## 10-ДӘРІС

## ҚҰРАМДАС ШИФРЛАР. ШАШЫРАТУ ЖӘНЕ АРАЛАСТЫРУ. РАУНДТАР

**Дәрістің мақсаты:** Құрамдас шифрлардың құрылымын түсіндіру, шашырату және араластыру қағидаларының мағынасын ашу, раундтық өңдеудің қажеттілігін көрсету және қарапайым түрлендірулердің көпраундты композиция арқылы күрделі шифрға айналуын талдау.

**Құрамдас шифр ұғымы**

Құрамдас шифр бірнеше қарапайым криптографиялық операцияны бір алгоритмде біріктіреді. Әдетте ауыстыру, орын алмастыру, кілтпен біріктіру және сызықтық не сызықтық емес түрлендірулер белгілі ретпен қайталанады. Негізгі мақсат – ашық мәтін, кілт және шифрмәтін арасындағы қарапайым статистикалық тәуелділіктерді әлсірету.

Жеке криптографиялық операция көбіне деректердің тек бір қасиетін өзгертеді. Мысалы, ауыстыру кезінде символ немесе бит басқа мәнмен алмастырылады, ал орын алмастыру кезінде олардың мәндері сақталып, орналасу реті өзгереді. Егер осы операциялар жеке-жеке қолданылса, бастапқы мәтіннің кейбір статистикалық ерекшеліктері сақталуы мүмкін. Сондықтан құрамдас шифрларда әртүрлі түрлендірулер бірінен кейін бірі орындалады.

Құрамдас шифрлаудың жалпы құрылымын келесі түрде көрсетуге болады:

$$M \rightarrow T_1 \rightarrow T_2 \rightarrow \ldots \rightarrow T_r \rightarrow C$$

мұндағы M – ашық мәтін, $T_1$, $T_2$, …, $T_r$ – криптографиялық түрлендірулер, C – шифрмәтін.

Мысалы, бастапқы блок M=ABCD болсын. Алдымен әр символ келесі символмен ауыстырылсын:

$$ABCD \rightarrow BCDE$$

Одан кейін символдардың орындары өзгертілсін:

$$BCDE \rightarrow DEBC$$

Бірінші операция символдардың мәндерін, ал екінші операция олардың орналасуын өзгертті. Нәтижесінде бастапқы ABCD блогының құрылымы бір ғана операция қолданылған жағдайға қарағанда көбірек өзгереді.

Қазіргі блоктық шифрларда мұндай операциялар бірнеше рет қайталанады. Әрбір қайталану кезеңі раунд деп аталады:

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

мұндағы $X_{i-1}$ – раундқа кіретін деректер, R – раундтық түрлендіру, $K_i$ – раундтық кілт, $X_i$ – раунд нәтижесі.

Осылайша құрамдас шифрдың беріктілігі тек бір күрделі операцияға емес, бірнеше операцияның өзара байланысына негізделеді. Әсіресе шашырату мен араластыру қасиеттерін бірге қалыптастыру маңызды.

**Шашырату ұғымы**

Шашырату (diffusion) – ашық мәтіннің бір символының немесе бір битінің әсерін шифрмәтіннің көптеген позицияларына тарату қағидасы. Жақсы шашыратуда ашық мәтіндегі шағын өзгеріс бірнеше раундтан кейін шифрмәтіннің көптеген биттерін өзгертеді.

Шашыратудың негізгі мақсаты – ашық мәтіннің статистикалық ерекшеліктерін шифрмәтінде тікелей байқатпау. Табиғи тілде кейбір әріптер немесе символдар басқаларға қарағанда жиі кездеседі. Егер олардың бұл ерекшелігі шифрмәтінде де сақталса, статистикалық талдау бастапқы мәтін туралы ақпарат беруі мүмкін. Шашырату осы статистикалық тәуелділікті бүкіл блокқа таратады.

Қарапайым мысал қарастырайық. Төрт элементтен тұратын блок берілсін:

$$X = (x_1, x_2, x_3, x_4)$$

Түрлендіруден кейін әрбір жаңа элемент бірнеше бастапқы элементке тәуелді болсын:

$$y_1 = x_1 \oplus x_2$$
$$y_2 = x_2 \oplus x_3$$
$$y_3 = x_3 \oplus x_4$$
$$y_4 = x_4 \oplus x_1$$

Егер бастапқы $x_1$ мәні өзгерсе, бірден $y_1$ және $y_4$ өзгереді. Келесі раундта осы өзгерген $y_1$ және $y_4$ басқа элементтермен қайта араласады. Нәтижесінде бірнеше раундтан кейін бастапқы бір ғана биттің өзгерісі блоктың көптеген бөліктеріне таралады.

1 биттің өзгеруі → бірнеше битке әсер → келесі раунд → бүкіл блокқа таралу

Шашырату ұғымымен көшкін әсері (avalanche effect) тығыз байланысты. Көшкін әсері кезінде ашық мәтіндегі немесе кілттегі өте аз өзгеріс, мысалы бір биттің ауысуы, шифрмәтіндегі көптеген биттердің өзгеруіне әкеледі.

Мысалы:

$$M_1 = 10110010$$
$$M_2 = 10110011$$

Бұл екі блок тек соңғы бір битімен ерекшеленеді. Жақсы жобаланған көпраундты шифрда олардың шифрмәтіндері бір-бірінен тек бір битпен емес, көптеген позициялар бойынша ерекшеленуі күтіледі.

Бір кіріс элементінің әсерін көптеген шығыс элементтеріне тарату

Шашырату көбіне орын алмастыру, биттерді араластыру және сызықтық түрлендірулер арқылы қамтамасыз етіледі.

**Араластыру ұғымы**

Араластыру (confusion) – шифрмәтін мен кілт арасындағы тәуелділікті күрделі ету қағидасы. Бұл үшін көбіне сызықтық емес ауыстырулар пайдаланылады. Нәтижесінде кілт биттерінің шифрмәтінге әсерін қарапайым алгебралық байланыспен сипаттау қиындайды.

Егер кілт пен шифрмәтін арасындағы тәуелділік өте қарапайым болса, шифрмәтіндегі өзгерістерді зерттеу арқылы кілт туралы белгілі бір заңдылықтарды анықтау мүмкін болуы ықтимал. Сондықтан шифрлау алгоритмі кілттің әсерін мүмкіндігінше күрделі түрде таратуға ұмтылады.

Қарапайым сызықтық тәуелділік шартты түрде:

$$C = M \oplus K$$

түрінде көрінуі мүмкін. Мұнда шығыс C кіріс M және кілт K-мен өте қарапайым операция арқылы байланысқан.

Ал араластыруды күшейту үшін деректерге сызықтық емес түрлендіру енгізіледі:

$$Y = S(X)$$

мұндағы S – сызықтық емес ауыстыру функциясы.

Мысалы, төрт мүмкін кіріс үшін шартты ауыстыру кестесі берілсін:

| **Кіріс** | **Шығыс** |
|---|---|
| 00 | 10 |
| 01 | 00 |
| 10 | 11 |
| 11 | 01 |

Мұнда кіріс мәні мен шығыс мәні арасында қарапайым «бірді қосу» немесе «позицияны ауыстыру» тәрізді тәуелділік жоқ. Сондықтан мұндай ауыстыру бірнеше раунд ішінде кілттің шифрмәтінге әсерін күрделендіруге көмектеседі.

Кілт пен шифрмәтін арасындағы байланысты күрделендіру

Араластыру кезінде сызықтық емес түрлендірулердің маңызы ерекше. Егер барлық операция тек сызықтық болса, олардың композициясы да белгілі бір сызықтық құрылымды

сақтауы мүмкін. Сызықтық емес операцияларды енгізу мұндай қарапайым математикалық тәуелділікті бұзады.

**Шашырату мен араластырудың айырмашылығы**

| Салыстыру белгісі | Шашырату (diffusion) | Араластыру (confusion) |
|---|---|---|
| Негізгі мақсаты | Ашық мәтін әсерін көптеген позицияларға тарату | Кілт пен шифрмәтін байланысын күрделендіру |
| Негізгі байланыс | Ашық мәтін → шифрмәтін | Кілт → шифрмәтін |
| Қолданылатын тәсілдер | Орын алмастыру, араластыру, сызықтық түрлендіру | Сызықтық емес ауыстыру |
| Нәтижесі | Бір кіріс биті көптеген шығыс биттеріне әсер етеді | Кілт әсерін қарапайым тәуелділікпен сипаттау қиындайды |
| Байланысты ұғым | Көшкін әсері | Сызықтық еместік |

Қазіргі құрамдас шифрларда бұл екі қағида жеке емес, бірнеше раунд ішінде бірге жүзеге асырылады. Бір операция араластыруды қамтамасыз етсе, келесі операция алынған өзгерістерді бүкіл блокқа шашыратады. Келесі раундта бұл процесс қайта қайталанады:

Кілтпен біріктіру → Араластыру → Шашырату → келесі раунд

Нәтижесінде бірнеше раундтан кейін ашық мәтіннің де, кілттің де жеке элементтерінің шифрмәтінге әсері күрделі және кең таралған сипатқа ие болады. Осы себепті араластыру мен шашыратудың үйлесуі құрамдас шифрларды құрудың негізгі қағидаларының бірі болып табылады.

**Раунд ұғымы**

Раунд – шифр алгоритміндегі белгілі бір криптографиялық операциялар жиынтығы қайталанып орындалатын өңдеу кезеңі. Бір раунд барлық қажетті шашырату мен араластыруды бірден қамтамасыз етпеуі мүмкін, сондықтан түрлендіру бірнеше рет қайталанады. Әрбір келесі раунд алдыңғы раундтың нәтижесін кіріс ретінде қабылдайды және оны жаңа раундтық кілттің көмегімен қайта өңдейді.

$$X_i = R(X_{i-1}, K_i), \quad i = 1,\ldots,r$$

Мұндағы $X_{i-1}$ – i-раундқа кіретін деректер, R – раундтық түрлендіру функциясы, $K_i$ – осы раундта қолданылатын раундтық кілт, $X_i$ – раунд нәтижесі, r – раундтардың жалпы саны.

Бастапқы ашық мәтін $X_0=M$ деп белгіленсе, бірінші раундтан кейін:

$$X_1 = R(X_0, K_1)$$

алынады. Екінші раунд бірінші раундтың нәтижесін өңдейді:

$$X_2 = R(X_1, K_2)$$

Осы процесс соңғы раундқа дейін жалғасады:

$$X_r = R(X_{r-1}, K_r) = C$$

мұндағы C – соңғы шифрмәтін. Демек, көпраундты өңдеудің жалпы сұлбасын келесі түрде көрсетуге болады:

$$M \rightarrow R_1 \rightarrow R_2 \rightarrow \ldots \rightarrow R_r \rightarrow C$$

Раундтың ішінде бірнеше операция орындалуы мүмкін. Мысалы, деректер алдымен раундтық кілтпен біріктіріледі, содан кейін сызықтық емес ауыстыру жүргізіледі, одан кейін биттердің немесе байттардың орындары өзгертіліп, нәтижесі келесі раундқа беріледі. Бұл операциялардың нақты құрамы қолданылатын шифр алгоритміне байланысты.

Бірінші раундта бастапқы мәтіннің кейбір құрылымдық ерекшеліктері әлі сақталуы мүмкін. Бірақ келесі раундтарда алдыңғы өзгерістер қайта өңделіп, олардың әсері блоктың басқа элементтеріне таралады. Сондықтан бірнеше раунд араластыру мен шашыратудың жинақталған әсерін қалыптастырады.

Алайда раунд саны неғұрлым көп болса, шифр соғұрлым міндетті түрде берік болады деп біржақты айтуға болмайды. Шифрдың беріктілігі раунд санына ғана емес, раундтық функцияның қасиеттеріне, қолданылатын түрлендірулерге және кілттерді қалыптастыру тәсіліне де байланысты.

**Раундтық кілттер**

Негізгі құпия кілттен әр раундқа арналған $K_1$, $K_2$, …, $K_r$ раундтық кілттер қалыптастырылады. Бұл процесс кілттерді кеңейту (key expansion) немесе кілттер кестесі (key schedule) деп аталады.

$$K \rightarrow K_1, K_2, \ldots, K_r$$

Мұндағы K – бастапқы құпия кілт, ал $K_i$ – i-раундта қолданылатын раундтық кілт. Раундтық кілттердің қолданылуы бірдей раундтық операциялардың әр кезеңде әртүрлі кілттік әсермен орындалуына мүмкіндік береді.

Егер барлық раундта еш өзгеріссіз бірдей мән пайдаланылса, раундтар арасында қажетсіз қайталанатын тәуелділіктер пайда болуы мүмкін. Сондықтан негізгі кілттен бірнеше өзара байланысқан, бірақ әртүрлі раундтық кілттер алынады.

$$K_1 = f_1(K), \quad K_2 = f_2(K), \quad \ldots, \quad K_r = f_r(K)$$

Мұндағы $f_1$, $f_2$, …, $f_r$ – кілтті кеңейту алгоритміндегі түрлендірулер. Раундтық кілттің деректермен біріктірілуінің қарапайым мысалы – XOR операциясы:

$$Y = X \oplus K_i$$

Мұнда X – раундтағы ағымдағы деректер, $K_i$ – раундтық кілт, Y – кілтпен біріктірілген нәтиже. Кілттерді кеңейту алгоритмі де криптожүйенің маңызды бөлігі болып табылады. Оның мақсаты – негізгі құпия кілттің әсерін барлық раундтарға тарату және әр раундта кілтке тәуелді өзгеріс енгізу.

**Лавиналық әсер**

Лавиналық әсер (avalanche effect) – кірістегі өте аз өзгерістің, мысалы бір биттің ауысуының, шифрлау нәтижесіндегі көптеген биттердің өзгеруіне әкелетін қасиет. Ол шашырату мен араластырудың бірлескен нәтижесін сипаттайтын маңызды практикалық белгі болып табылады.

Мысалы, екі ашық мәтін блогы берілсін:

$$M_1 = 10110010$$
$$M_2 = 10110011$$

Бұл екі блоктың айырмашылығы – тек бір бит. Егер олар бірдей кілтпен шифрланса, жақсы жобаланған көпраундты шифрда алынған $C_1$ және $C_2$ шифрмәтіндері көптеген биттер бойынша ерекшеленуі күтіледі.

1 биттің өзгеруі → 1-раунд → бірнеше өзгеріс → 2-раунд → өзгерістердің таралуы → …

Лавиналық әсерді сандық түрде бағалау үшін екі шифрмәтіндегі әртүрлі биттердің санын есептеуге болады. Егер блок ұзындығы n бит, ал өзгерген биттер саны d болса, өзгеру үлесін келесі формуламен көрсетуге болады:

$$A = (d / n) \cdot 100\%$$

Мысалы, 64 биттік екі шифрмәтіннің 31 биті әртүрлі болсын:

$$A = (31 / 64) \cdot 100\% \approx 48{,}4\%$$

Бұл мысалда кірістегі бір биттің өзгерісі шығыс биттерінің шамамен жартысына әсер еткен.

Лавиналық әсер тек ашық мәтін өзгергенде ғана емес, кілттің бір биті өзгергенде де зерттелуі мүмкін. Екі өте ұқсас кілтпен бірдей ашық мәтін шифрланған кезде алынған шифрмәтіндердің едәуір ерекшеленуі кілт әсерінің жақсы араластырылғанын көрсетеді.

Осы үш ұғым бір-бірімен тікелей байланысты:

Раундтар + әртүрлі раундтық кілттер → араластыру және шашырату → лавиналық әсер

Яғни раундтар өзгерістерді бірнеше рет өңдеуге мүмкіндік береді, раундтық кілттер әр кезеңге кілттік тәуелділік енгізеді, ал шашырату мен араластыру осы өзгерістерді блок бойынша таратады. Нәтижесінде ашық мәтіндегі немесе кілттегі шағын өзгеріс соңғы шифрмәтінде елеулі айырмашылық туғызады.

**Оқу мысалы**

8 биттік блок екі бөлікке бөлініп, бірінші кезеңде кілтпен XOR, екінші кезеңде позициялар ауыстырылсын. Бір ғана раундта байланыстар әлі байқалуы мүмкін. Сол операциялар жаңа раундтық кілттермен бірнеше рет қайталанса, бастапқы биттердің әсері блок бойына тарайды. Бұл мысал нақты стандартты шифр емес, раундтық композиция идеясын түсіндіруге арналған.

**Қауіпсіздікке әсері**

Раунд санын көбейту әрқашан автоматты түрде қауіпсіздікті шексіз арттырмайды. Раунд функциясының математикалық қасиеттері, кілт кестесі, блок өлшемі және криптоталдауға төзімділік бірге бағаланады.

**Қорытынды**

Құрамдас шифрлар шашырату мен араластыруды бірнеше раунд бойы біріктіреді. Шашырату ашық мәтін статистикасының әсерін таратады, араластыру кілт пен шифрмәтін арасындағы байланысты күрделендіреді, ал раундтық құрылым осы қасиеттерді біртіндеп күшейтеді.

**Бақылау сұрақтары**

1. Құрамдас шифр дегеніміз не?
2. Шашырату қағидасының мақсаты қандай?
3. Араластыру қағидасының мақсаты қандай?
4. Шашырату мен араластырудың айырмашылығы неде?
5. Раунд дегеніміз не?
6. Раундтық кілттер не үшін қажет?
7. Кілттерді кеңейту дегеніміз не?
8. Лавиналық әсер нені сипаттайды?
9. Неліктен бірнеше раунд қолданылады?
10. Құрамдас шифрдың беріктігі қандай факторларға тәуелді?

**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. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024.
5. Омассон Ж.-Ф. О криптографии всерьез. Практическое введение в современное шифрование. Москва: ДМК Пресс, 2021.