1-ДӘРІС
КІРІСПЕ. КРИПТОГРАФИЯНЫҢ НЕГІЗГІ ТҮСІНІКТЕРІ МЕН АНЫҚТАМАЛАРЫ.
КРИПТОГРАФИЯ ТАРИХЫ. ШИФРЛАРДЫҢ ФОРМАЛДЫ ҮЛГІЛЕРІ

Дәрістің мақсаты:

Студенттерді криптографияның негізгі ұғымдарымен, ақпаратты криптографиялық қорғаудың мақсаттары мен міндеттерімен, криптографияның тарихи даму кезеңдерімен және шифрлардың формалды математикалық модельдерімен таныстыру. Дәріс соңында студент ашық мәтін, шифрмәтін, кілт, шифрлау, дешифрлау, криптожүйе, криптоталдау ұғымдарын ажыратып, қарапайым шифрлау процесін математикалық түрде сипаттай алуы тиіс.

Ақпаратты қорғау және криптография

Қазіргі ақпараттық қоғамда деректер компьютерлерде, мобильді құрылғыларда, серверлерде және бұлттық жүйелерде сақталады және желілер арқылы үздіксіз беріледі. Ақпараттың цифрлық түрде сақталуы оны өңдеуді жеңілдеткенімен, рұқсатсыз оқу, өзгерту, көшіру немесе жалған хабарлама жіберу сияқты қауіптерді де арттырады.

Ақпараттық қауіпсіздік – ақпараттың және оны өңдейтін ақпараттық жүйелердің қорғалу жағдайы. Ақпараттық қауіпсіздіктің классикалық үш негізгі қасиеті құпиялылық, тұтастық және қолжетімділік болып табылады.

– Құпиялылық (confidentiality) – ақпаратқа тек оған рұқсаты бар субъектілердің қол жеткізуін қамтамасыз ету.

– Тұтастық (integrity) – ақпараттың рұқсатсыз өзгертілмеуін, жойылмауын немесе бұрмаланбауын қамтамасыз ету.

– Қолжетімділік (availability) – рұқсаты бар пайдаланушының қажетті ақпаратты немесе қызметті қажет уақытында алу мүмкіндігі.

Мысал. Университеттің ақпараттық жүйесіндегі студент бағалары бөгде адамға көрінбеуі тиіс – бұл құпиялылық. Бағаны рұқсатсыз өзгертуге болмайды – бұл тұтастық. Студент пен оқытушы жүйеге белгіленген уақытта кіре алуы керек – бұл қолжетімділік.

Криптография ұғымы

Криптография (грек тіліндегі kryptos – «жасырын», grapho – «жазамын») – ақпаратты математикалық түрлендіру әдістері арқылы қорғауды зерттейтін ғылым және практикалық әдістер жиынтығы.

Криптографияның негізгі идеясы – бастапқы ақпаратты арнайы алгоритм мен кілттің көмегімен бөгде адам түсіне алмайтын формаға түрлендіру. Қажетті кілті бар заңды пайдаланушы ғана ақпаратты бастапқы қалпына келтіре алады.

Криптология – криптография мен криптоталдауды біріктіретін кең ұғым.

Криптография – ақпаратты қорғау әдістерін құру және зерттеу.

Криптоталдау – кілт туралы толық ақпаратсыз криптографиялық қорғанысты талдау, оның әлсіз жақтарын анықтау және шифрланған ақпаратты қалпына келтіру мүмкіндігін зерттеу.

Осылайша, криптограф жаңа қорғау механизмін құруға ұмтылса, криптоталдаушы сол механизмнің қаншалықты сенімді екенін тексереді.

Криптографияның негізгі міндеттері

Заманауи криптография тек ақпаратты «жасырумен» шектелмейді. Ол бірнеше маңызды қауіпсіздік міндеттерін шешеді.

Құпиялылық – хабарламаның мазмұнын рұқсатсыз тұлғалардан жасыру.

Тұтастық – хабарламаның жіберілгеннен кейін өзгермегенін тексеру.

Аутентификация – пайдаланушының, құрылғының немесе хабарламаның шынайылығын тексеру.

Теріске шығармау (non-repudiation) – белгілі бір әрекетті орындаған субъектінің кейін оны негізсіз жоққа шығаруына жол бермеуге бағытталған қасиет.

Мысал. Электрондық құжатты жіберген кезде шифрлау оның мазмұнын жасырады; криптографиялық бақылау механизмі құжаттың өзгермегенін тексереді; цифрлық қолтаңба құжатқа кім қол қойғанын растауға көмектеседі.

Негізгі терминдер мен анықтамалар

Ашық мәтін (plaintext) – шифрлауға дейінгі бастапқы, оқуға түсінікті ақпарат.

***Шифрмәтін* (*ciphertext*)** – шифрлау нәтижесінде алынған түрлендірілген ақпарат.

***Шифр* (*cipher*)** – ашық мәтінді шифрмәтінге және кері бағытта түрлендіру ережелерінің немесе алгоритмдерінің жиынтығы.

Кілт (key) – криптографиялық түрлендірудің нақты нәтижесін анықтайтын параметр.

Шифрлау (encryption) – ашық мәтінді шифрмәтінге түрлендіру процесі.

Дешифрлау (decryption) – дұрыс кілттің көмегімен шифрмәтінді бастапқы ашық мәтінге қалпына келтіру процесі.

Криптожүйе (cryptosystem) – алфавиттер, кілттер, шифрлау және дешифрлау алгоритмдері мен оларды қолдану ережелерінен тұратын жүйе.

Қарсылас (adversary) – қорғалатын ақпаратты рұқсатсыз алуға, өзгертуге немесе криптографиялық механизмді бұзуға тырысатын тарап.

Криптографиялық байланыстың жалпы моделі

Криптографияда түсіндіру үшін шартты түрде Алиса (Alice) – хабарлама жіберуші, Боб (Bob) – хабарламаны қабылдаушы, ал Ева (Eve) – байланыс арнасын бақылауға тырысатын қарсылас ретінде алынады.

Алиса Бобқа M хабарламасын жібергісі келеді. Ашық арна арқылы M хабарламасын тікелей жіберсе, Ева оны оқуы мүмкін. Сондықтан Алиса хабарламаны K кілтімен E шифрлау алгоритмі арқылы түрлендіреді. Нәтижесінде C шифрмәтіні алынады. Боб C шифрмәтінін қабылдап, D дешифрлау алгоритмі мен тиісті кілтті пайдаланып M хабарламасын қалпына келтіреді.

$$\mathbf{M \rightarrow E(K, M) \rightarrow C \rightarrow D(K, C) \rightarrow M}$$

Мұндағы M – ашық мәтін, C – шифрмәтін, K – кілт, E – шифрлау алгоритмі, D – дешифрлау алгоритмі.

Шифрдың формалды математикалық моделі

Криптографиялық жүйені математикалық тұрғыдан бірнеше жиын арқылы сипаттауға болады:

M – мүмкін болатын ашық мәтіндер жиыны (message space).

C – мүмкін болатын шифрмәтіндер жиыны (ciphertext space).

K – мүмкін болатын кілттер жиыны (key space).

E – шифрлау түрлендірулерінің жиыны.

D – дешифрлау түрлендірулерінің жиыны.

Әрбір $k \in K$ кілті үшін шифрлау функциясы E_k және оған сәйкес дешифрлау функциясы D_k анықталады.

$$\mathbf{C = E_k(M)}$$

$$\mathbf{M = D_k(C)}$$

Дұрыс құрылған криптожүйенің негізгі шарты – заңды кілтпен шифрланған хабарламаны сол жүйенің тиісті дешифрлау операциясы бастапқы қалпына келтіруі керек:

$$D_k(E_k(M)) = M$$

Бұл теңдік криптографиялық түрлендірудің дұрыстығын сипаттайды.

Қарапайым формалды мысал: Цезарь шифры

Цезарь шифры – әрбір әріпті алфавитте белгілі бір тұрақты қадамға жылжытуға негізделген классикалық ауыстыру шифры. Түсіндіру үшін 26 әріптен тұратын латын алфавитін 0-ден 25-ке дейін нөмірлейік: A=0, B=1, ..., Z=25.

Егер кілт k=3 болса, шифрлау формуласы:

$$E_k(x) = (x + k) \bmod 26$$

ал дешифрлау формуласы:

$$D_k(y) = (y - k) \bmod 26$$

Мысал: CAT сөзін шифрлайық. C=2, A=0, T=19. k=3 болғанда C→F, A→D, T→W. Сондықтан:

CAT → FDW

Кері түрлендіруде F→C, D→A, W→T, яғни бастапқы CAT мәтіні қалпына келеді. Бұл мысал алгоритмнің ашық болуы мүмкін екенін, ал нақты түрлендіруді кілт анықтайтынын көрсетеді.

Кілт және кілттер кеңістігі

Кілт криптографиялық жүйенің маңызды элементі. Бір алгоритм әртүрлі кілттермен әртүрлі шифрмәтін береді. Мүмкін болатын барлық кілттердің жиыны кілттер кеңістігі деп аталады.

Егер кілт ұзындығы n бит болса, теориялық түрде мүмкін кілттер саны:

$$|K| = 2^n$$

Мысалы, 8 биттік кілт үшін $2^8 = 256$ мүмкіндік бар. Бұл оқу мысалы үшін жеткілікті болғанымен, нақты қорғаныс үшін өте аз. Кілт кеңістігінің көлемі криптожүйенің толық переборға қарсы беріктігіне әсер ететін факторлардың бірі.

Маңызды: үлкен кілт кеңістігі өздігінен алгоритмнің толық қауіпсіз екенін білдірмейді. Алгоритмнің математикалық құрылымында осалдық болса, қарсылас барлық кілтті тексермей-ақ шабуыл жасауы мүмкін.

Алгоритмнің құпиялығы және Керкгоффс принципі

Криптографиядағы маңызды қағидалардың бірі – жүйенің қауіпсіздігі алгоритмнің жасырын болуына ғана тәуелді болмауы тиіс. Қарсылас алгоритмнің қалай жұмыс істейтінін білсе де, құпия кілтті білмей қорғалған ақпаратты қалпына келтіре алмауы керек. Бұл идея Керкгоффс принципімен байланысты.

Практикалық мағынасы: сенімді криптожүйеде алгоритм ашық түрде талқыланып, зерттелуі мүмкін, ал құпия сақталатын негізгі элемент – кілт. Ашық стандарттардың кең сараптамадан өтуі олардың қателері мен әлсіз жақтарын ертерек анықтауға мүмкіндік береді.

10. Криптография, кодтау және стеганография

Бұл үш ұғымды шатастырмау қажет.

Әдіс	Негізгі мақсат	Құпия кілт міндетті ме?	Қарапайым мысал
Криптография	Ақпараттың мазмұнын қорғау	Көп жағдайда иә	Мәтінді шифрлау
Кодтау	Ақпаратты басқа форматта ұсыну	Жоқ	Мәтінді кодтық форматта ұсыну

Стеганография	Ақпараттың бар екенін жасыру	Міндетті емес	Хабарламаны басқа тасымалдаушы ішінде жасыру

Мысал. Егер «SALAM» сөзі белгілі ереже бойынша түсініксіз символдар тізбегіне айналса және оны қалпына келтіру үшін кілт қажет болса – бұл шифрлау. Егер ақпарат тек басқа стандартты көрініске ауыстырылса – бұл кодтау. Ал хабарлама сурет немесе басқа тасымалдаушының ішінде байқалмайтындай жасырылса – бұл стеганография.

Криптография тарихының негізгі кезеңдері

Криптографияның тарихы ақпаратты құпия сақтау қажеттілігімен бірге дамыды. Оның эволюциясын шартты түрде бірнеше кезеңге бөлуге болады.

1) Ежелгі және классикалық кезең. Қарапайым ауыстыру және орын алмастыру әдістері қолданылды. Спартадағы скитала, Цезарь шифры сияқты тәсілдер осы кезеңнің белгілі мысалдары.

2) Орта ғасырлар және полиалфавиттік идеялардың дамуы. Бір ғана ауыстыру алфавитінің әлсіздігі түсініліп, бірнеше алфавитті қолданатын әдістер пайда болды. Кейін мұндай тәсілдер Виженер шифры сияқты жүйелерде көрініс тапты.

3) Механикалық және электромеханикалық кезең. Байланыс көлемінің өсуі шифрлау процесін механикаландыруға әкелді. Роторлық машиналар күрделі көпқадамды түрлендірулерді автоматты орындауға мүмкіндік берді.

4) Компьютерлік криптография кезеңі. Электрондық есептеу техникасының дамуы биттер мен блоктарға негізделген алгоритмдерді кеңінен қолдануға мүмкіндік берді. Симметриялық блоктық шифрлар стандарттала бастады.

5) Ашық кілтті криптографияның пайда болуы. Бір кілтті алдын ала құпия арнамен бөлісу мәселесін шешуге бағытталған жаңа математикалық тәсілдер ұсынылды. Ашық және жабық кілт жұбына негізделген жүйелер электрондық қолтаңба және кілт алмасу технологияларының дамуына жол ашты.

6) Қазіргі кезең. Криптография интернет, мобильді байланыс, бұлттық есептеу, электрондық үкімет, банк жүйелері, цифрлық қолтаңба және басқа көптеген цифрлық қызметтердің базалық қорғаныс тетіктерінің біріне айналды.

Классикалық және қазіргі криптографияның айырмашылығы

Белгі	Классикалық криптография	Қазіргі криптография
Өңдеу бірлігі	Әріптер, символдар	Биттер, байттар, блоктар
Негізгі тәсілдер	Ауыстыру, орын алмастыру	Күрделі математикалық және логикалық түрлендірулер
Есептеу	Қолмен немесе механикалық	Компьютерлік
Қолданылуы	Құпия хат алмасу	Желі, банк, электрондық қызметтер, деректерді сақтау
Қауіпсіздікті бағалау	Көбіне тәжірибелік	Математикалық және есептеу күрделілігіне негізделген талдау

Криптографиялық жүйеге қойылатын жалпы талаптар

Заңды пайдаланушы үшін шифрлау және дешифрлау процедуралары анық әрі дұрыс жұмыс істеуі тиіс.

Кілтті білмейтін қарсылас үшін бастапқы ақпаратты қалпына келтіру практикалық тұрғыдан қиын болуы тиіс.

Бір ғана алгоритмді құпия сақтау қауіпсіздіктің негізгі шарты болмауы тиіс.

Кілттерді генерациялау, сақтау, тарату және ауыстыру қауіпсіз ұйымдастырылуы тиіс.

Қолданылатын криптографиялық механизм қорғалатын ақпараттың құндылығы мен жүйенің қауіп моделіне сәйкес болуы тиіс.

Криптографияның қолданылу салалары

- Интернет арқылы берілетін деректерді қорғау.
- Электрондық пошта және хабар алмасу жүйелерін қорғау.
- Банк операциялары мен электрондық төлемдерді қорғау.
- Файлдар мен деректер қорын шифрлау.
- Пайдаланушылар мен құрылғыларды аутентификациялау.
- Электрондық цифрлық қолтаңба және электрондық құжат айналымы.
- Бұлттық инфрақұрылымдардағы деректерді қорғау.
- Мобильді және корпоративтік ақпараттық жүйелердегі қауіпсіз байланыс.

Толық мысал: қарапайым криптожүйені сипаттау

Берілсін M = {A, B, ..., Z}, K = {0,1,...,25}. Әрбір k кілті үшін $E_k(x)=(x+k) \bmod 26$, ал $D_k(y)=(y-k) \bmod 26$ болсын.

Хабарлама: HELLO. Кілт: k=3. Әріптерді санға ауыстырамыз: H=7, E=4, L=11, L=11, O=14. Әр санға 3 қосып, 26 модулі бойынша қалдық аламыз: 10, 7, 14, 14, 17. Олар K, H, O, O, R әріптеріне сәйкес келеді.

HELLO → KHOOR

Дешифрлау кезінде әр шифрланған символдан 3 алынады және 26 модулі бойынша есептеледі. Нәтижесінде HELLO қайта алынады. Бұл мысал M, C, K, E және D элементтерінің өзара байланысын көрсетеді.

Қорытынды

Криптография – ақпараттық қауіпсіздіктің негізгі технологиялық бағыттарының бірі. Оның көмегімен ақпараттың құпиялылығын, тұтастығын, аутентификациясын және бірқатар басқа қауіпсіздік қасиеттерін қамтамасыз етуге болады. Кез келген криптографиялық жүйені түсіну үшін ашық мәтін, шифрмәтін, алгоритм, кілт, шифрлау және дешифрлау ұғымдарын нақты ажырату қажет. Формалды түрде криптожүйе хабарламалар, шифрмәтіндер және кілттер кеңістіктерімен, сондай-ақ шифрлау мен дешифрлау функцияларымен сипатталады. Келесі дәрісте шифрларды әртүрлі белгілері бойынша жіктеу және криптографиялық беріктілік ұғымдары қарастырылады.

Бақылау сұрақтары

1. Криптография дегеніміз не және оның негізгі мақсаты қандай?
2. Криптография мен криптоталдаудың айырмашылығы неде?
3. Құпиялылық, тұтастық және қолжетімділік ұғымдарын түсіндіріңіз.
4. Ашық мәтін және шифрмәтін дегеніміз не?
5. Криптографиялық кілт қандай қызмет атқарады?
6. Шифрлау және дешифрлау процестерін формуламен көрсетіңіз.
7. M, C, K, E, D жиындары нені білдіреді?
8. $D_k(E_k(M)) = M$ шартының мағынасы қандай?
9. Керкгоффс принципінің негізгі идеясы қандай?

10. Криптография, кодтау және стеганографияның айырмашылығы неде?
11. Цезарь шифры қалай жұмыс істейді?
12. Кілт ұзындығы n бит болғанда кілттер саны қалай есептеледі?
13. Криптографияның тарихи даму кезеңдерін атаңыз.
14. Қазіргі ақпараттық жүйелерде криптография қай салаларда қолданылады?

Ұсынылатын әдебиеттер

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016.
2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері: сандар теориясының, топтардың, өрістердің, сақиналардың элементтері. 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. Практическое введение в современное шифрование. М.: ДМК Пресс, 2021.
6. Рацеев С.М. Математические методы защиты информации и их основы. Сборник задач. М.: Лань, 2023.