2-ДӘРІС
ШИФРЛАРДЫ ӘРТҮРЛІ БЕЛГІЛЕРІ БОЙЫНША ЖІКТЕУ. КРИПТОГРАФИЯЛЫҚ БЕРІКТІЛІК, ҚОРҒАЛҒАНДЫҚ, ИМИТОБЕРІКТІЛІК ЖӘНЕ АУТЕНТИФИКАЦИЯ

Дәрістің мақсаты

Шифрларды негізгі жіктеу белгілері бойынша жүйелеу, симметриялық және асимметриялық, блоктық және ағындық, моноалфавиттік және полиалфавиттік тәсілдердің айырмашылықтарын түсіндіру; криптографиялық беріктілік, қорғалғандық, имитоберіктілік және аутентификация ұғымдарын мысалдармен ашу; қарсылас пен криптоталдау модельдері туралы бастапқы түсінік қалыптастыру.

Шифрларды не үшін жіктейміз?

Криптографиялық алгоритмдер бірдей мақсатқа қызмет еткенімен, олардың кілттерді қолдану тәсілі, өңдеу бірлігі, математикалық құрылымы және қолданылу ортасы әртүрлі. Жіктеу белгілі бір есепке лайық алгоритм класын таңдауға, оның артықшылықтары мен шектеулерін түсінуге және қауіпсіздік қасиеттерін салыстыруға мүмкіндік береді.

- Кілттердің түрі бойынша: симметриялық және асимметриялық.
- Деректерді өңдеу тәсілі бойынша: блоктық және ағындық.
- Классикалық түрлендіру бойынша: ауыстыру және орын алмастыру.
- Алфавит саны бойынша: моноалфавиттік және полиалфавиттік.
- Құрылымы бойынша: жеке түрлендірулер және құрамдас шифрлар.

Кілттерді қолдану тәсілі бойынша жіктеу:

1) Симметриялық криптография

Симметриялық криптожүйе – шифрлау және дешифрлау үшін бір ортақ құпия кілт немесе бір-бірінен оңай есептелетін құпия кілттер қолданылатын жүйе.

$$\mathbf{C = E_k(M),} \quad \mathbf{M = D_k(C)}$$

Мұнда жіберуші мен қабылдаушы k құпия кілтін алдын ала қауіпсіз түрде бөлісуі керек. Мысал: Алиса мен Бобта бірдей k кілті бар. Алиса M хабарламасын шифрлап C алады, Боб сол кілтпен C-ні қайта ашады.

Артықшылығы: үлкен көлемдегі деректерді жылдам өңдеуге қолайлы.

Негізгі ұйымдастырушылық мәселе: құпия кілтті қауіпсіз тарату және сақтау.

2) Асимметриялық криптография

Асимметриялық криптожүйе – математикалық байланысқан екі кілтті қолданатын жүйе: ашық кілт және жабық кілт. Ашық кілт таратылуы мүмкін, ал жабық кілт иесінде құпия сақталады.

$$\mathbf{C = E_(PK)(M),} \quad \mathbf{M = D_(SK)(C)}$$

PK – ашық кілт, SK – жабық кілт. Мысал: Боб өзінің ашық кілтін жариялайды. Алиса сол кілтпен хабарламаны шифрлайды. Шифрмәтінді Боб өзінің жабық кілтімен ашады.

Белгі	Симметриялық	Асимметриялық
Кілт	Ортақ құпия кілт	Ашық және жабық кілт
Жылдамдық	Әдетте жоғары	Әдетте баяуырақ

Негізгі мәселе	Кілтті қауіпсіз бөлісу	Жабық кілтті қорғау, ашық кілттің түпнұсқалығын растау
Қолданылуы	Деректерді жаппай шифрлау	Кілт алмасу, цифрлық қолтаңба, шағын деректерді қорғау

3) Блоктық және ағындық шифрлар

Блоктық шифр – ашық мәтінді белгіленген ұзындықтағы блоктарға бөліп, әр блокты кілтке тәуелді түрлендіретін шифр. Формалды түрде n биттік блок үшін:

$$\mathbf{E_k : \{0,1\}^n \rightarrow \{0,1\}^n}$$

Мысал. Егер оқу моделінде блок өлшемі 8 бит болса, 24 биттік хабарлама үш блокқа бөлінеді: B_1, B_2, B_3. Әр блок жеке немесе арнайы жұмыс режиміне сәйкес өңделеді.

Ағындық шифр – деректерді биттер немесе шағын символдар ағыны түрінде өңдеп, кілттік ағынмен біріктіретін тәсіл. Қарапайым модель:

$$\mathbf{C_i = M_i \oplus K_i, \quad M_i = C_i \oplus K_i}$$

XOR қасиеті бойынша $(a \oplus b) \oplus b = a$. Мысал: M=1011, K=1100 болса, C=0111. Қайтадан $C \oplus K = 1011$.

Белгі	*Блоктық шифр*	*Ағындық шифр*
Өңдеу	Белгілі өлшемді блоктар	Бит/байт ағыны
Негізгі идея	Блокты күрделі түрлендіру	Кілттік ағынмен біріктіру
Қолдану сипаты	Файлдар, сақтау, желілік хаттамалар	Үздіксіз ағын, кейбір байланыс сценарийлері

4) Ауыстыру және орын алмастыру шифрлары

Ауыстыру шифры (substitution cipher) – ашық мәтіндегі символдар басқа символдармен белгілі ереже бойынша алмастырылатын шифр. Символдардың орны негізінен сақталады, бірақ мәндері өзгереді. Цезарь шифры – қарапайым мысал.

$$\mathbf{E_k(x) = (x + k) \bmod m}$$

m – алфавит өлшемі. Мысалы, m=26 және k=3 болса A→D, B→E, C→F.

Орын алмастыру немесе транспозициялық шифр (transposition cipher) – символдардың өздері өзгермей, олардың мәтіндегі орындары белгілі ереже бойынша ауыстырылатын шифр.

Мысал. ABCDEF мәтінін тақ және жұп позициялар бойынша қайта орналастырудың оқу нұсқасы: ACEBDF. Мұнда A–F символдары өзгерген жоқ, тек реті өзгерді.

Белгі	*Ауыстыру*	*Орын алмастыру*
Не өзгереді?	Символдың мәні	Символдың позициясы
Не сақталады?	Позициялар құрылымы	Символдар құрамы
Мысал	Цезарь шифры	Бағандық/позициялық транспозиция

5) Моноалфавиттік және полиалфавиттік шифрлар

Моноалфавиттік шифрда бүкіл хабарлама бойында бір тұрақты ауыстыру ережесі қолданылады. Сондықтан бір ашық символ әдетте бірдей шифрсимволға айналады. Бұл жиілік заңдылықтарының сақталуына әкелуі мүмкін.

Полиалфавиттік шифрда бірнеше ауыстыру алфавиті кезектесіп қолданылады. Бір ашық символ мәтіндегі орнына немесе кілтке байланысты әртүрлі шифрсимволдарға айналуы мүмкін. Виженер шифры – классикалық мысал.

$$C_i = (M_i + K_i) \bmod m$$

Мысал: A=0,...,Z=25. M=CAT → (2,0,19), қайталанатын кілт KEY → (10,4,24). C=(12,4,17) → MER.

6) Құрамдас шифрлар

Құрамдас шифр – қауіпсіздікті күшейту үшін бірнеше қарапайым криптографиялық түрлендіруді кезекпен біріктіретін жүйе. Қазіргі блоктық шифрлар көбіне бірнеше раундта ауыстыру, орын алмастыру, кілтпен араластыру сияқты операцияларды қолданады.

$$C = E_{kr}(\dots E_{k2}(E_{k1}(M)) \dots)$$

Бірнеше раундтың мақсаты – ашық мәтін, кілт және шифрмәтін арасындағы қарапайым статистикалық тәуелділіктерді азайту. Бұл идея кейінгі дәрістерде шашырату (diffusion) және араластыру (confusion) ұғымдарымен тереңдетіледі.

Криптографиялық беріктілік

Криптографиялық беріктілік – қарсыластың белгілі ресурстар, уақыт және қолжетімді ақпарат жағдайында криптожүйенің қорғанысын бұзу қиындығын сипаттайтын қасиет. Беріктілік тек кілт ұзындығымен емес, алгоритм құрылымымен, кілттерді басқарумен, іске асыру сапасымен және шабуыл моделіне байланысты бағаланады.

Теориялық және практикалық беріктілік

Теориялық тұрғыдан абсолютті немесе ақпараттық-теориялық қауіпсіздік ұғымы қарсыластың есептеу қуаты шексіз болса да, шифрмәтіннен ашық мәтін туралы жеткілікті ақпарат ала алмауын сипаттайды. Практикалық немесе есептеуіш беріктілік – шабуылды орындауға қажет ресурс нақты жағдайда қолжетімсіз немесе экономикалық тұрғыдан мәнсіз болған жағдай.

Кілт ұзындығы және толық перебор

$$|K| = 2^n$$

n биттік кілт үшін мүмкін кілттер саны 2^n. Толық перебор кезінде қарсылас барлық ықтимал кілттерді тексереді. Орташа жағдайда дұрыс кілт кеңістіктің шамамен жартысын тексергеннен кейін табылуы мүмкін:

$$N_avg \approx 2^{n-1}$$

Оқу мысалы: n=8 болса 256 кілт бар, орташа шамамен 128 нұсқа тексеріледі. n=16 болса 65 536 кілт. Бұл мысал кілт ұзындығы бір битке өскен сайын кеңістік екі есе өсетінін көрсетеді.

Қорғалғандық ұғымы

Қорғалғандық – ақпараттық жүйенің немесе криптографиялық механизмнің белгіленген қауіптерге қарсы қажетті қауіпсіздік қасиеттерін сақтай алу дәрежесі. Криптографиялық алгоритм берік болғанымен, кілт ашық сақталса немесе пайдаланушы оны бөтен адамға берсе, бүкіл жүйенің қорғалғандығы төмендейді.

- Алгоритмнің криптографиялық сапасы.
- Кілт ұзындығы және кілттің кездейсоқтығы.
- Кілттерді сақтау және тарату.
- Бағдарламалық және аппараттық іске асыру.
- Пайдаланушы әрекеттері және қауіпсіздік саясаты.

Имитоберіктілік

Имитоберіктілік – қарсыластың заңды қатысушы атынан жалған хабарлама құрып, оны жүйеге шынайы хабарлама ретінде қабылдатуына қарсы тұру қабілеті. Мұнда мәселе тек хабарламаны құпия сақтау емес, оның түпнұсқалығы мен тұтастығын тексеру болып табылады.

Мысал. Банк жүйесінде «А шотынан В шотына 10 000 теңге аудару» деген хабарлама жіберілді делік. Қарсылас мәтінді оқи алмаса да, жалған төлем командасын жүйеге қабылдата алса, құпиялылықтың өзі жеткіліксіз. Сондықтан хабарламаның авторын және өзгермегенін тексеретін механизм қажет.

Аутентификация

Аутентификация – субъектінің, құрылғының немесе хабарламаның мәлімделген түпнұсқалығын тексеру процесі.

Түрі	*Нені тексереді?*	*Мысал*
Субъект аутентификациясы	Пайдаланушы/құрылғы кім екенін	Жүйеге кіру кезінде пайдаланушыны тексеру
Хабарлама аутентификациясы	Хабарламаның күтілген көзден келгенін және өзгермегенін	Қабылданған команданың түпнұсқалығын тексеру

Хабарлама аутентификациясында MAC (Message Authentication Code) тәрізді криптографиялық механизмдер қолданылуы мүмкін. Жалпы түрде:

$$\mathbf{T = MAC_k(M)}$$

Жіберуші M хабарламасы үшін құпия k кілтімен T тегін есептейді. Қабылдаушы сол кілтпен тегті қайта есептеп салыстырады. Егер хабарлама өзгерсе немесе дұрыс кілт қолданылмаса, тексеру сәтсіз болуы тиіс.

Хэш-функция және MAC айырмашылығына кіріспе

Криптографиялық хэш-функция хабарламаны тұрақты ұзындықтағы мәнге түрлендіреді:

$$\mathbf{h = H(M)}$$

Хэштің өзі құпия кілтті міндетті түрде қолданбайды, сондықтан ол жалғыз өзі хабарламаның кімнен келгенін дәлелдемейді. MAC құпия кілтке тәуелді болғандықтан, хабарлама аутентификациясына арналған. Бұл ұғымдар кейінгі тақырыптарда кеңейтіледі.

Белгі	*Хэш*	*MAC*
Кіріс	Хабарлама M	Хабарлама M + құпия кілт k

Нәтиже	h = H(M)	T = MAC_k(M)
Негізгі мақсат	Тұтастықты бақылауға негіз болатын дайджест	Тұтастық + хабарлама түпнұсқалығын тексеру

Қарсылас модельдері

Криптоталдауда қарсыластың қандай ақпаратқа қол жеткізе алатыны маңызды. Төмендегі модельдер шабуылдың бастапқы мүмкіндігін сипаттайды; олар нақты шабуылды орындау нұсқаулығы емес, криптожүйенің беріктігін бағалауға арналған теориялық модельдер.

Модель	*Қарсыласқа белгілі/қолжетімді ақпарат*
Ciphertext-only	Тек бір немесе бірнеше шифрмәтін
Known-plaintext	Шифрмәтінмен бірге кейбір сәйкес ашық мәтіндер
Chosen-plaintext	Қарсылас таңдаған ашық мәтіндердің шифрлану нәтижелерін ала алады
Chosen-ciphertext	Қарсылас таңдаған шифрмәтіндердің дешифрлану нәтижелеріне шектеулі түрде қол жеткізе алады

Пассивті және белсенді қарсылас

Пассивті қарсылас байланыс арнасын бақылайды, бірақ хабарламаларды өзгертпейді. Оның мақсаты көбіне ақпарат алу. Белсенді қарсылас хабарламаны өзгертуге, қайта жіберуге, жалған хабарлама енгізуге немесе байланыс процесіне араласуға тырысуы мүмкін.

Қарсылас	*Әрекет сипаты*	*Қорғанысқа қатысты негізгі қасиет*
Пассивті	Бақылау, тыңдау	Құпиялылық
Белсенді	Өзгерту, жалған хабарлама, қайта жіберу	Тұтастық, аутентификация, хаттамалық қорғаныс

Бір мысалда бірнеше қауіпсіздік қасиеті

Алиса Бобқа электрондық төлем командасын жібереді. 1) Егер хабарлама шифрланса, Ева оның мазмұнын оқи алмайды – құпиялылық. 2) Егер тұтастықты тексеру механизмі болса, соманың өзгергені анықталады – тұтастық. 3) Егер хабарлама аутентификациясы қолданылса, Боб команданың заңды тараптан келгенін тексереді – түпнұсқалық. Осыдан криптографиялық қорғаныс бір ғана шифрлау операциясымен шектелмейтіні көрінеді.

Қорытынды жіктеу кестесі

Жіктеу белгісі	*Негізгі түрлер*	*Мысал/идея*
Кілт бойынша	Симметриялық / асимметриялық	Ортақ кілт / ашық-жабық кілт
Өңдеу бойынша	Блоктық / ағындық	Блоктар / кілттік ағын
Түрлендіру бойынша	Ауыстыру / орын алмастыру	Символ мәні / позициясы
Алфавит бойынша	Моноалфавиттік / полиалфавиттік	Бір / бірнеше ауыстыру алфавиті
Құрылым бойынша	Қарапайым / құрамдас	Бір түрлендіру / бірнеше раунд

Қорытынды

Шифрларды жіктеу олардың құрылымы мен қолданылуын түсінуге мүмкіндік береді. Симметриялық және асимметриялық жүйелер кілттерді ұйымдастыруымен, блоктық және ағындық шифрлар деректерді өңдеу тәсілімен, ал ауыстыру және орын алмастыру шифрлары түрлендіру сипатымен ерекшеленеді. Криптографиялық беріктілік алгоритмнің шабуылға қарсы тұру қиындығын сипаттаса, жалпы қорғалғандық кілттерді басқару мен іске асыруды да қамтиды. Имитоберіктілік пен аутентификация жалған хабарламаларды қабылдаудан қорғау үшін маңызды.

16. Бақылау сұрақтары

1. Шифрларды қандай негізгі белгілер бойынша жіктеуге болады?
2. Симметриялық және асимметриялық криптожүйелердің айырмашылығы қандай?
3. Блоктық және ағындық шифрлар қалай ажыратылады?
4. Ауыстыру мен орын алмастыру шифрының айырмашылығы неде?
5. Моноалфавиттік және полиалфавиттік шифр дегеніміз не?
6. Криптографиялық беріктілік дегеніміз не?
7. 2^n формуласы нені көрсетеді?
8. Қорғалғандыққа алгоритмнен басқа қандай факторлар әсер етеді?
9. Имитоберіктілік дегеніміз не?
10. Субъект және хабарлама аутентификациясының айырмашылығы қандай?
11. MAC пен хэштің негізгі айырмашылығы неде?
12. Пассивті және белсенді қарсылас қалай ажыратылады?
13. Ciphertext-only және known-plaintext модельдерінің айырмашылығы қандай?

Ұсынылатын әдебиеттер

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Алматы: ҚазҰТЗУ, 2016.

2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері. Алматы: АЭжБУ, 2020.

3. Васильева И.Н. Криптографические методы защиты информации. М.: Юрайт, 2024.

4. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. М.: Юрайт, 2024.

5. Омассон Ж.-Ф. О криптографии всерьез. М.: ДМК Пресс, 2021.

6. Рацеев С.М. Математические методы защиты информации и их основы. М.: Лань, 2023.