1-ДӘРІС

Криптографияға кіріспе

Негізгі түсініктер мен анықтамалар • Криптография тарихы • Шифрлардың формалды үлгілері

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Криптографияның негізгі ұғымдары мен терминдерін түсіну.

Ақпаратты криптографиялық қорғаудың мақсаттары мен міндеттерін ажырату.

Шифрлау және дешифрлау процесін формалды түрде сипаттау.

Криптографияның тарихи даму кезеңдерін білу.

Қарапайым криптожүйенің жұмысын мысал арқылы түсіндіру.

Ақпараттық қауіпсіздіктің негізгі қасиеттері

Қасиет	Анықтама	Мысал
Құпиялылық	Ақпаратқа тек рұқсаты бар субъектілер қол жеткізеді	Студент бағасын бөгде адам көрмеуі тиіс
Тұтастық	Ақпарат рұқсатсыз өзгертілмейді немесе бұрмаланбайды	Бағаны рұқсатсыз өзгертуге болмайды
Қолжетімділік	Рұқсаты бар пайдаланушы ақпаратты қажет уақытында алады	Оқытушы жүйеге уақытында кіре алады

Криптография және криптология

Криптография – ақпаратты математикалық түрлендіру әдістері арқылы қорғауды зерттейтін ғылым және практикалық әдістер жиынтығы.

Криптология – криптография мен криптоталдауды біріктіретін кең ұғым.

Криптоталдау – кілт туралы толық ақпаратсыз криптографиялық қорғаныстың әлсіз жақтарын зерттеу.

Криптографияның негізгі міндеттері

Құпиялылық — хабарламаның мазмұнын рұқсатсыз тұлғалардан жасыру.

Тұтастық — хабарламаның өзгермегенін тексеру.

Аутентификация — пайдаланушының, құрылғының немесе хабарламаның шынайылығын тексеру.

Теріске шығармау — белгілі бір әрекетті орындаған субъектінің кейін оны негізсіз жоққа шығаруына жол бермеуге бағытталған қасиет.

Негізгі терминдер

Термин	Анықтама
Ашық мәтін (plaintext)	Шифрлауға дейінгі бастапқы ақпарат
Шифрмәтін (ciphertext)	Шифрлау нәтижесінде алынған түрлендірілген ақпарат
Шифр (cipher)	Ақпаратты түрлендіру ережелері немесе алгоритмі
Кілт (key)	Криптографиялық түрлендіру нәтижесін анықтайтын параметр
Шифрлау	Ашық мәтінді шифрмәтінге түрлендіру
Дешифрлау	Шифрмәтінді бастапқы мәтінге қалпына келтіру

Криптографиялық байланыстың жалпы моделі

Алиса — хабарлама жіберуші

Боб — хабарламаны қабылдаушы

Ева — байланыс арнасын
бақылауға тырысатын қарсылас



Шифрдың формалды математикалық моделі

$$C = E_k(M)$$

$$M = D_k(C)$$

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

Дұрыс кілтпен шифрланған хабарлама бастапқы қалпына келуі тиіс.

M — мүмкін болатын ашық мәтіндер жиыны

C — мүмкін болатын шифрмәтіндер жиыны

K — мүмкін болатын кілттер жиыны

E — шифрлау түрлендірулерінің жиыны

D — дешифрлау түрлендірулерінің жиыны

Цезарь шифры: формула және мысал

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

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

Латын алфавитін нөмірлейміз: A=0, B=1, …, Z=25.

Кілт: k = 3.

CAT: C=2, A=0, T=19.

C→F, A→D, T→W.

CAT → FDW

Кілт және кілттер кеңістігі

Кілттер кеңістігі – мүмкін болатын барлық криптографиялық кілттердің жиыны.

$$|K| = 2^n$$

n — кілт ұзындығы (бит).

8 биттік кілт: $2^8 = 256$ мүмкіндік.

Кілт кеңістігі ұлғайған сайын толық перебор қиындайды.

Бірақ үлкен кілт кеңістігі алгоритмнің өзінде осалдық жоқ дегенді білдірмейді.

Керкгоффс принципі

Негізгі қағида – криптожүйенің қауіпсіздігі алгоритмнің жасырын болуына ғана тәуелді болмауы тиіс.

Қарсылас алгоритмнің қалай жұмыс істейтінін білуі мүмкін.

Құпия сақталатын негізгі элемент — кілт.

Ашық алгоритмдерді көптеген мамандар талдай алады.

Кілтті генерациялау, сақтау және тарату қауіпсіз ұйымдастырылуы қажет.

Криптография, кодтау және стеганография

Әдіс	Негізгі мақсат	Кілт міндетті ме?	Мысал
Криптография	Мазмұнды қорғау	Көп жағдайда иә	Мәтінді шифрлау
Кодтау	Басқа форматта ұсыну	Жоқ	Стандартты кодтық көрініс
Стеганография	Ақпараттың бар екенін жасыру	Міндетті емес	Хабарламаны тасымалдаушыда жасыру

Криптография тарихының негізгі кезеңдері

1. Ежелгі және классикалық кезең — қарапайым ауыстыру және орын алмастыру әдістері.
2. Орта ғасырлар — бірнеше алфавитті қолданатын тәсілдердің дамуы.
3. Механикалық және электромеханикалық кезең — роторлық машиналар.
4. Компьютерлік криптография — биттер мен блоктарға негізделген алгоритмдер.
5. Ашық кілтті криптография — ашық және жабық кілт жұбы.
6. Қазіргі кезең — интернет, мобильді байланыс, бұлттық жүйелер, электрондық қызметтер.

Классикалық және қазіргі криптография

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
Бағалау	Көбіне тәжірибелік	Математикалық және есептеу күрделілігі

Криптографиялық жүйеге қойылатын талаптар

Шифрлау және дешифрлау заңды пайдаланушы үшін дұрыс жұмыс істеуі тиіс.

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

Алгоритмнің құпиялығы қауіпсіздіктің жалғыз шарты болмауы тиіс.

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

Қорғаныс механизмі ақпараттың құндылығы мен қауіп моделіне сәйкес болуы тиіс.

Криптографияның қолданылу салалары

- ✓ Интернет арқылы берілетін деректерді қорғау.
- ✓ Электрондық пошта және хабар алмасу жүйелері.
- ✓ Банк операциялары және электрондық төлемдер.
- ✓ Файлдар мен деректер қорын шифрлау.
- ✓ Пайдаланушылар мен құрылғыларды аутентификациялау.
- ✓ Электрондық цифрлық қолтаңба және құжат айналымы.
- ✓ Бұлттық және мобильді ақпараттық жүйелер.

Толық мысал: HELLO хабарламасын шифрлау

M = {A, B, …, Z}

K = {0, 1, …, 25}

k = 3

H=7, E=4, L=11, L=11, O=14

3 қосамыз: 10, 7, 14, 14, 17

Әріптерге қайта ауыстырамыз: K, H, O, O, R

HELLO
↓
KHOOR

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

Қорытынды

Криптография — ақпараттық қауіпсіздіктің негізгі технологиялық бағыттарының бірі.

Негізгі элементтер: ашық мәтін, шифрмәтін, алгоритм, кілт, шифрлау және дешифрлау.

Криптожүйе M, C, K жиындары және E, D функциялары арқылы формалды сипатталады.

Криптография құпиялылықпен қатар тұтастық пен аутентификация міндеттерін де шешеді.

Бақылау сұрақтары

1. Криптография дегеніміз не?
2. Криптография мен криптоталдаудың айырмашылығы қандай?
3. Ашық мәтін, шифрмәтін және кілт ұғымдарын түсіндіріңіз.
4. M, C, K, E, D нені білдіреді?
5. $D_k(E_k(M)) = M$ шартының мағынасы қандай?
6. Керкгоффс принципінің негізгі идеясы қандай?
7. Криптография, кодтау және стеганография қалай ажыратылады?
8. Кілт ұзындығы n бит болса, кілттер саны қалай есептеледі?

Ұсынылатын әдебиеттер

Ахметов Б.С. және т.б. Қолданбалы криптология: шифрлау әдістері. Алматы: ҚазҰТЗУ, 2016.

Ахметов Б.С. және т.б. Криптография негіздері. Алматы: АЭжБУ, 2020.

Васильева И.Н. Криптографические методы защиты информации. Юрайт, 2024.

Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. Юрайт, 2024.

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

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