3-ДӘРІС
АУЫСТЫРУ ШИФРЛАРЫНЫҢ МАТЕМАТИКАСЫ. АҒЫНДЫ, БЛОКТЫҚ, КӨПАЛФАВИТТІ ЖӘНЕ ДИСКІЛІ ШИФРЛАР

Дәрістің мақсаты

Ауыстыру шифрларының математикалық моделін түсіндіру; символдарды сандық түрде көрсету мен модульдік арифметиканың рөлін ашу; ағынды, блоктық, көпалфавитті және дискілі ауыстыру тәсілдерінің жұмыс істеу қағидаларын салыстыру; әр тәсілдің ерекшеліктерін, артықшылықтары мен шектеулерін мысалдар арқылы көрсету.

Ауыстыру шифрының математикалық негізі

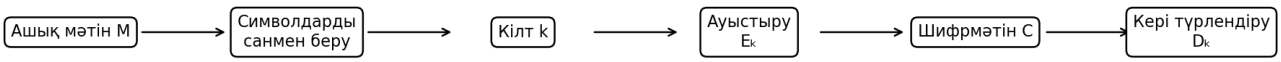
Ауыстыру шифры — ашық мәтіндегі әрбір символды белгілі бір ереже бойынша басқа символмен алмастыратын криптографиялық түрлендіру. Мұнда символдың мәтіндегі орны сақталады, ал оның мәні өзгереді. Сондықтан ауыстыруды математикалық тұрғыдан алфавит элементтерінің бір-біріне сәйкестендірілуі ретінде қарастыруға болады.

Алфавит $A=\{a_0,a_1,\ldots,a_{m-1}\}$ болсын. Әр символға 0-ден $m-1$-ге дейінгі сан сәйкестендіріледі. Сонда шифрлау функциясы E_k: $A\to A$ түрінде беріледі, ал дешифрлау үшін оған кері D_k функциясы қолданылады. Дұрыс дешифрлау үшін $D_k(E_k(x))=x$ шарты орындалуы тиіс. Демек, қарапайым ауыстыру бірмәнді және кері қайтарылатын бейнелеу болуы қажет.

Мысал. Латын алфавиті үшін A=0, B=1, …, Z=25 деп аламыз. Цезарь ауыстыруында $E_k(x)=(x+k) \bmod 26$, ал $D_k(y)=(y-k) \bmod 26$. k=3 болса A→D, B→E, C→F. Бұл мысалда модульдік арифметика алфавит соңына жеткенде қайта басына оралуға мүмкіндік береді.

Қарапайым ауыстыруда кілт міндетті түрде бір ғана сан емес. Ол бастапқы алфавиттің толық перестановкасы болуы мүмкін. 26 әріптік алфавит үшін теориялық ауыстырулар саны 26! болады. Бірақ үлкен кілт кеңістігі классикалық моноалфавиттік шифрды автоматты түрде берік етпейді, себебі бір символ әрдайым бір шифрсимволға ауысса, мәтіннің статистикалық құрылымы ішінара сақталады.

Ауыстыру шифрының жалпы схемасы



Сурет 1. Ауыстыру шифрының математикалық түрлендіру схемасы

Моноалфавиттік және көпалфавитті ауыстыру

Моноалфавиттік ауыстыруда бүкіл хабарлама бойында бір тұрақты сәйкестік қолданылады. Егер ашық мәтіндегі A әрпі D-ға ауыстырылса, ол хабарламаның барлық позицияларында сол D-ға айналады. Бұл қасиет шифрлауды қарапайым етеді, бірақ табиғи тілдегі әріп жиіліктерінің заңдылықтарын толық жоймайды.

Көпалфавитті немесе полиалфавиттік шифрда бірнеше ауыстыру алфавиті кезектесіп қолданылады. Сондықтан бір ашық символ мәтіндегі позициясына немесе кілт символына қарай әртүрлі шифрсимволға айналуы мүмкін. Жалпы модельді $C_i=(M_i+K_i) \bmod m$ түрінде көрсетуге болады.

Мысал. A=0,…,Z=25. Ашық мәтін CAT → (2,0,19), кілт KEY → (10,4,24). Сонда C=(12,4,17), яғни MER. Егер мәтінде бір әріп бірнеше рет кездессе, оған сәйкес кілт символдары әртүрлі болған жағдайда шифрмәтінде де әртүрлі символдар алынуы мүмкін.

Көпалфавитті тәсілдің негізгі ерекшелігі — жиілік құрылымын бір алфавитке қарағанда жақсырақ жасыруы. Бірақ кілт қысқа болып, мәтін бойында периодты қайталанса, осы период криптоталдау үшін қосымша заңдылық қалыптастыруы мүмкін. Сондықтан кілттің ұзындығы мен қолданылу тәртібі маңызды.

Белгі	Моноалфавиттік	Көпалфавитті
Ауыстыру алфавиті	Бір тұрақты	Бірнеше алфавит
Бір ашық символ	Әдетте бір шифрсимвол	Позицияға қарай әртүрлі болуы мүмкін
Статистикалық із	Көбірек сақталады	Жиілік таралуы жақсырақ жасырылады
Классикалық мысал	Цезарь, қарапайым ауыстыру	Виженер
Негізгі шектеу	Жиіліктік талдауға әлсіз	Қайталанатын кілт периодтылық туғызуы мүмкін

Ағынды шифрлар

Ағынды шифр — деректерді бит, байт немесе шағын символдар ағыны түрінде біртіндеп өңдейтін шифрлау тәсілі. Қазіргі ағындық модельде құпия кілт пен бастапқы параметр негізінде кілттік ағын $K_1,K_2,\ldots$ қалыптастырылып, ол ашық мәтін ағынымен біріктіріледі. Екілік деректер үшін ең қарапайым операция — XOR: $C_i=M_i \oplus K_i$. Дешифрлау да $M_i=C_i \oplus K_i$ формуласы арқылы орындалады.

XOR операциясының бұл қасиеті $(a \oplus b) \oplus b=a$ теңдігіне негізделеді. Мысалы, M=1011 және K=1100 болса, C=0111. Қабылдаушы сол K ағынын қолданып $0111 \oplus 1100=1011$ бастапқы мәтінін алады.

Ағынды шифрдың ерекшелігі — хабарламаның толық блогын күтпей, деректер келген сайын өңдеуге болатындығы. Сондықтан ол үздіксіз байланыс ағындарына қолайлы. Бірақ кілттік ағынды қалыптастыру мен синхрондау өте маңызды. Бірдей кілттік ағынды әртүрлі хабарламаларға орынсыз қайта қолдану олардың арасындағы математикалық байланысты ашып қоюы мүмкін.

Ағындық тәсілдерді синхронды және өзін-өзі синхрондайтын модельдерге бөлуге болады. Синхронды модельде кілттік ағын ашық мәтін мен шифрмәтінге тәуелсіз генерацияланады, сондықтан жіберуші мен қабылдаушы генераторларының күйі сәйкес болуы керек. Өзін-өзі синхрондайтын модельде келесі кілттік элементтер алдыңғы шифрмәтін элементтерінің белгілі бөлігіне тәуелді болуы мүмкін.

Мысал. Дауыс немесе телеметрия ағыны үздіксіз келіп тұрса, әрбір шағын порцияны келген бойда өңдеу қажет болуы мүмкін. Мұндай сценарийде ағындық тәсілдің кідірісі төмен. Бірақ нақты жүйеде құпиялылықпен қатар хабарламаның тұтастығы мен түпнұсқалығын қамтамасыз ететін механизм де қажет.

Блоктық шифрлар

Блоктық шифр — ашық мәтінді белгіленген ұзындықтағы блоктарға бөліп, әр блокты құпия кілтке тәуелді қайтымды түрлендіру арқылы шифрлайтын алгоритм. n биттік блок үшін $E_k: \{0,1\}^n \rightarrow \{0,1\}^n$. Белгілі бір k кілті үшін E_k барлық n-биттік блоктар жиынында перестановка болуы тиіс, өйткені әр шифрблокқа бір ғана бастапқы блок сәйкес келуі керек.

Мысал. Оқу моделінде блок ұзындығы 8 бит болсын. 24 биттік хабарлама B_1, B_2, B_3 үш блокқа бөлінеді. Әр блок E_k функциясы арқылы түрлендіріледі. Нақты алгоритмдерде блок өлшемі үлкен және түрлендіру бірнеше раундтан тұрады.

Блоктық шифрдың ішкі құрылымында ауыстыру идеясы маңызды орын алады. Қазіргі шифрларда S-box деп аталатын ауыстыру кестелері шағын биттік топтарды басқа биттік мәндерге бейнелейді. Бірақ қауіпсіз блоктық алгоритм тек бір ауыстырудан тұрмайды: бірнеше раундта ауыстыру, орын алмастыру немесе сызықтық араластыру және раундтық кілтпен біріктіру орындалады.

Блоктық шифрды ұзын хабарламаға қолдану үшін жұмыс режимі қажет. Себебі алгоритмнің негізгі функциясы тек бір бекітілген блокты түрлендіреді. Жұмыс режимі бірнеше блоктың қалай байланысатынын, бастапқы вектор немесе nonce қалай қолданылатынын анықтайды. Бірдей ашық блоктардың бірдей шифрблокқа айналуын болдырмау үшін режимді дұрыс таңдау маңызды.

Блоктық шифрлардың *артықшылығы* — үлкен көлемдегі деректерді тиімді өңдеу және қазіргі аппараттық/бағдарламалық платформаларда жоғары өнімділік.

Шектеуі — блоктарға бөлу, режимді, бастапқы параметрлерді және тұтастықты қорғауды дұрыс ұйымдастыру қажеттілігі.

Белгі	**Ағынды шифр**	**Блоктық шифр**
Өңдеу бірлігі	Бит/байт немесе шағын ағын	Белгіленген өлшемді блок
Негізгі математикалық идея	Кілттік ағынмен біріктіру	Кілтке тәуелді блоктық перестановка
Кідіріс	Әдетте төмен	Блоктың қалыптасуына тәуелді
Маңызды шарт	Кілттік ағынды дұрыс генерациялау және қайталамау	Жұмыс режимі мен бастапқы параметрлерді дұрыс қолдану
Қолдану сипаты	Үздіксіз ағындар	Файлдар, сақтау, хаттамалар

Дискілі шифрлар

Дискілі шифр — ауыстыру алфавиттерін механикалық түрде таңдауға мүмкіндік беретін шифрлау тәсілі. Классикалық шифрлау дискісі әдетте бір оське бекітілген екі немесе бірнеше айналмалы шеңберден тұрады. Сыртқы және ішкі сақиналарда алфавит символдары орналасады. Дискілердің өзара қалпы ашық символ мен шифрсимвол арасындағы сәйкестікті анықтайды.

Дискілі шифрдың математикалық мағынасы — бір немесе бірнеше ауыстыру перестановкасын механикалық түрде жүзеге асыру. Егер ішкі диск сыртқы дискіге қатысты k позицияға жылжытылса, қарапайым жағдайда бұл $E_k(x)=(x+k) \bmod m$ тәрізді циклдік ауыстыруға сәйкес келеді. Егер дискідегі символдардың реті стандартты емес болса, жалпы еркін перестановка алынады.

Дискінің қалпы шифрлау барысында өзгермесе, жүйе моноалфавиттік ауыстыруға ұқсайды. Ал диск белгілі ереже бойынша бұрылып отырса, әр позицияда басқа сәйкестік пайда болып, тәсіл көпалфавитті сипат алады. Осы себепті шифрлау дискілері бірнеше алфавитті ауыстыру идеясын көрнекі түрде түсіндіруге ыңғайлы.

Мысал. Екі дискіде 26 әріп бар делік. Алғашқы қалыпта ішкі диск үш позицияға жылжытылса, A сыртқы символына D ішкі символы сәйкес келеді. Бірнеше символдан кейін диск тағы бір позицияға бұрылса, келесі A енді бұрынғы D-ға емес, басқа символға сәйкесуі мүмкін. Яғни бірдей ашық әріптің шифрмәтіндегі бейнесі диск күйіне тәуелді.

Дискілі шифрдың ерекшелігі — кілтті тек символдық жол ретінде емес, дискілердің бастапқы орналасуы, алфавит реті және айналдыру ережесі ретінде көрсетуге болатындығы. Артықшылығы — көпалфавитті ауыстыруды қолмен орындауды жеңілдетуі. Кемшілігі — механикалық ережелердің периодтылығы және қазіргі есептеу мүмкіндіктері жағдайында классикалық дискілі жүйелердің дербес қорғаныс құралы ретінде жеткіліксіздігі.

Төрт тәсілдің өзара байланысы

Тәсіл	**Не өзгереді?**	**Кілттің рөлі**	**Негізгі ерекшелік**	**Оқу мысалы**
Қарапайым ауыстыру	Символ мәні	Бір сәйкестік таңдайды	Бір алфавит	Цезарь
Көпалфавитті	Символ мәні	Позицияға тәуелді ауыстыруды таңдайды	Бірнеше алфавит	Виженер
Ағынды	Бит/байт мәні	Кілттік ағын генерациясына негіз болады	Дерек біртіндеп өңделеді	XOR моделі

Блоктық	Бүкіл блок	Блоктық перестановканы анықтайды	Белгіленген блоктар	n-биттік E_k
Дискілі	Символ мәні	Диск қалпы/айналу ережесін анықтайды	Механикалық көпалфавиттілік	Шифрлау дискісі

Кешенді мысал

Бір ғана DATA сөзін әртүрлі тәсілмен қарастырайық. Қарапайым Цезарь ауыстыруында k=3 болса әр символ бірдей ығысумен түрленеді. Көпалфавитті тәсілде әр позиция үшін кілттің басқа символы қолданылып, бірдей ашық әріптер әртүрлі нәтиже беруі мүмкін. Дискілі тәсілде дәл осы өзгеріс дисктің қалпын ауыстыру арқылы механикалық орындалады. Ағындық тәсілде мәтін символдар немесе биттер тізбегі ретінде қарастырылып, кілттік ағынмен біріктіріледі. Блоктық тәсілде DATA кодталғаннан кейін белгіленген өлшемдегі блоктың бөлігі ретінде тұтас түрлендіріледі.

Бұл салыстыру «ағынды», «блоктық» және «көпалфавитті» ұғымдарының бір жіктеу осінде тұрмайтынын көрсетеді. Ағынды және блоктық — деректерді өңдеу тәсілі бойынша жіктеу; моноалфавиттік және көпалфавитті — қолданылатын ауыстыру алфавиттерінің саны бойынша жіктеу. Дискілі шифр болса ауыстыруды механикалық жүзеге асыру тәсілі. Сондықтан бір криптографиялық жүйеде бірнеше жіктеу белгісі қатар сипатталуы мүмкін.

Қорытынды

Ауыстыру шифрларының математикалық негізі — алфавит немесе биттер жиынындағы қайтымды сәйкестік. Модульдік арифметика циклдік ауыстыруларды формалдауға, ал перестановка ұғымы жалпы ауыстыруды сипаттауға мүмкіндік береді. Көпалфавитті шифрлар бірнеше сәйкестікті кезектестіреді; ағынды шифрлар деректерді біртіндеп кілттік ағынмен өңдейді; блоктық шифрлар бекітілген өлшемдегі блоктарға кілтке тәуелді қайтымды түрлендіру қолданады; дискілі шифрлар ауыстыру алфавиттерін механикалық түрде іске асырады. Бұл ұғымдарды ажырату кейінгі гаммалау, құрамдас шифрлар және қазіргі симметриялық криптография тақырыптарын түсіну үшін негіз болады.

Бақылау сұрақтары

1. Ауыстыру шифры математикалық тұрғыдан қалай анықталады?
2. Неліктен ауыстыру функциясы қайтымды болуы керек?
3. Модульдік арифметика Цезарь шифрында қандай рөл атқарады?
4. Моноалфавиттік және көпалфавитті шифрлардың айырмашылығы қандай?
5. Ағынды шифрдың негізгі математикалық моделі қандай?
6. XOR операциясы дешифрлауға неге мүмкіндік береді?
7. Блоктық шифрдың $E_k: \{0,1\}^n \to \{0,1\}^n$ моделі нені білдіреді?
8. Блоктық және ағынды шифрлар қалай ажыратылады?
9. Дискілі шифрдың математикалық мағынасы неде?
10. Дискілі шифр қандай жағдайда көпалфавитті сипат алады?