Дәріс 1. Криптологияға кіріспе: анықтамалар, принциптер

Дәріскер: PhD Темирбекова Ж.Е.

Дәріс жоспары:

- Криптография тарихы, принциптері
- Атбаш шифры
- Полибий шаршысы
- Сцитал шифры

Криптография тарихы, принциптері

- • Криптография – деректердің құпиялығы мен тұтастығын сақтау әдістері
- • Қолөнер кезеңі → ғылыми кезең (К. Шеннон, 1949)
- • Физикалық, стеганографиялық, криптографиялық әдістер

Криптографияның негізгі әдістері

- • Физикалық қорғау
- • Стеганография
- • Криптография
- • Шифрлау мен шифрын ашу анықтамалары

Керкгоффс талаптары

- 1. Жүйе іс жүзінде ашылмауы тиіс
- 2. Пайдаланушыға қолайсыздық болмауы керек
- 3. Кілт есте сақтауға жеңіл
- 4. Криптограмма берілуге ыңғайлы
- 5. Аппаратура портативті
- 6. Жүйе қарапайым болуы керек

Қазіргі шифрлар класы

- • Классикалық
- • Симметриялық (AES, DES)
- • Асимметриялық (RSA, ECC)
- • Ағындық
- • Блоктық

Қолданбалар

- • Электрондық қолтаңба
- • Электрондық ақша
- • Электрондық жеребе
- • Онлайн келісімшарттар
- • Құжаттарды қорғау
- • Электрондық дауыс беру

Атбаш шифры

- • Әріпті алфавиттің қарама-қарсы әрпімен алмастыру
- • Кілт жоқ, жалғыз түрлендіру
- • Мысалы: «баба» ⟶ «юяюя»

Полибий шаршысы

- • 5×5 кесте
- • Әріптер координаттармен алмастырылады
- • Мысалы: A → 11, B → 12

Сцитал шифры

- • Спарта, б.з.д. V ғ.
- • Бірдей диаметрлі цилиндрге таспаны орап жазу
- • Кілт – цилиндр радиусы
- • Ауыстыру шифрларының негізі

Қорытынды

- Бұл дәрісте криптологияның негізгі ұғымдары, оның құрамдас бөліктері – криптография және криптоталдау, сондай-ақ ақпаратты қорғауда қолданылатын негізгі принциптер қарастырылды. Криптология – деректердің құпиялылығын, тұтастығын, түпнұсқалығын және қолжетімділігін қамтамасыз ететін ғылым саласы екендігі атап өтілді.
- Криптография әдістері шифрлау және дешифрлау процестеріне негізделетіні, ал криптоталдау осы алгоритмдердің әлсіз тұстарын зерттейтіні көрсетілді. Ақпараттық қауіпсіздіктің негізгі принциптері – Керкхоффс принципі, қауіпсіздікке негізделген дизайн, кездейсоқтықтың маңыздылығы, кілттердің дұрыс басқарылуы сияқты қағидалар қазіргі криптожүйелердің сенімділігін қамтамасыз ететіні түсіндірілді.