№6 Лекция тақырыбы: Трисемустың шифрлау кестесі. Плейфейрдің биграмдық шифры

Лекцияның оқыту нәтижиелері: Трисемус және Плейфейр шифрларының тарихи маңызын және қолдану принциптерін түсінеді. Трисемус және Плейфейр шифрлаудың алгоритмін және шифрлау/дешифрлау алгоритмін сипаттай алады. Плейфейрдің биграмдық шифрлау жүйесінің ерекшеліктерін талдап, оны Трисемус әдісімен салыстыра алады.

Лекция мазмұны:

- Трисемус және Плейфейр шифрлаудың шығу тарихы
- Жұмыс істеу принципітері
- Артықшылықтары мен кемшіліктері

- Трисемус және Плейфейр шифрлаудың шығу тарихы

Ақпараттық қауіпсіздік қазіргі заманда өте маңызды тақырыптардың бірі. Криптография – мәліметтерді қорғаудың ең тиімді әдістерінің бірі. Бұл рефератта екі танымал классикалық шифрлау әдісітері «Трисемус шифры» және «Плейфейр шифры» қарастырылады. Олардың тарихы, жұмыс принциптері, артықшылықтары мен кемшіліктері, сонымен қатар қызықты фактілер туралы баяндалады.

Трисемус шифрын алғаш рет Иоганн Трисемус (1462–1516) атты неміс теологы, математик және астролог ойлап тапқан. Ол криптографияға ерекше қызығушылық танытып, "Polygraphia" атты еңбегінде бұл шифрлау әдісін сипаттап өткен. Орта ғасырларда бұл әдіс құпия хат алмасуда, алхимиктердің жазбаларында қолданылған.

Плейфер шифрын 1854 жылы Чарльз Уитстон ойлап тапқан, бірақ оны алғаш әскери мақсатта қолданған Чарльз Плейфер болғандықтан, шифр оның атымен аталып кеткен. Бұл әдіс Бірінші дүниежүзілік соғыста британдық әскери шифрлау жүйесінде пайдаланылған.

Жұмыс істеу принципітері

Трисемус шифры – ауыстыру (алмастыру) шифрының бір түрі. Оның негізгі идеясы – шифрлау кестесін (кілттік тор) пайдалану:

1. Кілттік сөз таңдалады (мысалы, "ҚАЗАҚСТАН").
2. Осы кілттік сөз көмегімен 5х6 тор жасалады.
3. Қалған бос орындарға алфавиттегі әріптер жазылады.
4. Әр әріп кестедегі өз орнына байланысты жаңа әріппен алмастырылады.

Плейфейр шифры екі әріптен тұратын жұптарды алмастыру арқылы жұмыс істейді. Шифрлау үшін арнайы 5х5 тор қолданылады:

1. Кілттік сөз таңдалады ("БАУЫРСАҚ" сияқты).
2. Торға алдымен осы сөздің әріптері, кейін қалған алфавит толтырылады.
3. Мәтін екі әріптен тұратын жұптарға бөлінеді.
4. Тордың ережелеріне сай әріптер алмастырылады.

Артықшылықтары мен кемшіліктері

Артықшылықтары:

- Оңай әрі жылдам шифрлау әдісі.
- Қарапайым қолдануға ыңғайлы.
- Бір әріпті емес, әріп жұптарын алмастыратындықтан, жиілікті талдауға төзімді.
- Жаңа бастап үйренетіндерге пайдалы.

Кемшіліктері:

- Жиілікті талдау арқылы бұзу оңай.
- Қосымша қорғау шараларын қажет етеді.
- Ұзын мәтіндерді шифрлау үшін тиімсіз.
- Бірдей әріптер кездессе, олардың арасына қосымша әріптер қосылады.
- Жиілікті талдауға мықтырақ болғанымен, ұзақ мәтіндер үшін жеткіліксіз қауіпсіз.

Мысал

Мысалы, "ҚҰПИЯ" кілті бойынша жасалған кесте:

Қ	Ұ	П	И	Я	А
Б	В	Г	Д	Е	Ж
З	К	Л	М	Н	О
Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Ы	Э	Ю

Енді "ҚАЗАҚ" сөзін шифрлайық:

"Қ" -> "Б"
"А" -> "Ж"
"З" -> "К"
"А" -> "Ж"
"Қ" -> "Б"

Шифрланған мәтін: "БЖКЖБ"

Шифрларды бұзу әдістері

Трисемус және Плейфер шифрларының әлсіз жақтары болғандықтан, оларды арнайы әдістермен бұзуға болады:

Жиілікті талдау әдісі - әріптердің немесе әріп жұптарының қайталануын зерттеу.

Кілттік сөзді анықтау - белгілі бір мәтін бөліктерін пайдаланып, кілтті табу.

Анық мәтіндік шабуыл (Known Plaintext Attack, KPA) - шифрланған мәтіннің бір бөлігін білу арқылы кілтті ашу.

Оқытудың техникалық құралдары: Компьютер, мультимедиялық проектор, интерактивті тақта, презентация слайдтары, интернет желісі, Python немесе онлайн шифрлау құралдары, баспа материалдары мен кестелер.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Лекция түсіндіру және демонстрация түрінде өткізіледі. Оқыту әдістері: баяндау, сұрақ-жауап, интерактивті талқылау, тәжірибелік мысалдармен жұмыс.

Түрлері: теориялық дәріс, практикалық элементтері бар аралас лекция.

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

БӨЖ: Студент Трисемус шифрлау кестесін құрып, 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: Плейфейр шифрының 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)*

Негізгі әдебиеттер:

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

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

4. Дүйсебекова, К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау: Оқу құралы. - Стер. бас - Алматы: Қазақ университеті, 2020. - 156 б. http://rmebrk.kz

6. Камалова Г.А., Диярова, Л.Б. Ақпараттық қауіпсіздік және ақпаратты қорғау: Оқу құралы. / Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті. - Алматы: Альманах, 2020. - 116б. http://rmebrk.kz

Қосымша әдебиеттер:

1. Ахметова, С. Бағдарламалау технологиясы: Лекция жинағы. / ЮКГУ им. М.О. Ауезова. - Шымкент: ОҚМУ, 2007. - 51 б. https://rmebrk.kz/book/50006