квадрат" шифрын ұсынды. Бұл әдіс оның досы Лайонел Плейфермен бірлескен зерттеулерінің нәтижесі ретінде пайда болды. Кейде бұл шифр "Плейфер шифры" деп аталып шатастырылады, бірақ Уитстонның әдісі екі матрицаны қолдануымен және күрделілігімен ерекшеленеді.

XIX ғасыр – криптографияның қарқынды дамыған кезеңі. Бұл кезде Еуропадағы өнеркәсіптік революция, телеграфтың пайда болуы және халықаралық қатынастардың күрделенуі құпия хабарламаларды қорғаудың жаңа әдістерін талап етті. Сол кездегі қарапайым моноалфавиттік шифрлар, мысалы, Цезарь шифры немесе қарапайым ауыстыру әдістері, жиілік талдауы арқылы оңай бұзылатын еді. Уитстон осы кемшіліктерді ескеріп, полиграммалық шифрлаудың алғашқы түрлерінің бірін ұсынды. "Қосарланған квадрат" шифры әскери және дипломатиялық мақсаттарда қолданылды, әсіресе Британия империясының құпия байланыстарында. Оның пайда болуы криптографияның жаңа кезеңін ашты және кейінгі күрделі әдістердің дамуына негіз болды.

Шифрдың негізінде 5×5 өлшемді кесте қолданылады. Кесте кілт сөз арқылы толтырылады.

Кілт сөздегі әріптер қайталанбай жазылады, ал қалған тор бос орындары әліпби бойынша толтырылады.

Плейфер кестесін құру ережесі:

1) Кілт сөз жазылады (мысалы: ҚАУІПСІЗДІК)
2) Қайталанатын әріптер алынып тасталады
3) Қалған бос ұяшықтар әліпби ретімен толтырылады

Шифрлау ережелері:

Мәтін екі әріптен тұратын жұптарға бөлінеді. Егер жұптағы әріптер бірдей болса, арасына «Х» қойылады. Егер жұп бір жолда болса – әрқайсысы оңға 1 орын жылжиды. Егер бір бағанда болса – төменге жылжиды. Егер төртбұрыш түзілсе - сол төртбұрыштың қарсы бұрышындағы таңба алынады.

2. Қосарланған орналастыру (Double Transposition)

Қосарланған орналастыру – классикалық криптографиядағы ең тұрақты шифрлардың бірі. Бұл әдіс мәтінді екі рет кестелік ауыстыру арқылы шифрлайды.

Алгоритм:

1) Мәтін кілттік сөз бойынша кестеге жазылады
2) Бірінші рет жолдарды/бағандарды кілт ретімен қайта орналастырады
3) Екінші рет басқа кілтпен қайта орналастыру орындалады

Артықшылығы: қарапайым, бірақ анализге төзімді

Кемшілігі: шифрлау жылдамдығы төмен

"Қосарланған квадрат" шифры екі 5x5 матрицаға негізделген. Бұл матрицалар кілттік сөздер арқылы әріптермен толтырылады, ал "қосарланған орналастыру" термині осы екі матрицаның қолданылуын білдіреді. Ағылшын алфавитінде 26 әріп болғанымен, шифрда 25 әріп қана қолданылады – әдетте "J" әрпі "I" әрпімен алмастырылады. Қазақ тілінде қолданғанда әріптер санына байланысты бейімдеу қажет болуы мүмкін, бірақ классикалық нұсқа негізінде түсіндіріледі.

Қосарланған орналастырудың мәні – шифрлау кезінде екі матрицаның қиылысуы арқылы жаңа әріптер таңдалады. Бұл процесс шифрды моноалфавиттік әдістерден күрделі етеді, себебі әріптердің шифрланған нұсқасы контекстке байланысты өзгереді.

3. Шифрдың жұмыс механизмі

Шифрлау процесі бірнеше қадамдардан тұрады:

Мәтінді дайындау: Ашық мәтін екі әріптен тұратын топтарға (биграммалар) бөлінеді. Егер мәтіннің ұзындығы тақ болса немесе бір топта қайталанатын әріптер болса, қосымша әріп (мысалы, "Х") қосылады. Мысалы, "САЛАМАТ" сөзі "СА ЛА МА ТХ" деп бөлінеді.

4. Қосарланған орналастырудың ерекшеліктері және артықшылықтары.

"Қосарланған орналастыру" – шифрдың ең басты ерекшелігі. Бұл принцип екі матрицаның қиылысуына негізделген, бұл оны моноалфавиттік шифрлардан (мысалы, Цезарь шифры) айтарлықтай ажыратады. Моноалфавиттік шифрларда бір әріп әрқашан бір ғана шифрланған әріпке сәйкес келсе, "қосарланған квадратта" бір әріптің шифрланған нұсқасы оның жұбындағы екінші әріпке байланысты өзгереді. Мысалы, "CA" және "CE" биграммаларындағы "C" әрпі әртүрлі шифрланған әріптерге айналады.

Екі кілттік сөзді пайдалану шифрдың қауіпсіздігін одан әрі арттырады. Криптоаналитик шифрды бұзу үшін екі матрицаны және олардың кілттерін анықтауы қажет, бұл қолмен талдауды өте қиындатады. Сонымен қатар, полиграммалық шифрлау әдісі ретінде "қосарланған квадрат" бір мезетте екі әріпті шифрлайды, бұл оны сол кездегі басқа әдістерден тиімді етті. Бұл ерекшеліктер Уитстонның шифрын өз уақытында алдыңғы қатарлы технологияға айналдырды.

Оқытудың техникалық құралдары: Компьютер, ноутбук, интернет.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру және мысалдар арқылы көрсету
- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау
- Қорытынды сұрақтар мен талқылау

Оқыту әдістері мен түрлері:

- Түсіндірмелі-баяндамалық әдіс
- Көрнекілік және демонстрациялық әдіс
- Практикалық тапсырмалар орындау
- Интерактивті сұрақ-жауап және топтық талқылау

БӨЖ және ОБӨЖ тапсырмалары,олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

БӨЖ: Уитстонның «қосарланған квадрат» шифры және қосарланған орналастыру әдісі арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллды құрайды.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -20 балл

- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: Уитстонның «қосарланған квадрат» шифры және қосарланған орналастыру әдісі арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллды құрайды.

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- **БӨЖ — 60% (60 балл)**
- **ОБӨЖ — 40% (40 балл)**

Пайдалынатын әдебиеттер тізімі:

Негізгі:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Кауфман Ч., Перлман Р., Спеснер М. *Network Security: Private Communication in a Public World.* – Prentice Hall, 2016.

3. Schneier B. *Applied Cryptography.* – Wiley, 2015.

4. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

Қосымша:

1. Ж.З.Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтурсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz