Ауыстыру шифрларының математикасы: ағынды, блоктық, көпалфавитті және дискілі шифрлар.

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Шифрларды негізгі белгілері бойынша жіктеу.

Симметриялық/асимметриялық және блоктық/ағындық тәсілдерді салыстыру.

Криптографиялық беріктілік пен қорғалғандықты түсіндіру.

Имитоберіктілік және аутентификация ұғымдарын ажырату.

Қарсылас модельдерімен танысу.

Кілттер бойынша — симметриялық және асимметриялық.

Өңдеу тәсілі бойынша — блоктық және ағындық.

Түрлендіру бойынша — ауыстыру және орын алмастыру.

Алфавит саны бойынша — моноалфавиттік және полиалфавиттік.

Құрылымы бойынша — қарапайым және құрамдас шифрлар.

Анықтама: шифрлау және дешифрлау үшін ортақ құпия кілт қолданылатын жүйе.

Жіберуші мен қабылдаушы k кілтін алдын ала қауіпсіз бөлісуі керек.

Артықшылығы: үлкен көлемдегі деректерді жылдам өңдеуге қолайлы.

Мәселе: кілтті қауіпсіз тарату және сақтау.

Анықтама: математикалық байланысқан ашық және жабық кілт жұбын қолданатын жүйе.

РК — ашық кілт, таратылуы мүмкін.

SK — жабық кілт, иесінде құпия сақталады.

Қолданылуы: кілт алмасу, цифрлық қолтаңба және басқа криптографиялық міндеттер.

Цезарь шифрының мысалы

Белгі	Симметриялық	Асимметриялық
Кілт	Ортақ құпия	Ашық + жабық
Жылдамдық	Әдетте жоғары	Әдетте баяуырақ
Негізгі мәселе	Кілтті бөлісу	Жабық кілтті қорғау және ашық кілтті растау
Қолданылуы	Деректерді жаппай шифрлау	Кілт алмасу, қолтаңба

Анықтама: деректерді белгіленген ұзындықтағы блоктармен өңдейтін шифр.

Мысал: 24 биттік хабарлама 8 биттік үш блокқа бөлінеді: B_1, B_2, B_3.

Әр блок кілтке тәуелді түрлендіріледі.

Анықтама: деректерді бит/байт ағыны ретінде өңдеп, кілттік ағынмен біріктіретін тәсіл.

Мысал: М=1011, К=1100 → С=0111.

Кері есептеу: С⊕К = 1011.

Көпалфавитті шифр

Белгі	Блоктық	Ағындық
Өңдеу	Блоктар	Бит/байт ағыны
Негізгі идея	Блокты күрделі түрлендіру	Кілттік ағынмен біріктіру
Қолдану сипаты	Файлдар, сақтау, хаттамалар	Үздіксіз ағын сценарийлері

Анықтама: символ басқа символмен белгілі ереже бойынша алмастырылады.

Символдың позициясы сақталып, мәні өзгереді.

Цезарь шифры — классикалық мысал.

k=3: A→D, B→E, C→F.

Виженердің қысқа мысалы

Анықтама: символдардың мәні өзгермей, мәтіндегі орындары ауыстырылады.

Оқу мысалы: ABCDEF → ACEBDF.

Ауыстыруда символ мәні өзгереді; транспозицияда позиция өзгереді.

Ағынды шифр

Белгі	Моноалфавиттік	Полиалфавиттік
Алфавит	Бір тұрақты ауыстыру	Бірнеше ауыстыру алфавиті
Бір символ	Әдетте бірдей шифрсимвол	Орны/кілтке қарай әртүрлі болуы мүмкін
Классикалық мысал	Цезарь	Виженер

XOR операциясы

A=0,…,Z=25.

M = CAT → (2, 0, 19).

K = KEY → (10, 4, 24).

C = (12, 4, 17) → MER.

Анықтама: бірнеше қарапайым криптографиялық түрлендіруді кезекпен біріктіретін жүйе.

Қазіргі блоктық шифрлар бірнеше раунд қолдануы мүмкін.

Мақсат: ашық мәтін, кілт және шифрмәтін арасындағы қарапайым тәуелділіктерді азайту.

Анықтама: қарсыластың белгілі ресурс, уақыт және ақпарат жағдайында криптожүйені бұзу қиындығын сипаттайтын қасиет.

Беріктілікке кілт ұзындығы ғана емес, алгоритм құрылымы, кілттерді басқару және іске асыру сапасы әсер етеді.

Теориялық және практикалық (есептеуіш) беріктілік ажыратылады.

$$|K| = 2^n$$

n=8 → 256 кілт, орташа ≈128 тексеру.

n=16 → 65 536 кілт.

Кілт ұзындығы 1 битке артса, кілттер кеңістігі 2 есе өседі.

Блоктық шифрдың мысалы

Анықтама: жүйенің белгіленген қауіптерге қарсы қажетті қауіпсіздік қасиеттерін сақтай алу дәрежесі.

Алгоритм берік болса да, кілт дұрыс қорғалмаса жүйе осал болуы мүмкін.

Факторлар: алгоритм, кілт кездейсоқтығы, кілтті сақтау/тарату, іске асыру, пайдаланушы әрекеттері.

Анықтама: қарсыластың жалған хабарламаны заңды хабарлама ретінде қабылдатуына қарсы тұру қабілеті.

Құпиялылық жалғыз өзі жалған командалардан қорғамайды.

Мысал: төлем командасының сомасы мен жіберушісінің түпнұсқалығын тексеру қажет.

Блоктық шифрдың жұмыс режимі

Түрі	Нені тексереді?	Мысал
Субъект аутентификациясы	Пайдаланушы/құрылғы кім екенін	Жүйеге кіру
Хабарлама аутентификациясы	Хабарлама көзі мен өзгермегенін	Команданың түпнұсқалығын тексеру

Ағынды және блоктық шифрлар

Белгі	Хэш	MAC
Кіріс	M	M + құпия k
Нәтиже	h = H(M)	$T = MAC_k(M)$
Мақсат	Тұтастықты бақылауға негіз болатын дайджест	Тұтастық + хабарлама аутентификациясы

Дискілі шифр

Модель	Қарсыласқа қолжетімді ақпарат
Ciphertext-only	Тек шифрмәтін
Known-plaintext	Кейбір ашық мәтін + сәйкес шифрмәтін
Chosen-plaintext	Таңдалған ашық мәтіндердің шифрлану нәтижесі
Chosen-ciphertext	Таңдалған шифрмәтіндердің дешифрлану нәтижесіне шектеулі қолжетімділік

Дискілі шифрдың математикасы

Қарсылас	Әрекет	Негізгі қорғаныс қасиеті
Пассивті	Бақылау, тыңдау	Құпиялылық
Белсенді	Өзгерту, жалған хабарлама, қайта жіберу	Тұтастық, аутентификация

Дискілі шифрдың мысалы

Шифрлау → хабарлама мазмұны жасырын: құпиялылық.

Тұтастықты тексеру → өзгеріс анықталады: тұтастық.

Хабарлама аутентификациясы → заңды көзден келгені тексеріледі.

Қорытынды: криптографиялық қорғаныс тек шифрлаумен шектелмейді.

Тәсілдерді қорытынды салыстыру

Белгі	Түрлер	Негізгі айырмашылық
Кілт	Симметриялық / асимметриялық	Ортақ / ашық-жабық
Өңдеу	Блоктық / ағындық	Блок / ағын
Түрлендіру	Ауыстыру / транспозиция	Мән / позиция
Алфавит	Моно / полиалфавиттік	Бір / бірнеше алфавит
Құрылым	Қарапайым / құрамдас	Бір / бірнеше түрлендіру

1. Симметриялық және асимметриялық жүйелер қалай ажыратылады?
2. Блоктық және ағындық шифр дегеніміз не?
3. Ауыстыру мен транспозиция айырмашылығы қандай?
4. Криптографиялық беріктілік дегеніміз не?
5. $|K|=2^n$ формуласы нені білдіреді?
6. Имитоберіктілік пен аутентификация қалай байланысты?
7. MAC пен хэштің айырмашылығы неде?
8. Пассивті және белсенді қарсылас қалай ажыратылады?

Шифрларды жіктеу олардың құрылымы мен қолданылуын жүйелейді.

Криптографиялық беріктілік — шабуылды жүзеге асыру қиындығы.

Қорғалғандық алгоритмнен бөлек кілттерді басқару мен іске асыруды қамтиды.

Имитоберіктілік пен аутентификация жалған хабарламаларға қарсы маңызды.

Келесі тақырыптарда классикалық шифрлар мен олардың криптоталдауы тереңдетіледі.