4-ДӘРІС
ГАММАЛАУ ШИФРЛАРЫНЫҢ МАТЕМАТИКАСЫ

Дәрістің мақсаты

Гаммалау арқылы шифрлаудың математикалық негіздерін түсіндіру, гамма және кілттік ағын ұғымдарының мағынасын ашу, модуль бойынша қосу мен XOR операциясының шифрлау және дешифрлау үдерісіндегі рөлін көрсету, бір реттік блокноттың теориялық қасиеттерін түсіндіру, гамманы генерациялау мен синхрондаудың маңызын талдау және гаммалау тәсілдерінің артықшылықтары мен шектеулерін нақты мысалдар арқылы көрсету.

Гаммалау шифрының негізгі идеясы

Гаммалау шифры – ашық мәтіннің символдарын немесе биттерін арнайы қалыптастырылған кілттік тізбекпен, яғни гаммамен біріктіру арқылы шифрлау тәсілі. Гамма хабарламаның әрбір элементіне сәйкес келетін кілттік элементтер тізбегінен тұрады. Ашық мәтін мен гамма белгілі математикалық операция арқылы біріктірілгенде шифрмәтін алынады. Қабылдаушы дәл сол гамманы немесе оны қалыптастыруға мүмкіндік беретін құпия кілтті пайдаланып, кері операция арқылы бастапқы мәтінді қалпына келтіреді.

Гаммалаудың маңызды ерекшелігі – шифрлау нәтижесі тек ашық мәтінге ғана емес, мәтіннің әр позициясында қолданылатын гамма элементіне де тәуелді. Сондықтан бірдей символдар әртүрлі позицияларда әртүрлі гамма элементтерімен біріктірілсе, олардың шифрмәтіндегі бейнесі де әртүрлі болуы мүмкін. Бұл қасиет қарапайым моноалфавиттік ауыстыруға тән тұрақты жиілік іздерін әлсіретеді.

Гамма және кілттік ағын

Гамма – ашық мәтінді шифрлау үшін пайдаланылатын сандық немесе екілік тізбек. Қазіргі терминологияда оған жақын ұғым ретінде кілттік ағын (keystream) қолданылады. Кілттік ағын құпия кілттің, ал кейбір жүйелерде қосымша бастапқы параметрдің негізінде генерацияланады. Егер ашық мәтін $M_1, M_2, \ldots, M_n$ элементтерінен, ал гамма $G_1, G_2, \ldots, G_n$ элементтерінен тұрса, әрбір M_i элементі сәйкес G_i элементімен біріктіріледі.

$$M = (M_1, M_2, \ldots, M_n), \quad G = (G_1, G_2, \ldots, G_n)$$

Гамманың ұзындығы хабарламаның ұзындығына тең болуы немесе қысқа бастапқы кілттен арнайы генератор арқылы қажетті ұзындыққа дейін қалыптастырылуы мүмкін. Қауіпсіздік тұрғысынан гамма элементтерінің болжануы қиын болуы және оларды орынсыз қайталап қолданбау маңызды.

Модуль бойынша қосуға негізделген гаммалау

Егер хабарлама символдары сандық түрде берілсе, гаммалау модуль бойынша қосу операциясына негізделуі мүмкін. Алфавитте m символ бар болсын. Ашық мәтіннің i-позициясындағы символ M_i, ал гамманың сәйкес элементі G_i болса, шифрлау формуласы төмендегідей жазылады:

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

Дешифрлау кезінде гамма шифрмәтіннен модуль бойынша алынады:

$$M_i = (C_i - G_i) \bmod m$$

Мұндағы mod m операциясы нәтиженің әрқашан 0 мен $m-1$ аралығында қалуын қамтамасыз етеді. Егер есептеу нәтижесі теріс болса, оған m саны қосылып, алфавиттің рұқсат етілген диапазонына келтіріледі.

Мысал: әріптік гаммалау

Латын алфавитін A=0, B=1, …, Z=25 деп нөмірлейік. Ашық мәтін CAT болсын: C=2, A=0, T=19. Гамма KEY болсын: K=10, E=4, Y=24. m=26 жағдайында әр позиция бойынша есептейміз.

$C_1 = (2 + 10) \bmod 26 = 12 \rightarrow M$

$C_2 = (0 + 4) \bmod 26 = 4 \rightarrow E$

$C_3 = (19 + 24) \bmod 26 = 17 \rightarrow R$

Нәтижесінде CAT ашық мәтіні MER шифрмәтініне айналады. Дешифрлау кезінде MER символдарының сандық мәндерінен KEY гаммасының сәйкес мәндері алынады. Мысалы, бірінші символ үшін $(12-10) \bmod 26 = 2$, яғни C алынады. Осылайша бастапқы CAT мәтіні толық қалпына келеді.

Екілік гаммалау және XOR операциясы

Компьютерлік жүйелерде ақпарат екілік түрде ұсынылатындықтан, гаммалаудың кең таралған математикалық операциясы XOR, яғни модуль 2 бойынша қосу болып табылады. XOR операциясында екі бит бірдей болса нәтиже 0, ал әртүрлі болса нәтиже 1 болады.

M	**G**	**M ⊕ G**
0	0	0
0	1	1
1	0	1
1	1	0

XOR операциясының гаммалау үшін өте ыңғайлы болуының себебі – оның өзіне-өзі кері қасиеті:

$$(a \oplus b) \oplus b = a$$

Сондықтан екілік гаммалау кезінде шифрлау мен дешифрлау бір операциямен орындалады:

$$C_i = M_i \oplus G_i$$

$$M_i = C_i \oplus G_i$$

Екілік мысал

Ашық мәтіннің шағын фрагменті M=10110110, ал гамма G=01101101 болсын. Әр позиция бойынша XOR орындаймыз:

M = 10110110

G = 01101101

C = 11011011

Қабылдаушы C=11011011 шифрмәтінін дәл сол G=01101101 гаммасымен XOR операциясы арқылы біріктіреді. Нәтижесінде 10110110 бастапқы тізбегі алынады. Демек, гамманы дұрыс қалпына келтіру немесе синхронды түрде генерациялау дешифрлаудың негізгі шарты болып табылады.

Бір реттік блокнот

Гаммалаудың теориялық тұрғыдан маңызды үлгісі – бір реттік блокнот (one-time pad). Бұл тәсілде гамма шын мәнінде кездейсоқ болуы, хабарлама ұзындығына тең болуы, құпия сақталуы және тек бір рет қолданылуы тиіс. Осы шарттар орындалғанда шифрмәтіннің өзі ашық мәтін туралы жеткілікті ақпарат бермейді.

Бір реттік блокноттың математикалық моделі екілік жағдайда өте қарапайым: $C=M \oplus G$. Бірақ оның практикалық күрделілігі алгоритмде емес, гамманы қауіпсіз генерациялау, сақтау және екі тарапқа жеткізу мәселесінде. Ұзын хабарлама үшін дәл сондай ұзын құпия гамма қажет болады. Сондықтан бұл тәсіл теориялық эталон ретінде маңызды болғанымен, күнделікті ақпараттық жүйелерде кілтті басқару жағынан қолайсыз болуы мүмкін.

Неліктен гамманы қайталап қолдануға болмайды?

Бір гамманы бірнеше тәуелсіз хабарламаға қолдану олардың арасында математикалық байланыс қалыптастырады. Егер $C_1=M_1 \oplus G$ және $C_2=M_2 \oplus G$ болса, екі шифрмәтінді XOR арқылы біріктіргенде гамма жойылады:

$$C_1 \oplus C_2 = (M_1 \oplus G) \oplus (M_2 \oplus G) = M_1 \oplus M_2$$

Бұл теңдік бірдей кілттік ағынды қайта қолданудың қауіпті екенін көрсетеді. Сондықтан нақты жүйелерде кілттік ағынның бірегейлігін қамтамасыз ететін кілттерді, nonce немесе бастапқы вектор тәрізді параметрлерді дұрыс қолдану маңызды. Мұнда негізгі қағида – бірдей гамма фрагментінің әртүрлі хабарламалар үшін қайталануына жол бермеу.

Псевдокездейсоқ гамма

Ұзындығы хабарламаға тең шын кездейсоқ гамманы сақтау әрқашан ыңғайлы емес. Сондықтан практикалық жүйелерде қысқа құпия кілттен ұзын кілттік ағын қалыптастыратын криптографиялық генераторлар қолданылады. Мұндай тізбек детерминделген түрде есептелуі мүмкін, бірақ кілтті білмейтін бақылаушы үшін оның келесі элементтерін болжау практикалық тұрғыдан қиын болуы тиіс.

Псевдокездейсоқ гамма генераторының негізгі талаптарына жеткілікті ұзын период, статистикалық заңдылықтардың айқын болмауы, кілтке жоғары тәуелділік және келесі элементтерді болжаудың қиындығы жатады. Тек сыртқы көрінісі кездейсоқ болатын қарапайым генератор криптографиялық мақсат үшін автоматты түрде жарамды болып саналмайды.

Синхронды гаммалау

Синхронды гаммалауда жіберуші мен қабылдаушы кілттік ағынды бірдей бастапқы параметрлерден тәуелсіз түрде генерациялайды. Шифрмәтіннің і-элементін дұрыс ашу үшін қабылдаушының генераторы дәл сол і-позициядағы G_i гамма элементін шығаруы керек. Сондықтан екі жақтың күйі синхронды болуы маңызды.

Мысалы, байланыс кезінде бір элемент жоғалып кетсе және жүйеде синхрондауды қалпына келтіру механизмі болмаса, одан кейінгі гамма позициялары сәйкес келмеуі мүмкін. Осы себепті нақты хаттамалар кілтпен қатар бастапқы параметрлерді, есептегіштерді немесе nonce мәндерін келісілген тәртіппен қолданады.

Өзін-өзі синхрондайтын гаммалау

Өзін-өзі синхрондайтын модельде келесі гамма элементтері алдыңғы шифрмәтін элементтерінің белгілі бір бөлігіне тәуелді қалыптасуы мүмкін. Мұндай тәсілде қабылдаушы белгілі көлемдегі шифрмәтінді алғаннан кейін генератор күйін қайта қалпына келтіре алады. Бірақ бір шифрмәтін элементіндегі қате келесі бірнеше элементтің дешифрлануына әсер етуі ықтимал.

Синхронды және өзін-өзі синхрондайтын тәсілдердің айырмашылығы гамманы қалыптастыру механизмінде жатыр. Біріншісінде кілттік ағын хабарлама ағынынан тәуелсіз генерацияланады, екіншісінде алдыңғы шифрмәтін күйдің бір бөлігі ретінде қолданылуы мүмкін.

Гаммалау мен Виженер шифрының байланысы

Виженер шифрын символдық алфавитте орындалатын периодты гаммалаудың классикалық үлгісі ретінде қарастыруға болады. Кілт сөзінің символдары сандық гаммаға айналып, мәтін бойында қайталанады. Шифрлау $C_i=(M_i+K_i) \bmod m$ формуласы бойынша орындалады. Егер кілт қысқа болса, гамма белгілі периодпен қайталанады. Сондықтан Виженер қарапайым

моноалфавиттік шифрға қарағанда жиілік құрылымын жақсырақ жасырғанымен, қайталанатын кілт ұзындығы қосымша заңдылық туғызады.

Қазіргі гаммалау тәсілдерінің айырмашылығы – кілттік ағынды қарапайым қайталанатын сөзден емес, криптографиялық генератордан қалыптастыруға ұмтылуында. Бұл кілттік ағынның ұзақ периодты және болжануы қиын болуына мүмкіндік береді.

Гаммалау мен блоктық шифрдың айырмашылығы

Белгі	**Гаммалау/ағындық тәсіл**	**Блоктық тәсіл**
Өңдеу бірлігі	Бит, байт немесе шағын элемент	Белгіленген өлшемді блок
Негізгі операция	Кілттік ағынмен біріктіру	Кілтке тәуелді блоктық түрлендіру
Кідіріс	Әдетте төмен	Блоктың қалыптасуына тәуелді
Маңызды параметр	Гамманың бірегейлігі және синхрондау	Жұмыс режимі, IV/nonce және кілт
Қолдану сипаты	Үздіксіз деректер ағыны	Файлдар, сақтау және желілік деректер

Гаммалаудың артықшылықтары мен шектеулері

Гаммалаудың негізгі артықшылығы – математикалық операциялардың қарапайымдылығы және деректерді келген бойда өңдеу мүмкіндігі. XOR операциясы аппараттық және бағдарламалық деңгейде өте жылдам орындалады. Сонымен қатар дұрыс қалыптастырылған кілттік ағын бірдей ашық символдардың әр позицияда әртүрлі шифрлануына мүмкіндік береді.

Негізгі шектеулер гамманы басқарумен байланысты. Кілттік ағынның қайталануы, болжанатын генератор, кілттің немесе бастапқы параметрдің дұрыс қорғалмауы жүйенің қауіпсіздігін төмендетеді. Сондай-ақ гаммалау өздігінен хабарламаның тұтастығы мен түпнұсқалығын міндетті түрде қамтамасыз етпейді. Сондықтан қазіргі жүйелерде құпиялылықпен қатар аутентификацияланған тұтастықты қамтамасыз ететін механизмдер де қолданылады.

Толық есептік мысал

A=0, B=1, …, Z=25 алфавитін қолданайық. Ашық мәтін DATA, ал гамма CODE болсын. Сандық түрде DATA=(3,0,19,0), CODE=(2,14,3,4). Шифрлау $C_i=(M_i+G_i) \bmod 26$ бойынша:

D: $(3 + 2) \bmod 26 = 5 \rightarrow$ F

A: $(0 + 14) \bmod 26 = 14 \rightarrow$ O

T: $(19 + 3) \bmod 26 = 22 \rightarrow$ W

A: $(0 + 4) \bmod 26 = 4 \rightarrow$ E

Сондықтан DATA → FOWE. Дешифрлау кезінде кері есептеу орындалады: $(5-2) \bmod 26=3 \rightarrow$ D; $(14-14) \bmod 26=0 \rightarrow$ A; $(22-3) \bmod 26=19 \rightarrow$ T; $(4-4) \bmod 26=0 \rightarrow$ A. Бастапқы DATA мәтіні қалпына келеді. Бұл мысал гаммалаудың модульдік арифметикаға негізделген жалпы логикасын көрсетеді.

Қорытынды

Гаммалау шифрлары ашық мәтін элементтерін кілттік тізбекпен біріктіру қағидасына негізделеді. Символдық алфавитте бұл модуль бойынша қосу, ал екілік деректерде көбіне XOR операциясы арқылы іске асырылады. Гаммалау тиімді болуы үшін кілттік ағын болжануы қиын, дұрыс синхрондалған және әртүрлі хабарламаларда орынсыз қайталанбайтын болуы тиіс. Бір реттік блокнот гаммалаудың теориялық тұрғыдан ең маңызды үлгісі болып табылады, ал практикалық жүйелерде ұзын кілттік ағын криптографиялық генератор арқылы

қалыптастырылады. Гаммалау құпиялылықты қамтамасыз етуге бағытталғанымен, нақты ақпараттық жүйеде тұтастық пен аутентификация мәселелері де бөлек ескерілуі қажет.

Бақылау сұрақтары

1. Гаммалау шифры дегеніміз не және оның негізгі идеясы қандай?
2. Гамма мен кілттік ағын ұғымдарының мағынасы қандай?
3. Модуль бойынша қосуға негізделген гаммалау қалай орындалады?
4. XOR операциясы неге екілік гаммалауға ыңғайлы?
5. Бір реттік блокноттың негізгі шарттары қандай?
6. Бір гамманы бірнеше хабарламаға қайта қолдану неге қауіпті?
7. Псевдокездейсоқ гамма генераторына қандай талаптар қойылады?
8. Синхронды және өзін-өзі синхрондайтын гаммалаудың айырмашылығы неде?
9. Виженер шифрын гаммалау тәсілімен қалай байланыстыруға болады?
10. Гаммалау хабарламаның тұтастығы мен аутентификациясын өздігінен қамтамасыз ете ме?

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. Оқу құралы. 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.