11-ДӘРІС
СИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕЛЕР ЖӘНЕ ҚҰРУ ПРИНЦИПІ. ФЕЙСТЕЛЬ ЖЕЛІСІ

Дәрістің мақсаты: Симметриялық криптожүйелердің негізгі қағидасын түсіндіру, блоктық және ағындық тәсілдердің орнын көрсету, Фейстель желісінің құрылымын, раундтық функциясын және шифрлау-дешифрлау симметриясын талдау.

Симметриялық криптожүйе ұғымы

Симметриялық криптожүйе – шифрлау мен дешифрлау үшін бір құпия кілт немесе бір-бірінен оңай есептелетін құпия кілттер қолданылатын криптографиялық жүйе. Жіберуші мен қабылдаушы осы кілтті алдын ала қауіпсіз түрде келісуі және оны бөгде тұлғалардан қорғауы керек.

$$C = E_K(M)$$
$$M = D_K(C)$$

Мұндағы M – ашық мәтін, C – шифрмәтін, K – құпия кілт, E_K – K кілтімен орындалатын шифрлау функциясы, D_K – дешифрлау функциясы.

$$D_K(E_K(M)) = M$$

Мысалы, жіберушіде M хабарламасы бар делік. Ол ортақ құпия K кілтін пайдаланып C шифрмәтінін алады. Байланыс арнасы арқылы C жіберіледі. Қабылдаушыда сол K кілті болғандықтан, ол C-ны дешифрлап, бастапқы M хабарын қалпына келтіреді.

$$M \rightarrow E_K \rightarrow C \rightarrow D_K \rightarrow M$$

Бұл жерде байланыс арнасымен құпия кілт емес, шифрмәтін беріледі. Сондықтан симметриялық криптожүйенің қауіпсіздігі кілттің құпия сақталуына тікелей байланысты.

Негізгі қасиеттер

Симметриялық алгоритмдердің маңызды артықшылығы – жоғары жылдамдық. Олар үлкен көлемдегі деректерді өңдеуге қолайлы болғандықтан, файлдарды, деректер қорын, желілік трафикті және басқа көлемді ақпаратты қорғауда кеңінен қолданылады.

Екінші маңызды қасиет – шифрлау мен дешифрлауда қолданылатын кілттердің өзара тығыз байланысы. Көп жағдайда екі тарап бірдей құпия кілтті қолданады.

$$K_{жіберуші} = K_{қабылдаушы}$$

Бірақ осы ерекшелік симметриялық криптографияның негізгі ұйымдастырушылық мәселесін туғызады: құпия кілтті тараптарға қалай қауіпсіз жеткізу керек? Егер кілт қорғалмаған арнамен жіберіліп, оны үшінші тұлға алса, шифрланған ақпараттың құпиялығы бұзылады. Сондықтан кілтті генерациялау, қауіпсіз бөлу, сақтау, мерзімді жаңарту және қажет болғанда жою криптографиялық жүйенің маңызды бөлігі болып табылады.

Пайдаланушылар саны артқан сайын кілттерді басқару да күрделене түседі. Егер әрбір екі пайдаланушы жеке құпия кілтпен байланысуы қажет болса, n пайдаланушы үшін кілт жұптарының саны:

$$N = n(n - 1) / 2$$

формуласы бойынша өседі. Мысалы, 10 пайдаланушы үшін:

$$N = 10 \cdot 9 / 2 = 45$$

Яғни 10 пайдаланушы арасында жеке-жеке қорғалған байланыс ұйымдастыру үшін 45 құпия кілт қажет болуы мүмкін. Бұл симметриялық криптографиядағы кілттерді басқару мәселесінің маңызын көрсетеді.

Ағындық және блоктық шифрлар

Симметриялық шифрлар деректерді өңдеу тәсіліне қарай негізінен ағындық және блоктық шифрларға бөлінеді.

Белгі	Ағындық шифр	Блоктық шифр
Өңдеу бірлігі	Бит немесе байт ағыны	Белгіленген өлшемді блок
Негізгі идея	Деректерді кілттік ағынмен біріктіру	Блокты кілтке тәуелді түрлендіру
Өңдеу сипаты	Деректер ретімен өңделеді	Деректер блоктарға бөлінеді
Негізгі операция	Көбіне кілттік ағынмен XOR	Көпраундты блоктық түрлендіру
Қолдану	Үздіксіз деректер ағындары	Файлдар, хабарламалар, сақтау жүйелері

Ағындық шифрда деректер біртіндеп, мысалы бит немесе байт бойынша өңделеді. Арнайы алгоритм құпия кілт негізінде кілттік ағын қалыптастырады:

$$Z = z_1, z_2, \ldots, z_n$$

Ашық мәтін $M = m_1, m_2, \ldots, m_n$ болса, қарапайым модельде шифрмәтін:

$$c_i = m_i \oplus z_i$$

арқылы алынады. Дешифрлау:

$$m_i = c_i \oplus z_i$$

түрінде орындалады. Бұл XOR операциясының $a \oplus b \oplus b = a$ қасиетіне негізделеді.

Блоктық шифрда ашық мәтін белгіленген ұзындықтағы блоктарға бөлінеді:

$$M = M_1, M_2, \ldots, M_t$$

Әрбір блок құпия кілтке тәуелді көпраундты түрлендіруден өтеді:

$$C_i = E_K(M_i)$$

Блоктық шифрдың ішінде ауыстыру, орын алмастыру, XOR, сызықтық және сызықтық емес түрлендірулер сияқты бірнеше операция қолданылуы мүмкін. Олардың бірнеше раунд бойы қайталануы араластыру мен шашыратуды қамтамасыз етуге бағытталған.

Фейстель желісінің идеясы

Фейстель желісі (Feistel network) – блоктық шифрларды құруда қолданылатын көпраундты құрылымдардың бірі. Оның негізгі ерекшелігі – кіріс блоктың екі бөлікке бөлінуі және әр раундта осы бөліктердің бір-бірімен раундтық функция арқылы байланыстырылуы.

$$X_0 = (L_0, R_0)$$

Мұндағы L_0 – блоктың сол жақ бөлігі, R_0 – оң жақ бөлігі. Әрбір i-раундта келесі түрлендіру орындалады:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Мұндағы F – раундтық функция, K_i – i-раундтың кілті, $\oplus$ – XOR операциясы. Алдымен алдыңғы раундтың оң бөлігі R_{i-1} раундтық F функциясына беріледі. Функцияға K_i раундтық кілті енгізіледі. Алынған нәтиже алдыңғы сол бөлікпен XOR арқылы біріктіріліп, жаңа оң бөлікке айналады. Бұрынғы оң бөлік жаңа сол бөлік болады.

$$(L_{i-1}, R_{i-1}) \rightarrow (R_{i-1}, L_{i-1} \oplus F(R_{i-1}, K_i))$$

Фейстель раундының қарапайым мысалы

Бастапқы екі жарты L_0=1010 және R_0=0110 болсын. Оқу мысалы ретінде раундтық функцияның нәтижесі $F(R_0,K_1)$=1100 деп берілсін.

$$L_1 = R_0 = 0110$$
$$R_1 = L_0 \oplus F(R_0,K_1)$$
$$R_1 = 1010 \oplus 1100 = 0110$$

Сондықтан бірінші раундтың нәтижесі:

$$(L_1, R_1) = (0110, 0110)$$

Бұл шағын мысалда F функциясының нәтижесі дайын берілді. Негізгі мақсат – Фейстель желісінде екі жарты блоктың қалай ауысатынын және XOR операциясының қалай қолданылатынын түсіну.

Бірнеше раундтың орындалуы

Фейстель желісі бір ғана раундпен шектелмейді. Бірінші раундтан алынған (L_1,R_1) екінші раундтың кірісі болады:

$$L_2 = R_1$$
$$R_2 = L_1 \oplus F(R_1,K_2)$$

Одан кейін келесі раундта:

$$L_3 = R_2$$
$$R_3 = L_2 \oplus F(R_2,K_3)$$

Осылайша процесс r раунд бойы қайталанады. Әр раундта басқа K_i раундтық кілті қолданылғандықтан, деректердің өзгеруі біртіндеп бүкіл блокқа таралады.

Фейстель желісінің маңызды ерекшелігі

Фейстель желісінің маңызды қасиеттерінің бірі – раундтық F функциясының өзі міндетті түрде кері функцияға ие болуы шарт емес. Бүкіл құрылымның қайтымдылығы XOR операциясының қасиеттері мен жарты блоктардың ауысуы арқылы қамтамасыз етіледі.

$$A \oplus B \oplus B = A$$

Сондықтан шифрлау кезінде қосылған раундтық функцияның нәтижесін дешифрлау кезінде қайта XOR арқылы алып тастауға болады.

Фейстель құрылымында дешифрлау кезінде негізінен сол раундтық құрылым пайдаланылады, бірақ раундтық кілттер кері ретпен қолданылады:

$$K_r, K_{r-1}, \ldots, K_2, K_1$$

Яғни шифрлау $K_1 \rightarrow K_2 \rightarrow \ldots \rightarrow K_r$ ретімен орындалса, дешифрлау $K_r \rightarrow K_{r-1} \rightarrow \ldots \rightarrow K_1$ ретімен орындалады. Осы қасиет Фейстель желісінің практикалық маңызын арттырады: шифрлау мен дешифрлау үшін түбегейлі екі бөлек құрылым жасаудың қажеті жоқ.

Блокты екіге бөлу → $F(R,K_i)$ → XOR → бөліктердің рөлін ауыстыру → келесі раунд

Бірнеше раундтың нәтижесінде бастапқы блоктың сол және оң бөліктеріндегі ақпарат өзара араласып, өзгерістер блок бойынша таралады. Сондықтан Фейстель желісі араластыру,

шашырату, раундтық өңдеу және раундтық кілттер қағидаларын бір құрылымда жүзеге асырудың көрнекі мысалы болып табылады.

Раунд теңдеулері

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Мұндағы F – раундтық функция, K_i – і-раундтық кілт.

Фейстель құрылымының қайтымдылығы

Фейстель құрылымының маңызды қасиеті – раундтық функцияның F өзі міндетті түрде кері функцияға ие болмауы мүмкін. Соған қарамастан, бүкіл Фейстель құрылымы қайтымды болады, яғни шифрмәтіннен бастапқы ашық мәтінді қалпына келтіруге мүмкіндік береді.

Бір раундтың формулалары:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Бірінші теңдіктен алдыңғы оң бөлікті бірден анықтаймыз:

$$R_{i-1} = L_i$$

Екінші теңдеуден L_{i-1} мәнін қалпына келтіруге болады:

$$L_{i-1} = R_i \oplus F(L_i, K_i)$$

Бұл мүмкіндік XOR операциясының маңызды қасиетіне негізделеді:

$$A \oplus B \oplus B = A$$

Яғни белгілі бір мәнді B-мен XOR арқылы өзгертіп, кейін дәл сол B-мен қайта XOR жасасақ, бастапқы мән қалпына келеді.

Қарапайым мысал

Алдыңғы раундта L_0=1010, R_0=0110 және $F(R_0,K_1)$=1100 болсын. Шифрлау кезінде:

$$L_1 = R_0 = 0110$$
$$R_1 = L_0 \oplus F(R_0,K_1)$$
$$R_1 = 1010 \oplus 1100 = 0110$$

Сонымен, раунд нәтижесі:

$$(L_1, R_1) = (0110, 0110)$$

Енді бастапқы мәндерді қайта қалпына келтіреміз. Алдымен:

$$R_0 = L_1 = 0110$$

Содан кейін:

$$L_0 = R_1 \oplus F(L_1,K_1)$$
$$L_0 = 0110 \oplus 1100 = 1010$$

Нәтижесінде бастапқы блок толық қалпына келеді:

$$(L_0, R_0) = (1010, 0110)$$

Раундтық кілттердің кері ретпен қолданылуы

Көпраундты Фейстель желісінде шифрлау кезінде раундтық кілттер $K_1, K_2, K_3, \ldots, K_r$ ретімен қолданылса, дешифрлау кезінде олардың реті кері болады:

$$K_r, K_{r-1}, K_{r-2}, \ldots, K_1$$

Мысалы, төрт раунд үшін:

Шифрлау: $K_1 \rightarrow K_2 \rightarrow K_3 \rightarrow K_4$

Дешифрлау: $K_4 \rightarrow K_3 \rightarrow K_2 \rightarrow K_1$

Осылайша шифрлау мен дешифрлау үшін түбегейлі екі түрлі алгоритм құру қажет емес. Негізгі раундтық құрылым сақталады, тек раундтық кілттердің қолданылу реті өзгереді. Бұл

Фейстель желісінің аппараттық және бағдарламалық іске асырылуын ықшамдайтын маңызды артықшылықтарының бірі.

Бірдей раундтық құрылым + кілттердің кері реті → дешифрлау

Сондықтан Фейстель желісінің ерекшелігі тек деректерді бірнеше раундта араластыруында емес, қайтымдылықты қарапайым әрі тиімді құрылым арқылы қамтамасыз етуінде.

Бір раундтың оқу мысалы

$L_0=1010$, $R_0=1100$ болсын. Оқу үшін $F(R_0,K_1)=0110$ деп алайық. Сонда $L_1=1100$, ал $R_1=1010 \oplus 0110=1100$. Бұл мысалда F функциясының ішкі есебі қарастырылмайды; мақсат – жарты блоктардың раундта қалай өзгеретінін көрсету.

Көпраундты құрылым

Бір раунд жеткілікті шашырату мен араластыру бермейді. Сондықтан Фейстель желісі бірнеше раундтан тұрады. Әр раундта жаңа K_i кілті қолданылып, бастапқы блоктың биттері біртіндеп күрделі тәуелділікке түседі.

Құру принциптері

Симметриялық блоктық шифрды жобалауда блок пен кілт өлшемі, раунд саны, раундтық функцияның сызықтық еместігі, кілт кестесінің қасиеттері және белгілі криптоталдау әдістеріне төзімділік ескеріледі.

Қорытынды

Симметриялық криптожүйелер бір құпия кілтке сүйенеді және деректерді жылдам өңдеуге қолайлы. Фейстель желісі блокты екі бөлікке бөліп, раундтық функция мен XOR арқылы көпраундты түрлендіру орындайды; дешифрлау кезінде сол құрылым кілттерді кері ретпен қолданады.

Бақылау сұрақтары

1. Симметриялық криптожүйе дегеніміз не?
2. Симметриялық шифрлаудың негізгі кілттік мәселесі қандай?
3. Ағындық және блоктық шифрлардың айырмашылығы неде?
4. Фейстель желісінде блок қалай бөлінеді?
5. Фейстель раундының теңдеулері қалай жазылады?
6. F раундтық функциясының рөлі қандай?
7. Фейстель желісінде дешифрлау қалай орындалады?
8. Неліктен F функциясы міндетті түрде кері функция болмауы мүмкін?
9. Көп раунд не үшін қажет?
10. Симметриялық шифрды жобалауда қандай факторлар ескеріледі?

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.