5-ДӘРІС
КОДТАУ. КОМПОЗИЦИЯЛЫҚ ШИФРЛАР

Дәрістің мақсаты

Кодтау ұғымын криптографиялық шифрлаудан ажырату, ақпаратты сандық және символдық түрде ұсынудың негізгі қағидаларын түсіндіру, бірнеше қарапайым түрлендіруді бір жүйеге біріктіретін композициялық шифрлардың құрылымын ашу, ауыстыру мен орын алмастыру операцияларының бірлескен қолданылуын мысалдар арқылы көрсету және композицияның криптографиялық беріктілікке әсерін түсіндіру.

Кодтау ұғымы

Кодтау – ақпаратты белгілі бір ережеге сәйкес бір ұсыну формасынан екінші формаға түрлендіру процесі. Кодтаудың негізгі мақсаты ақпаратты компьютерде көрсету, сақтау, беру немесе өңдеуге ыңғайлы форматқа келтіру болып табылады. Кодтау кезінде құпия кілттің болуы міндетті емес және түрлендіру ережесі белгілі болса, ақпаратты бастапқы түріне қайтару әдетте қиын есеп болып саналмайды.

Мысалы, мәтіндегі әріптерді олардың реттік нөмірлерімен көрсету кодтаудың қарапайым түрі. A=0, B=1, …, Z=25 сәйкестігін қолдансақ, DATA сөзі (3,0,19,0) тізбегіне айналады. Бұл жерде ақпарат жасырылған жоқ, тек басқа формада ұсынылды.

Кодтау мен шифрлаудың айырмашылығы

Белгі	**Кодтау**	**Шифрлау**
Негізгі мақсат	Ақпаратты басқа форматта ұсыну	Ақпараттың мазмұнын құпиялау
Құпия кілт	Міндетті емес	Көп жағдайда қажет
Кері түрлендіру	Ереже белгілі болса оңай	Дұрыс кілтке тәуелді
Қауіпсіздік мақсаты	Негізгі мақсат емес	Құпиялылықты қамтамасыз ету
Мысал	Символды санмен көрсету	Цезарь, Виженер, қазіргі шифрлар

Кодтау мен шифрлауды шатастыруға болмайды. Ақпарат түсініксіз символдарға айналғанының өзі оның криптографиялық қорғалғанын білдірмейді. Егер түрлендіру жалпыға белгілі және құпия параметр қолданылмаса, мұндай операция көбіне кодтау болып табылады.

Ақпаратты сандық кодтау

Криптографиялық алгоритмдер математикалық операциялармен жұмыс істейтіндіктен, символдар алдымен сандарға немесе биттік тізбектерге сәйкестендіріледі. Алфавит $A=\{a_0,a_1,\ldots,a_{m-1}\}$ болса, әр символға 0-ден $m-1$-ге дейінгі бүтін сан беріледі. Осыдан кейін модульдік арифметика, матрицалық көбейту немесе логикалық операциялар қолдануға болады.

$a_i \leftrightarrow i, \quad 0 \le i < m$

Компьютерлік жүйеде символдар байттармен кодталады. Криптографиялық алгоритм үшін маңыздысы – ақпараттың нақты мағынасынан тәуелсіз, оны бірмәнді биттік тізбек ретінде өңдеу мүмкіндігі.

Композициялық шифр ұғымы

Композициялық шифр – екі немесе одан да көп қарапайым криптографиялық түрлендірулерді белгілі ретпен біріктіретін шифр. Бір ғана қарапайым ауыстыру немесе орын алмастыру мәтіндегі статистикалық заңдылықтарды толық жоя алмайды. Ал бірнеше әртүрлі

түрлендіруді кезекпен қолдану ашық мәтін мен шифрмәтін арасындағы байланысты күрделендіреді.

$$C = E_n(E_{n-1}(\dots E_2(E_1(M))\dots))$$

Мұнда E_1, E_2, …, E_n – бірінен кейін бірі орындалатын криптографиялық түрлендірулер. Дешифрлау кері ретпен жүргізіледі:

$$M = D_1(D_2(\dots D_{n-1}(D_n(C))\dots))$$

Ауыстыру мен орын алмастыру композициясы

Композицияның қарапайым оқу үлгісінде бірінші кезеңде символдардың мәндері ауыстырылады, ал екінші кезеңде олардың позициялары өзгереді. Мысалы, ABCD мәтінін Цезарь тәсілімен k=1 жылжытсақ BCDE аламыз. Одан кейін 1↔3 және 2↔4 позицияларын ауыстыру ережесін қолдансақ DEBC нәтижесі шығады. Қарсы бағытта алдымен позициялар қалпына келтіріліп, содан кейін символдар бір позицияға кері жылжытылады.

Бұл шағын мысал композицияның идеясын көрсетеді: бірінші түрлендіру символ мәнін өзгертсе, екіншісі олардың мәтіндегі орналасуын өзгертеді. Нәтижесінде бастапқы мәтіннің құрылымын тікелей байқау қиындайды.

Каскадты шифрлау

Бірнеше шифрлау операциясын тізбектей қолдану каскадты түрлендіру деп қарастырылуы мүмкін. Егер әр кезеңде әртүрлі кілт қолданылса, жалпы түрлендіру бірнеше кілтке тәуелді болады. Бірақ бірнеше әлсіз алгоритмді жай ғана біріктіру автоматты түрде қауіпсіз жүйе жасамайды. Композицияның құрылымы, кілттердің тәуелсіздігі және түрлендірулердің өзара әсері талдануы тиіс.

Раундтық құрылымға кіріспе

Қазіргі блоктық шифрлардың көпшілігінде композиция бір рет емес, бірнеше раунд бойы қайталанады. Раунд – шифрдың ішіндегі бір типтік өңдеу кезеңі. Әр раундта ауыстыру, араластыру, орын алмастыру және раундтық кілтпен біріктіру тәрізді операциялар орындалуы мүмкін.

$X_i = R(X_{i-1}, K_i)$

Мұнда X_{i-1} – алдыңғы раундтың нәтижесі, K_i – i-раундтың кілті, R – раундтық түрлендіру. Соңғы X_r мәні шифрмәтінді қалыптастырады. Раундтар саны мен олардың құрылымы нақты алгоритмге байланысты.

Композиция және статистикалық байланыстар

Қарапайым моноалфавиттік ауыстыруда әріптердің жиілік қатынастары ішінара сақталады. Тек орын алмастыруда символдардың жиілігі мүлде өзгермейді. Осы екі операцияны бірнеше рет біріктіру символдардың мәні мен позициясы арасындағы тәуелділікті күрделендіреді. Бұл идея кейінгі дәрістерде шашырату және араластыру ұғымдарымен тереңдетіледі.

Толық оқу мысалы

Ашық мәтін M=CODE болсын. Бірінші кезең – Цезарь ауыстыруы, k=2: C→E, O→Q, D→F, E→G. Аралық нәтиже EQFG. Екінші кезең – символдарды кері ретпен орналастыру: GFQE. Демек, композициялық шифрлау нәтижесі C=GFQE.

Дешифрлау кезінде операциялар кері ретпен орындалады. GFQE тізбегін кері орналастырсақ EQFG аламыз. Одан кейін әр символды екі позицияға кері жылжытқанда CODE бастапқы мәтіні қалпына келеді.

Композициялық шифрлардың артықшылықтары мен шектеулері

Композициялық тәсілдің артықшылығы – әртүрлі қарапайым түрлендірулердің қасиеттерін біріктіру арқылы ашық мәтін құрылымын күрделірек өзгерту мүмкіндігі. Бұл қазіргі симметриялық криптографиядағы көпраундты құрылымдардың қалыптасуына негіз болған маңызды идея.

Шектеуі – композиция дұрыс жобаланбаса, қосымша кезеңдер күтілген қауіпсіздікті бермеуі мүмкін. Криптографиялық жүйенің беріктігі тек операциялар санына емес, олардың математикалық қасиеттеріне, кілт кеңістігіне, раундтық кілттерді қалыптастыруға және белгілі криптоталдау әдістеріне қарсы тұрақтылығына байланысты.

Қорытынды

Кодтау ақпаратты басқа формада ұсынуға арналған және өздігінен криптографиялық құпиялылықты қамтамасыз етпейді. Композициялық шифрлар бірнеше криптографиялық түрлендіруді бірізді қолдану арқылы ашық мәтін мен шифрмәтін арасындағы байланысты күрделендіреді. Ауыстыру мен орын алмастырудың үйлесуі, каскадты өңдеу және раундтық құрылым қазіргі криптографиялық алгоритмдердің негізгі идеяларын түсінуге негіз болады.

Бақылау сұрақтары

1. Кодтау дегеніміз не және оның негізгі мақсаты қандай?
2. Кодтау мен шифрлаудың негізгі айырмашылығы неде?
3. Символдарды сандық кодтау криптографияда не үшін қажет?
4. Композициялық шифр дегеніміз не?
5. Композициялық шифрлауда дешифрлау операциялары қандай ретпен орындалады?
6. Ауыстыру мен орын алмастыруды біріктіру қандай нәтиже береді?
7. Каскадты шифрлау дегеніміз не?
8. Раунд ұғымы нені білдіреді?
9. Бірнеше әлсіз түрлендіруді біріктіру неге автоматты түрде берік шифр жасамайды?
10. Композициялық шифрлар қазіргі блоктық шифрлармен қалай байланысты?

Әдебиеттер тізімі

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016. – 500 б.

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. Москва: Юрайт, 2024.

4. Омассон Ж.-Ф. О криптографии всерьез. Практическое введение в современное шифрование. Москва: ДМК Пресс, 2021.