5-ДӘРІС

КОДТАУ. КОМПОЗИЦИЯЛЫҚ ШИФРЛАР

Ақпаратты криптографиялық қорғау негіздері

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің мақсаты

Кодтау мен криптографиялық шифрлаудың мақсатын және айырмашылығын түсіну.

Символдық ақпараттың сандық және биттік түрде берілу қағидасын меңгеру.

Композициялық шифрдың бірнеше түрлендіруден қалай құрылатынын түсіну.

Ауыстыру мен орын алмастыруды біріктіруді нақты мысалдармен орындау.

Каскадты және раундтық құрылымдардың мәнін түсіндіру.

Композицияның статистикалық байланыстар мен криптографиялық беріктілікке әсерін талдау.

Кодтау дегеніміз не?

Кодтау – ақпаратты белгілі бір ереже бойынша бір ұсыну формасынан екінші формаға түрлендіру.

Кодтаудың мақсаты – ақпаратты көрсетуге, сақтауға, беруге немесе компьютерде өңдеуге ыңғайлы ету.

Кодтау үшін құпия кілт міндетті емес. Ереже белгілі болса, бастапқы ақпаратты қалпына келтіру әдетте оңай.

Сондықтан кодтау өздігінен ақпараттың құпиялылығын қамтамасыз етпейді.

Мысал 1. Әріпті санмен кодтау

A=0, B=1, C=2, …, Z=25

Символ	**D**	**A**	**T**	**A**
Сандық код	3	0	19	0

DATA → (3, 0, 19, 0)

Ақпарат жасырылған жоқ: тек символдар басқа формада көрсетілді.

Егер сәйкестік кестесі белгілі болса, (3,0,19,0) → DATA түрлендіруі бірден орындалады.

Кодтау мен шифрлаудың айырмашылығы

Белгі	Кодтау	Шифрлау
Мақсат	Форматты өзгерту	Мазмұнды құпиялау
Құпия кілт	Міндетті емес	Көп жағдайда қажет
Кері түрлендіру	Ереже белгілі болса оңай	Дұрыс кілтке тәуелді
Қауіпсіздік	Негізгі мақсат емес	Құпиялылық – негізгі мақсаттардың бірі
Мысал	A→0, B→1	Цезарь, Виженер, блоктық шифр

Қорытынды: кодтау – ұсыну тәсілі, шифрлау – криптографиялық түрлендіру.

Ақпаратты сандық кодтау

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

Криптографиялық алгоритмдер математикалық амалдар орындайды, сондықтан символдар алдымен сандарға немесе биттерге сәйкестендіріледі.

Егер алфавит $A=\{a_0,a_1,\ldots,a_{m-1}\}$ болса, әр символға 0-ден m−1-ге дейінгі сан беріледі.

Сандық ұсынудан кейін модульдік арифметика, матрицалық көбейту және логикалық операциялар қолдануға болады.

Компьютерлік жүйеде мәтін, сурет немесе дыбыс ақырында биттік тізбек ретінде өңделеді.

Мысал 2. Сандық кодтау және модульдік амал

A=0, …, Z=25, m=26

Цезарь түрлендіруі: E(x) = (x + k) mod 26

Әріп	**C**	**O**	**D**	**E**
x	2	14	3	4
k=2 кейін	4	16	5	6
Нәтиже	E	Q	F	G

CODE → EQFG

Композициялық шифр ұғымы

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

Композициялық шифр – екі немесе одан да көп қарапайым криптографиялық түрлендіруді белгілі ретпен біріктіретін шифр.

Бір ғана ауыстыру немесе бір ғана орын алмастыру мәтіннің кейбір статистикалық заңдылықтарын сақтауы мүмкін.

Әртүрлі түрлендірулерді тізбектей қолдану ашық мәтін мен шифрмәтін арасындағы байланысты күрделендіреді.

E_1 бірінші орындалса, одан кейін E_2, …, E_n орындалады.

Композициялық шифрды дешифрлау

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

Шифрлау кезінде операциялар $E_1 \rightarrow E_2 \rightarrow \ldots \rightarrow E_n$ ретімен орындалады.

Дешифрлау кезінде олардың кері түрлендірулері кері ретпен қолданылады.

Соңғы орындалған шифрлау операциясы бірінші болып кері қайтарылады.

Бұл қағида функциялар композициясының кері түрлендірілуіне негізделеді.

Есте сақтаңыз: шифрлау реті мен дешифрлау реті қарама-қарсы.

Мысал 3. Ауыстыру + орын алмастыру

Кезең	Операция	Нәтиже
1	Ашық мәтін	ABCD
2	Цезарь, k=1	BCDE
3	1↔3 және 2↔4	DEBC

ABCD → BCDE → DEBC

Бірінші операция символ мәндерін өзгертеді.

Екінші операция символдардың позицияларын өзгертеді.

Нәтижесінде бастапқы құрылымды тікелей байқау қиындайды.

Мысал 3. Дешифрлау

Шифрмәтін: DEBC

1-қадам: позицияларды кері ауыстыру **DEBC → BCDE**

2-қадам: Цезарь k=1 кері жылжыту **BCDE → ABCD**

Бастапқы мәтін толық қалпына келді.

Толық мысал. CODE сөзін композициялық шифрлау

Қадам	Түрлендіру	Нәтиже
0	Ашық мәтін	CODE
1	Цезарь, k=2	EQFG
2	Символдарды кері ретпен жазу	GFQE

$$C = GFQE$$

Дешифрлау: GFQE → EQFG → CODE.

Алдымен соңғы операция кері қайтарылады, содан кейін бірінші операция.

Каскадты шифрлау

$$M \rightarrow E_1(K_1) \rightarrow E_2(K_2) \rightarrow \ldots \rightarrow E_n(K_n) \rightarrow C$$

Бірнеше шифрлау операциясын тізбектей қолдануды каскадты түрлендіру ретінде қарастыруға болады.

Әр кезең жеке кілтке тәуелді болуы мүмкін: K_1, K_2, …, K_n.

Кілттердің тәуелсіздігі мен әр кезеңнің қасиеттері жалпы жүйенің беріктілігіне әсер етеді.

Бірнеше әлсіз алгоритмді жай ғана біріктіру автоматты түрде берік жүйе жасамайды.

Каскадқа қарапайым оқу мысалы

M = DATA

Кезең	Ереже	Нәтиже
1	Цезарь $k_1=1$	EBUB
2	Кері ретпен орналастыру	BUBE
3	Цезарь $k_2=2$	DW DG → DWDG (аралық мысал)

Мақсат – нақты стандартты алгоритмді емес, бірнеше кезеңнің бір-біріне тәуелді орындалуын көрсету.

Раундтық құрылым

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

Қазіргі блоктық шифрларда композиция бір рет емес, бірнеше раунд бойы қайталанады.

Раунд – алгоритм ішіндегі типтік өңдеу кезеңі.

Раундта ауыстыру, араластыру, орын алмастыру және раундтық кілтпен біріктіру орындалуы мүмкін.

Әр раундтың нәтижесі келесі раундтың кірісіне айналады.

Раундтық өңдеудің сұлбасы

$$X_0 \rightarrow \overset{R_1, K_1}{\rightarrow} \overset{R_2, K_2}{\rightarrow} \overset{R_3, K_3}{\rightarrow} X_3 = C$$

K_i – әр раундта қолданылатын раундтық кілт.

Раундтар саны мен нақты операциялар алгоритмге байланысты.

Бірнеше раунд бастапқы мәтіннің құрылымын біртіндеп күрделірек өзгертеді.

Статистикалық байланыстар неге маңызды?

Тәсіл	Не сақталуы мүмкін?
Моноалфавиттік ауыстыру	Әріптердің жиілік қатынастары ішінара сақталады
Тек орын алмастыру	Әріп жиіліктері толық сақталады
Композиция	Мән мен позиция арасындағы тәуелділік күрделенеді

Композицияның мақсаты – қарапайым түрлендірулердің әлсіз жақтарын азайтып, байланыстарды күрделендіру.

Мысал 4. Жиілік тұрғысынан түсіндіру

Ашық мәтін: AAAAA BBB C

Тек орын алмастыру қолданылса, A саны – 5, B саны – 3, C саны – 1 болып қалады.

Демек, символдардың орындары өзгергенімен, жиілік сипаттамасы өзгермейді.

Ауыстыру символ атауларын өзгертеді, бірақ қарапайым моноалфавиттік жағдайда жиілік құрылымы басқа таңбаларға көшеді.

Сондықтан қазіргі шифрларда бірнеше операция мен бірнеше раунд қолданылады.

Композициялық шифрлардың артықшылықтары

- Әртүрлі түрлендірулердің пайдалы қасиеттерін бір алгоритмде біріктіруге мүмкіндік береді.
- Символ мәні мен позициясын қатар өзгертуге болады.
- Ашық мәтіннің тікелей құрылымын күрделірек етеді.
- Көпраундты симметриялық шифрлардың құрылымдық идеясын түсіндіреді.
- Кейінгі «шашырату» және «араластыру» ұғымдарын меңгеруге негіз болады.

Шектеулері және жобалау талаптары

- ✓ Кезеңдер санының көп болуы өздігінен қауіпсіздік кепілі емес.
- ✓ Әлсіз операцияларды механикалық түрде қосу күтілген нәтиже бермеуі мүмкін.
- ✓ Жалпы беріктілік операциялардың математикалық қасиеттеріне тәуелді.
- ✓ Кілт кеңістігі жеткілікті болуы және кілттер дұрыс қалыптастырылуы керек.
- ✓ Раундтық кілттердің байланысы мен криптоталдау әдістеріне төзімділік бағалануы тиіс.

Сабақта талдауға арналған шағын тапсырма

1) *M=HELLO мәтінін A=0,…,Z=25 кодтауымен сандарға айналдырыңыз*.
2) Әр символға k=3 Цезарь ығысуын қолданыңыз.
3) Алынған мәтіндегі символдарды кері ретпен орналастырыңыз.
4) Соңғы шифрмәтінді жазыңыз.
5) Дешифрлауды кері ретпен орындап, HELLO мәтінінің қалпына келетінін тексеріңіз.
6) Қай кезең символ мәнін, қай кезең позициясын өзгертетінін түсіндіріңіз.

Әріптерді **A = 0, B = 1, …, Z = 25** ережесі бойынша сандарға айналдырамыз:

- **H = 7**
- **E = 4**
- **L = 11**
- **L = 11**
- **O = 14**

Сондықтан:

$$\boxed{M = HELLO \rightarrow (7,\ 4,\ 11,\ 11,\ 14)}$$

Жауабы: (7, 4, 11, 11, 14).

Өзін-өзі тексеру мысалы

M = CODE, k = 2

Сұрақ	Жауап
Сандық код	(2,14,3,4)
Цезарьдан кейін	EQFG
Кері реттен кейін	GFQE
Дешифрлау реті	Кері орналастыру → k=2 кері ығысу
Бастапқы мәтін	CODE

Қорытынды

Кодтау ақпаратты басқа формада көрсетеді, бірақ өздігінен криптографиялық құпиялылық бермейді.

Криптографияда символдар математикалық өңдеу үшін сандарға және биттерге түрлендіріледі.

Композициялық шифр бірнеше криптографиялық түрлендіруді белгілі ретпен біріктіреді.

Дешифрлау кезінде операциялар кері ретпен орындалады.

Ауыстыру + орын алмастыру комбинациясы символ мәні мен позициясын қатар өзгертеді.

Каскадты және көпраундты құрылымдар қазіргі симметриялық криптографияны 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. Дешифрлау операциялары неге кері ретпен орындалады?
6. Ауыстыру мен орын алмастыруды біріктіру қандай нәтиже береді?
7. Каскадты шифрлау дегеніміз не?
8. Раунд және раундтық кілт дегеніміз не?
9. Неліктен бірнеше әлсіз операция автоматты түрде берік шифр жасамайды?
10. Композициялық шифрлар қазіргі блоктық шифрлармен қалай байланысты?