4-ДӘРІС

ГАММАЛАУ ШИФРЛАРЫНЫҢ МАТЕМАТИКАСЫ

Криптографиялық қорғаудың ағындық тәсілдері

Модуль бойынша қосу және XOR операциясы

Бір реттік блокнот, гамманы генерациялау және синхрондау

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Гаммалау арқылы шифрлаудың математикалық негіздерін түсіндіру.

Гамма және кілттік ағын ұғымдарының мағынасын ашу.

Модуль бойынша қосу мен XOR операциясының шифрлау және дешифрлаудағы рөлін көрсету.

Бір реттік блокноттың теориялық қасиеттерін түсіндіру.

Гамманы генерациялау мен синхрондаудың маңызын және тәсілдің артықшылықтары мен шектеулерін талдау.

Гаммалау шифрының негізгі идеясы



Әрбір мәтін элементі өз позициясындағы гамма элементімен біріктіріледі.

Бірдей символдар әр позицияда әртүрлі шифрлануы мүмкін.

Гамма және кілттік ағын

Гамма — ашық мәтінді шифрлау үшін қолданылатын сандық немесе екілік тізбек.

Кілттік ағын (keystream) құпия кілттен және кейбір жүйелерде бастапқы параметрден генерацияланады.

Гамма хабарлама ұзындығына тең болуы немесе қысқа кілттен генератор арқылы қалыптастырылуы мүмкін.

$$M = (M_1, M_2, \ldots, M_n)$$

$$G = (G_1, G_2, \ldots, G_n)$$

Қауіпсіздік шарты: гамма болжануы қиын және орынсыз қайталанбауы тиіс.

Модуль бойынша қосуға негізделген гаммалау

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

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

m — алфавиттегі символдар саны.

mod m нәтижені 0 мен m−1 аралығында ұстайды.

Теріс нәтиже шықса, оған m саны қосылып рұқсат етілген диапазонға келтіріледі.

Мысал: әріптік гаммалау

A=0, B=1, …, Z=25; ашық мәтін CAT, гамма KEY, m=26.

Позиция	M_i	G_i	Есептеу	C_i
1	C = 2	K = 10	(2+10) mod 26 = 12	M
2	A = 0	E = 4	(0+4) mod 26 = 4	E
3	T = 19	Y = 24	(19+24) mod 26 = 17	R
Нәтиже	CAT	KEY		MER

CAT → MER

Екілік гаммалау және XOR операциясы

XOR — модуль 2 бойынша қосу. Биттер бірдей болса 0, әртүрлі болса 1.

XOR операциясының өзіне-өзі кері қасиеті шифрлау мен дешифрлауды бір операциямен орындауға мүмкіндік береді.

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

$$C_i = M_i \oplus G_i$$

$$M_i = C_i \oplus G_i$$

M	G	M ⊕ G
0	0	0
0	1	1
1	0	1
1	1	0

Екілік мысал

$$M = 10110110$$

$$G = 01101101$$

$$C = M \oplus G = 11011011$$

$$C \oplus G = 10110110 = M$$

Дешифрлау үшін қабылдаушы дәл сол гамманы дұрыс позицияда қолдануы тиіс.

Бір реттік блокнот (One-Time Pad)

Гамма шын мәнінде кездейсоқ болуы тиіс.

Гамма ұзындығы хабарлама ұзындығына тең болуы тиіс.

Гамма құпия сақталып, тек бір рет қолданылуы тиіс.

Екілік модель: $C = M \oplus G$.

Практикалық қиындық: ұзын гамманы қауіпсіз генерациялау, сақтау және екі тарапқа жеткізу.

Неліктен гамманы қайталап қолдануға болмайды?

$$C_1 = M_1 \oplus G$$

$$C_2 = M_2 \oplus G$$

$$C_1 \oplus C_2 = M_1 \oplus M_2$$

Екі шифрмәтінді XOR арқылы біріктіргенде бірдей гамма жойылады.

Сондықтан әртүрлі хабарламаларда бірдей кілттік ағын фрагментін қайталауға болмайды.

Нақты жүйелерде кілттер, nonce немесе бастапқы вектор тәрізді параметрлердің бірегейлігі маңызды.

Псевдокездейсоқ гамма және синхрондау

Криптографиялық генератор қысқа құпия кілттен ұзын кілттік ағын қалыптастырады.

Негізгі талаптар: ұзын период, айқын статистикалық заңдылықтардың болмауы, кілтке жоғары тәуелділік, келесі элементті болжаудың қиындығы.

Синхронды гаммалауда екі тарап бірдей бастапқы параметрлерден бірдей G_i тізбегін генерациялайды.

Элемент жоғалса немесе позициялар ығысса, синхрондау бұзылуы мүмкін.

Өзін-өзі синхрондайтын гаммалау және Виженер шифры

Өзін-өзі синхрондайтын модельде келесі гамма элементтері алдыңғы шифрмәтін элементтеріне тәуелді болуы мүмкін.

Белгілі көлемдегі шифрмәтін алынғаннан кейін генератор күйі қайта қалпына келуі мүмкін.

Виженер шифрын периодты символдық гаммалаудың классикалық үлгісі ретінде қарастыруға болады.

Виженер формуласы: $C_i = (M_i + K_i) \bmod m$.

Қысқа кілт қайталанғандықтан, периодтық заңдылық пайда болады; қазіргі тәсілдер кілттік ағынды криптографиялық генератордан қалыптастырады.

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

Артықшылықтары

Операциялары қарапайым және жылдам.

Деректерді келген бойда өңдеуге болады.

Дұрыс кілттік ағын бірдей символдарды әр позицияда әртүрлі шифрлайды.

Шектеулері

Кілттік ағынның қайталануы қауіпті.

Болжанатын генератор қауіпсіздікті төмендетеді.

Гаммалау өздігінен тұтастық пен түпнұсқалықты қамтамасыз етпейді.

Толық есептік мысал: DATA + CODE

A=0, B=1, …, Z=25; DATA=(3,0,19,0), CODE=(2,14,3,4).

Әріп	Есептеу	Нәтиже	Шифрәріп
D	(3+2) mod 26	5	F
A	(0+14) mod 26	14	O
T	(19+3) mod 26	22	W
A	(0+4) mod 26	4	E

DATA → FOWE

Қорытынды

Гаммалау ашық мәтін элементтерін кілттік тізбекпен біріктіруге негізделеді.

Символдық алфавитте модуль бойынша қосу, екілік деректерде көбіне XOR қолданылады.

Қауіпсіз кілттік ағын болжануы қиын, дұрыс синхрондалған және қайталанбайтын болуы тиіс.

Бір реттік блокнот — гаммалаудың теориялық эталоны.

Нақты жүйеде құпиялылықпен бірге тұтастық пен аутентификация да ескерілуі қажет.

Бақылау сұрақтары

1. Гаммалау шифры дегеніміз не?
2. Гамма мен кілттік ағынның айырмашылығы қандай?
3. Модуль бойынша гаммалау қалай орындалады?
4. XOR неге екілік гаммалауға ыңғайлы?
5. Бір реттік блокноттың негізгі шарттары қандай?
6. Бір гамманы қайта қолдану неге қауіпті?
7. Псевдокездейсоқ генераторға қандай талаптар қойылады?
8. Синхронды және өзін-өзі синхрондайтын гаммалау несімен ерекшеленеді?
9. Виженер шифры гаммалаумен қалай байланысты?
10. Гаммалау тұтастық пен аутентификацияны өздігінен қамтамасыз ете ме?

Список источников

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

2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері. 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.