Лекция 4 DES ЖӘНЕ AES ШИФРЛАУ АЛГОРИТМДАРЫ

Негізгі мәліметтер

Жабық кілті бар криптографиялық жүйелердің ең танымалы DES – Data Encryption Standard. Бұл жүйе деректерді шифрлау облыста мемлекеттік стандарт статусты ең бірінші алған болатын. Оны ойлап жасаған IBM фирманың мамандары және АҚШ-а іске қосылды 1977 жылы. DES алгоритмы деректерді сақтағанда және түрлі есептеуіш жүйелер арасында деректерді беру кезінде; пошталық жүйелерде; электронды сызбалар жүйелерде және коммерциялық ақпаратпен электронды алмасу кезінде кең пайдаланатын. DES стандарты бағдарламалық та аппараттық та жүзеге асырылатын.

Соңғы уақытта бұл жүйеде мемлекеттік стандарт статусы болмасада, ол бұрынғыдай кең қолданылады және жабық кілті бар блокты шифрларды оқып үйренгенде бұл алгоритмға назар аудару жөн.

DES алгоритмда кілт ұзындығы 56 бит. Дәл осыған байланысты негізгі проблема - DES әртүрлі шабуылдарға шыдай алама? Қандай да болса блокты шифрды бұзуға болады, егер барлық мүмкін болатын кілттер комбинациясын іріктеп алатын болсақ. Кілт ұзындығы 56 бит болғанда мүмкін болатын түрлі кілттердің саны 2^{56}. Егер компьютер бір секундта 1000000 кілтті (2^{20} жуық) іріктеп алса, онда барлық 2^{56} кілтті ірктеп алу үшін 2^{36} секунд қажет болады немесе екі мың жылдай.

Бірақ, дербес компьютерден жылдам және қымбат есептеуіш жүйелерді де пайдалануға болады. Мысалы, егер параллель есептеуді жүргізу үшін миллион процессорды біріктіретің болсақ, онда кілтті іріктеп алу үшін 18 сағат ғана қажет. Сондықтан, криптоталдаушының қолында осындай қымбат техника болса, DES пен шифрланған деректерді жеткілікті уақытта ашып оқуға қиын емес.

Сонымен, DES жүйесін аса үлкен емес және аса бағалы емес қосымшаларда деректерді шифрлау үшін пайдалануға болады. Мемлекеттік маңыздылығы бар немесе үлкен коммерциялық бағасы бар деректерді шифрлау үшін DES жүйесі қазір пайдаланбайды. 2001 жылы АҚШ-та блокты шифрдың жаңа стандарты қабылданды, ол AES (Advanced Encryption Standard) деп аталады. Оның негізінде бельгия мамандары жасаған Rijndael шифры жатыр.

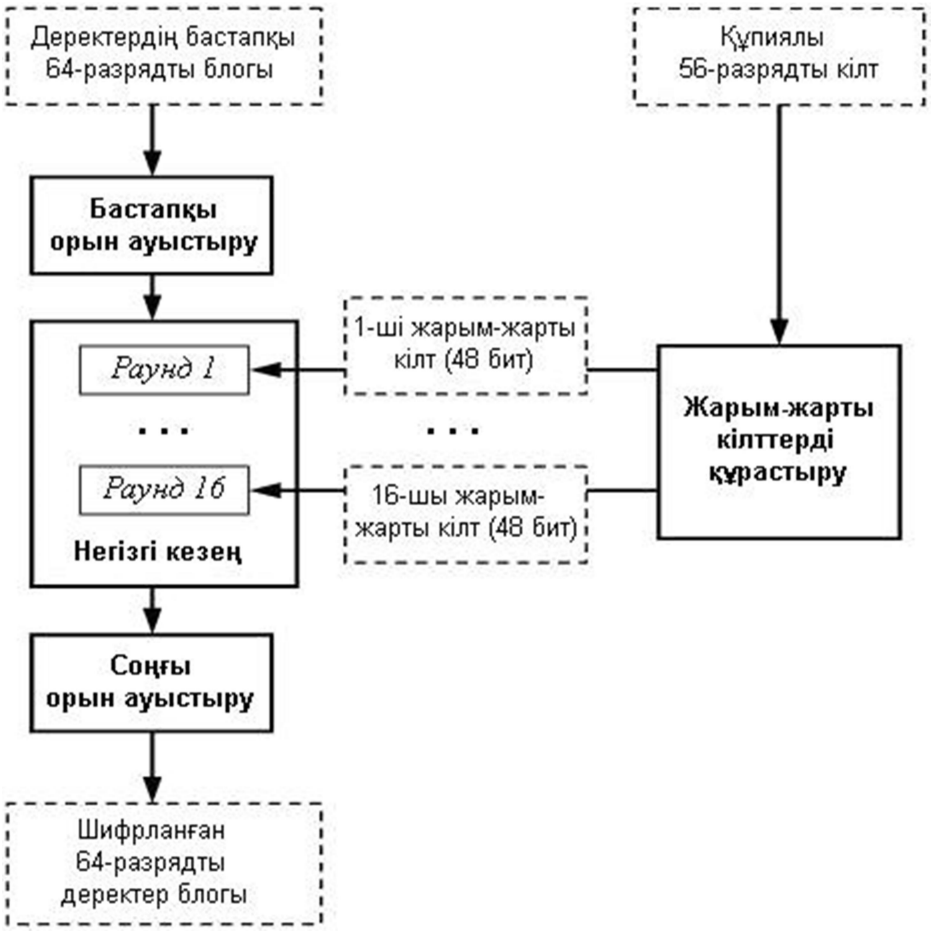
DES-ң негізгі параметрі: блок өлшемі 64 бит, кілт ұзындығы 56 бит, раунд саны – 16. DES бұл екі бұтағы бар классикалық Фейштель желісі. Алгоритм бірнеше раундта деректердің 64-битты кіру блогын 64-битты шығу блокка түрлендіреді. DES стандарты орын ауыстыруды, алмастыруды және гаммалауды араластырып пайдаланады. Шифрланатын деректер екілік түрде болу керек.

Шифрлау

DES-ң жалпы құрылымы 4.1 суретте көрсетілген. Бастапқы мәліметтердің әрбір 64-битты блоктын шифрлау процесін үш кезеңге бөлуге болады:

1. деректер блогын дайындау;
2. «негізгі циклдың» 16 раунды;
3. деректер блогының соңғы өңдеуі.

Бірінші кезеңде бастапқы мәтіннің 64-битты блогының бастапқы орын ауыстыруы орындалады, сол кезде биттер белгілі түрде қайтала реттеледі.



Сурет 4.1. DES-ң жалпы схемасы

Келесі (негізгі) кезеңде блок екі бөлшекке (бұтаққа) бөлінеді, әрбіреуі 32 бит. Оң жақ бұтағы кейбір F функцияны және сәйкес жарым-жарты кілтті пайдаланып түрлендіріледі. Жарым-жарты кілт шифрлаудың негізгі кілтінен арнайы алгоритмы бойынша алынады. Сосын блоктың сол жақ пен оң жақ бұтақтарымен деректер алмастырылады. Бұл циклда 16 рет қайталанады.

Ақырында, үшінші кезеңде негізгі циклдың он алты қадамынан кейін алынған нәтиженің орыны ауыстыралады. Бұл орын ауыстыру бастапқы орын ауыстыруға кері болады.

DES стандарты бойынша криптографиялық түрлендірудің барлық кезеңдерін толық қарап шығайық.

Бірінші кезеңде бастапқы деректердің 64-битты блогы бастапқы орын ауыстыруға душар етеді. Әдебиетте осы операцияны кейде «ағарту» - whitening деп атайды. Бастапқы орын ауыстыруда деректер блогының биты белгілі түрде қайтала реттеледі. Бұл операция бастапқы хабарға кейбір «ретсіздік» береді, сонымен статистикалық әдісі арқылы криптоталдаудың пайдалану мүмкіндігін азайтады.

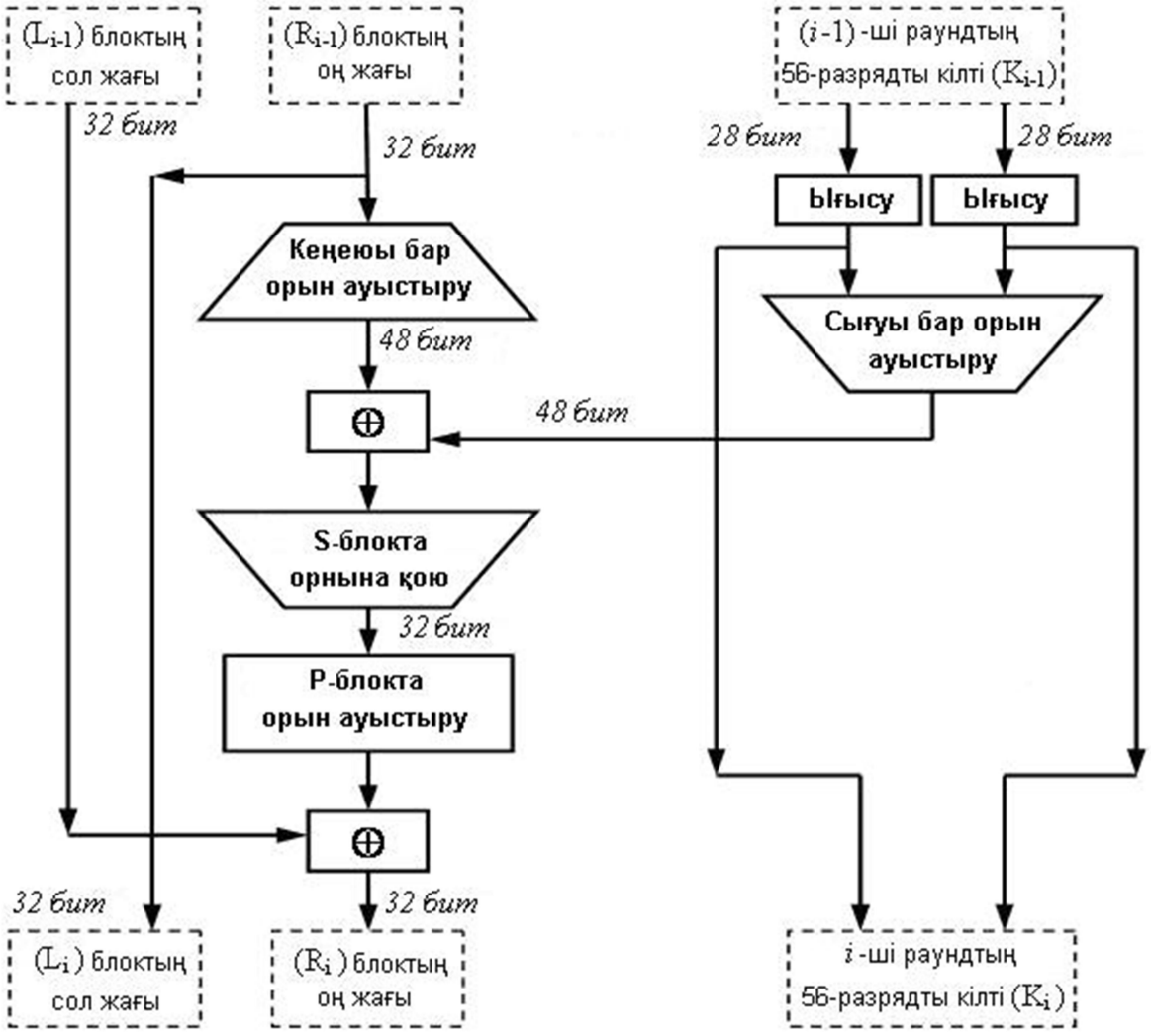
Деректер блоктың бастапқы орын ауыстыруы мен бірге кілттің 56 битын бастапқы орын ауыстыруы орындалады. 4.1 суреттен көрініп тұр, әрбір раундта сәйкес 48-битты жарым-жарты кілт K_i пайдаланады. K_i кілттер нақты алгоритм арқылы бастапқы кілттің әрбір битын бірнеше рет пайдалана отырып алынады. Әрбір раундта 56-битты кілт екі 28-битты жартыға бөлінеді. Сосын жартылар солға қарай раунд нөміріне байланысты бір не екі битқа ығысады. Ығысудан кейін белгілі бір түрде 56 биттан 48 таңдап алынады. Осы

кезде биттың бағынынқы көптігі ғана таңдап алынбай олардың реті де өзгереді, сондықтан бұл операция «сығуымен бірге орын ауыстыру» деп аталады. Оның нәтижесі 48 биттен тұратын жиынтық. Орта есеппен бастапқы 56-битты кілттің әрбір биты 16 қосалқы кілттерден 14-де пайдаланады.

Онан әрі түрлендірудің негізгі циклы орындалады. Ол Фейштель желі бойынша ұйымдастырылған және 16 бірдей раундтан тұрады. Бұл кезде әрбір раундта (сур. 4.2) аралық 64-битты мән пайда болады, ол сосын келесі раундта өңделеді.

Әрбір аралық мәннің сол жақ және оң жақ бұтағы жеке 32-битты мәні секілді өңделеді, олар белгіленген L және R.

Алдымен, орын ауыстыруды және 16 битке кеңейтуді анықтайтын кестені пайдаланып, R_i блоктың оң жағы 48 битке дейін кеңейтіледі. XOR операцияны орындау үшін бұл операция оң жақ бөліктің мөлшерін кілт мөлшеріне сәйкестіреді. Одан басқа, осы операцияның орындауынан бастапқы деректер мен кілттің биттерінен нәтиженің барлық биттерінің тәуелділігі тез күшейеді (бұл «көшкін эффектісі» деп аталады).



Сурет 4.2. DES-ң бір раундтың құрылымы

Алынған 48-битты мәні үшін кеңейюімен бірге орын ауыстыруды орындағаннан кейін, 48-битты қосалқы кілтпен K_i XOR операциясы орындалады. Сосын алынған 48-битты мәні ауыстыру блоктың S (ағыл. *Substitution* – ауыстыру, орнына қою) кіруіне беріледі, нәтижесінде 32-битты мән алынады. Ауыстыру сегіз ауыстыру блокта немесе сегіз S-блокта (S-boxes) жасалынады. Осы операция орындалғанда деректердің 48 биты

сегіз 6-битты қосалқы блокқа бөлінеді, олардың әрбіреуі төрт битпен ауыстырылады. *S*-блок көмегімен ауыстыру DES-ң ең маңызды кезеңі болып табылады. Осы операцияға максимал қауіпсіздігін қамтамасыз ету үшін ауыстыру кестелері арнайы жобаланған. Бұл кезеңнің нәтижесінде сегіз 4-битты блок пайда болады, олар қайтадан бірыңғай 32-битты мәніне бірлеседі.

Әрі қарай 32-битты мән *P* орын ауыстыру (ағыл. *Permutation* – орын ауыстыру), көмегімен өңделеді, ол пайдаланатың кілтке тәуелді болмайды. Орын ауыстырудың мақсаты - келесі шифрлау раундта әрбір бит басқа *S*-блокпен өңделсін деп биттерді максимал қайта реттеуі.

Ақырында, орын ауыстыру нәтижесі XOR операция көмегімен бастапқы 64-битты деректер блоктың сол жақ жартысымен бірлеседі. Сосын сол жақ және оң жақ жартылары орнымен алмасады, және келесі раунд басталады.

Он алты шифрлау раундтан кейін нәтиженің соңғы орын ауыстыруы орындалады. Бұл орын ауыстыру бастапқы орын ауыстыруға инверсты (кері).

Барлық көрсетілген қадамдарды орындағаннан кейін деректер блогы толық шифрланған деп есептеледі және бастапқы хабардың келесі блогын шифрлауға болады.

Сонымен, қағаздағы DES-ң жай бейнелеуі ғана күрделі болып көрінеді, ал оның бағдарламалық жүзеге асыруы одан да қиын!

Дешифрлау (ашып оқу)

Криптографиялық жүйе хабарларды шифрлау мен бірге дешифрлауға да мүмкіндік беру керек. DES бойынша ашып оқу процесі өте шиеленген деп күтуге болар еді. Бірақ құрастырушылар шифрлау мен дешифрлау үшін бірдей алгоритмды пайдаланады. Ашып оқу кезінде алгоритмның кіруіне шифрланған мәтін беріледі. Бір ғана айырмашылық жарым-жарты кілттерді K_i кері ретпен пайдалану. K_{16} бірінші раундта пайдаланады, K_1 – соңғы раундта.

Ашып оқудың соңғы раундынан кейін шығудың екі жартысы орындарымен алмасады, аяқтау орын ауыстырудың кіруі R_{16} мен L_{16} құрастырған болатындай. Бұл сатының шығуы ашық мәтін.

4.2 Екі еселі DES және «ортада кездесу» шабуыл

Қазіргі уақытта DES-ң негізгі кемшілігі кілттің кішкене ұзындығы. Криптоталдауды күрделендірудің ең қарапайым тәсілі әртүрлі кілттермен бірдей алгоритм көмегімен екі еселі шифрлауды пайдалану.

Егер M – хабар, K_1, K_2 – кілт, f – DES бойынша шифрлау процесі, ал E – шифрланған хабар болса, онда жазуға болады

$$E = f(f(M,K)),$$

яғни алдымен блок бір кілтпен шифрланады, сосын алынған шифрмәтін екінші кілтпен шифрланады.

Дешифрлау кері ретпен жүргізіледі (f^{-1} – DES бойынша ашып оқу):

$$E = f^{-1}(f^{-1}(E,K_2),K_1)$$

Бұл жағдайда кілт ұзындығы тең 56 2 = 112 бит, сондықтан блокты шифрлаған екі есе кілтті табу үшін жалпы 2^{112} әрекет қажет болады.

Осы проблеманы зерттеп американ ғалымдары Меркл мен Хеллман ашық мәтін арқылы шабуылдың тәсілін ойлап тапты, оған 2^{112} емес 2^{57} әрекет қажет.

Шабуылдың бұл варианты «ортада кездесу» деп аталады. Ол алгоритмның келесі қасиетіне негізделген. Бізде болсын

$$E = f(f(M,K_1),K_2)$$

мұндағы M – хабар, K_1, K_2 – кілт, f – DES бойынша шифрлау процесі, ал E – шифрланған хабар.

Онда $X = f(M, K_1) = f^{-1}(E, K_2)$.

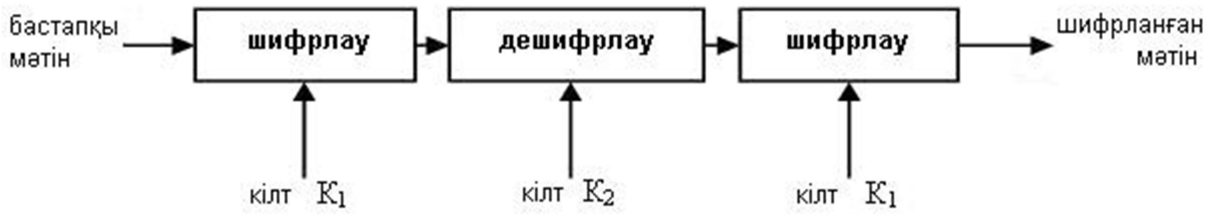
Шабуылдың маңызы мынада. Шабуыл жасаушы бірнеше «ашық мәтін – оған сәйкес шифрланған мәтін» жұптарды (*M*, *E*) білу керек. Мұнда алдымен барлық 2^{56} мүмкін болатын K_1 мәні үшін *M* шифрланады. Осы нәтиже ЭЕМ-ң жадында сақталынады. Сақталынған мәліметтер *X* мәні бойынша реттеледі. Келесі қадам - барлық 2^{56} мүмкін болатын K_2 мәнің қолданып *E*-ны дешифрлау. Әрбір орындалған дешифрлау үшін бірінші кестеден оған тең мән ізделінеді. Егер осындай мән табылса, онда бұл кілттер дұрыс деп есептеледі, сосын олар келесі белгілі жұпта тексеріледі. Шифрлаудың максимал әрекеттер саны тең $2 \cdot 2^n$, немесе 2^{n+1} (мұнда *n* – әрбір шифрлау кезеңдегі кілт ұзындығы; DES үшін *n* тең 56).

«Ортада кездесу» деп қойылған аттың себебі: бір жағынан шифрлау орындалады, екінші жағынан – дешифрлау, және ортада алынған нәтижелер салыстырылады.

«Ортада кездесу» шабуылды өткізу үшін жадтың үлкен көлемі қажет: 2^n блок (мұнда *n* – кілт ұзындығы). 56-битты кілтті пайдаланатын DES үшін 2^{56} 64-разрядты жад блогы қажет болады. Бұл 2^{62} байт немесе 2^{22} Тбайт. Осыған қарамастан, екі еселі DES ешқашан пайдаланбады.

4.3 Үш еселі DES

«Ортада кездесу» шабуылға қарсы әрекет жасау мақсатымен екі кілтпен үш еселі шифрлауды ұсынды (сур. 4.3).



Сурет 4.3. Екі кілтпен үш еселі DES шифрлауы

Бұл жағдайда шифрлау-дешифрлау-шифрлау тізбегі орындалады (EDE – ағыл. *Encrypt - Decrypt - Encrypt*). Осы процесті былай көрсетуге болады:

$$E = f(f^{-1}(f(M, K_1), K_2), K_1)$$

Жіберуші алдымен хабарды бірінші кілтпен шифрлайды, сосын екінші кілтпен дешифрлайды және ақырында, біржолата біріншімен шифрлайды. Алушы алдымен бірінші кілтпен дешифрлайды, сосын екінші кілтпен шифрлайды және қайтадан біріншімен дешифрлайды. Осында кілт ұзындығы екі есе өседі және 112 бит болады.

Оған сенімдірек балама ретінде әрбір кезеңде үш әртүрлі кілтті пайдаланатын үш еселі шифрлау әдісі ұсынылады. Осындай әдісте кілттің жалпы ұзындығы өседі (112+56=168), сонда бірнеше жүздеген битты сақтау әдетте қиын емес.

Үш еселі DES кең тараған балама болып саналады және кілтті басқаруда ANSI X9.17, ISO 8732 және ISO 8732 стандарттарда пайдаланады. Кейбір криптоталдаушылар одан ары сенімді шифрлау үшін үш немесе бес кілтпен бес еселі DES-ң пайдалануын ұсынады.

4.4 Rijndael алгоритмы

Rijndael алгоритмды («Рейндал» деп оқылады) бельгияның мамандары Joan Daemen (Proton World International) және Vincent Rijmen (Katholieke Universiteit Leuven) жасаған болатын. Бұл шифр АҚШ-та AES (Advanced Encryption Standard) атағын алу үшін конкурста жеңді және 2001 жылы жаңа американ стандарты ретінде қабылданды. Rijndael

алгоритмды бейнелеу оңай емес, сондықтан тек негізгі құру аспектілерін және пайдалану ерекшелігін қарастырайық.

Rijndael / AES шифры (яғни ұсынылатын стандарт) 128 битты блокпен, кілт ұзындығымен 128, 192 немесе 256 бит және кілт ұзындығына тәуелді раундтар санымен 10, 12 немесе 14 сипатталады. Rijndael құрылымын 32-ге еселі блок пен кілттің түрлі мөлшеріне лайықтауға болады және раунд санын өзгертуге болады.

DES пен ГОСТ 28147-89 ұсынатын шифрларға қарағанда Rijndael негізінде Фейштель желісі жатпайды. Rijndael негізінде сызықты-ауыстырылу деп аталатын түрлендіру жатыр. Деректер блогы байттар массивтерге бөлінеді, және әрбір шифрлау операциясы байт-бағытталған болып табылады. Әрбір раунд үш әртүрлі қайтымды түрлендіруден тұрады, оларды қабаттар деп атайды. Бұл қабаттар келесі.

1. Сызықты емес қабат. Бұл қабатта байттар ауыстыруы орындалады. Қабат тиімді сызықты еместігі бар *S*-блоктар көмегімен жүзеге асырылған, және дифференциал, сызықтық және басқа криптоталдау әдістерінің пайдалану мүмкіндігін болдырмайды.

2. Сызықтық араластыру қабаты статистикалық байланысты жасыру үшін блок символдарының өзара ішіне кіруінің жоғары дәрежесін кепілдейді. Бұл қабатта тікбұрышты байт массивінде массив жолдарының ығысуы мен бағандардың орын ауыстыруы орындалады.

3. Қосалқы кілті бар модуль 2 бойынша қосу қабаты шифрлауды тікелей орындайды.

Шифр кілтпен қосуымен басталады және аяқталады. Бұл белгілі мәтін арқылы шабуыл кезінде бірінші раундтың кіруін жабады және соңғы раундтың нәтижесін криптографиялық маңызды болып істейді.

Алгоритмда кестелік есептер кең пайдаланады, барлық қажетті кестелер тұрақты түрде беріледі, яғни не кілтке не деректерге тәуелді емес.

Айта кетейік, Фейштель желі бойынша құрастырылған шифрларға қарағанда, Rijndael-да шифрлау мен дешифрлау функциялары әртүрлі.

Rijndael алгоритмы бағдарламалық та аппараттық та жүзеге асыруда жақсы орындалады. Rijndael-да жадқа қойылатын талаптары аса жоғары емес, сондықтан оны шектелген ресурстары бар жүйеде пайдалануға болады. Rijndael алгоритмның сенімділігі өте жоғары.

4.5 Блокты алгоритмдердің жұмыс тәртіптері

Блокты шифрлар әртүрлі есептерді орындау үшін пайдалану мүмкін. Сондықтан, түрлі симметриялық блокты шифрлау алгоритмы үшін оның бірнеше қолдану тәртібі анықталған. Әрбір тәртіптің өз ерекшелігі мен қолдану саласы бар.

Кейбір блокты шифр бар болсын, ол *K* кілт көмегімен бастапқы *X* деректер блогының *Y* шифрланған блоққа *f* түрлендіруін орындайды:

$$Y = f(X, K)$$

Түрлендіру *f*-ң кейбір мүмкін болатын орындау тәртіптерің қарап шығайық.

Ең қарапайым тіртібі **қарапайым блокша ауыстыру тәртібі**. Мамандар бұл тәртіпті **ECB - Electronic CodeBook** деп атайды (аудырылады – электронды код кітабі). Осы тәртіпте бастапқы деректердің әрбір блогы бірдей кілтті пайдаланып басқа блоктарға тәуелсіз шифрланады. Егер хабар блок ұзындығынан артық болса, онда ол сәйкес ұзындығы бар X_1, X_2,..., X_n блоктарға бөлінеді. Керек болса соңғы блок тіркелген мәндірімен толтырылады. Әрбір блок блокты шифрмен шифрланады:

$$Y = f(X_i, K) \text{ барлық 1-ден } n\text{-ға дейін } i \text{ үшін}$$

Бастапқы X_i деректер блоктарының шифрлау нәтижесінде шифрланған хабар $Y = Y_1, Y_2,..., Y_n$ алынады.

Дешифрлау мына ереже бойынша орындалады

$$X = f^{-1}(Y_i, K) \text{ барлық 1-ден } n\text{-ға дейін } i \text{ үшін}$$

ECB тәртіптің анықтамасынан шығады, хабардың ашып оқуын шифрмәтін блоктарын ретсіз түрде таңдап жүргізуге болады. Осындай тәртіп көп нақты жағдайларда ыңғайлы. Мысалы, ECB тәртібінде шифрланған деректер базамен жұмыс істеуге болады, егер оның әрбір жазуы жеке деректер блогы болса және басқалардан жеке шифрланған болса.

Осы тәртіптің кемшілігі - бастапқы мәтіннің бірдей блоктары бірдей шифрмәтінге түрлендіріледі. Нақты шифрланатын деректер жиынтықтарда қайталанатын элементтер жиі кездеседі. Хабарларда жоғары артықшылығы болу мүмкін: қайталанатын бастары және аяқтары немесе нөлдер мен ақ жолдарының ұзын сериясы. Сонымен, қарсыластын қолына жиілік талдауды жүргізу үшін мәліметтер түсу мүмкін. Және де қарсылас алушыны алдау үшін шифрланған хабарды өзгерту немесе ауыстыру мүмкін.

Толығымен, ECB тәртібі бөлек қысқа хабарларды (мысалы, криптографиялық кілтті) беру үшін пайдалануға ұсынылады.

Бірнеше деректер блоктарын бергенде ECB-ң кемшіліктерін жою үшін келесі тәртіп ұсынылады **CBC (Chipher Block Chaining)** – **шифр блоктарын тіркелу тәртібі**.

CBC тәртіпте түрлендіру былай жүргізіледі: ашық мәтіннің әрбір блогы модуль 2 бойынша бұрынғы блоктың шифрлау нәтижесімен қосылады. Сонымен, бұрынғы блоктарының шифрлау нәтижелері келесі блоктардың шифрлауына әсер етеді. CBC тәртіпте шифрлау операциясы математикалық түрде келесі формуламен сипатталады:

$$Y = f((X_i \oplus Y_{i-1}), K) \quad \text{барлық 1-ден } n\text{-ға дейін } i \text{ үшін}$$

Яғни келесі блоктың шифрлауының алдында ашық мәтін үстіне және бұрынғы блоктың шифрлау нәтижесінің үстіне «модуль 2 бойынша қосынды» деген операция орындалады. Ашық мәтін блогы шифрланғаннан кейін, ол шифраушы құрылғының жадында сақталынады, мысалы, кері байланыс регистрде. Келесі деректер блогын шифрлаудын алдында, ол кері байланыс регистрмен бірге «модуль 2 бойынша қосынды» операцияға душар болады және осыдан кейін ғана шифрланады. Алынған шифрланған блок қайтадан кері байланыс регистрде сақталынады және келесі кіру деректер блокты шифрлауда пайдаланады, және әрі қарай хабардың аяғына дейін. Y_0 блогы бастапқы деректердің бірінші блогын шифрлауының алдында құрастырылу қажет. Ол *инициализациялау векторы* деп аталады және кіру деректердің бірінші блогымен модуль 2 бойынша қосу үшін пайдаланылады.

Кері байланысты пайдалану нәтижесінде әрбір блоктын шифрлауы барлық бұрыңғы блоктарға тәуелді болады.

Шифрланған хабарды келесі түрде ашып оқуға болады:

$$X_i = Y_{i-1} \oplus f^{-1}(Y_i, K) \quad \text{барлық 1-ден } n\text{-ға дейін } i \text{ үшін}$$

Шифрмәтін блогы алдымен кері байланыс регистрде сақталынады, сосын әдеттегідей дешифрланады. Онан әрі келесі блок дешифрланады және кері байланыс регистрмен «модуль 2 бойынша қосынды» операцияға душар болады. Осылай хабардын аяғына дейін орындалады.

Егер бастапқы X_i деректердің барлық блоктары ұқсас болса да, шифрмәтін әртүрлі Y блоктан тұрады. Бұл тәртіпті блок мөлшерінен артық болатын хабарларды шифрлауға жөн. Бірақ, екі бірдей хабар бірдей де шифрланады. Осыны болдырмау үшін әрбір шифрлауда әртүрлі инициализациялау векторын пайдалану қажет. Инициализациялау векторы деректерді ашып оқу үшін де қажет, сондықтан оларды не шифрланған хабармен бірге адресатқа жіберу керек не кездейсоқ тәріздес инициализациялау векторын адресатпен бірге құрастыру керек.

CBC тәртіпте шифрланған хабарды, тек бірінші блоктан бастап рет-ретімен ашып оқуға болады.

Негізгі ұғымдар

AES (Advanced Encryption Standard) – АҚШ-та 2001 жылдан деректерді шифрлау облыста мемлекеттік стандарт ретінде пайдаланатын шифрлау алгоритмы. Стандарт негізінде Rijndael шифры жатыр. Rijndael / AES шифры (яғни ұсынылатын стандарт) 128 битты блокпен, кілт ұзындығымен 128, 192 немесе 256 бит және кілт ұзындығына тәуелді раундтар санымен 10, 12 немесе 14 сипатталады. Rijndael негізін сызықты-ауыстырылу деп аталатын түрлендірулер құрайды. Rijndael құрылымын 32-ге еселі блок пен кілттің түрлі мөлшеріне лайықтауға болады және раунд санын өзгертуге болады. Алгоритмда кестелік есептер кең пайдаланады, барлық қажетті кестелер тұрақты түрде беріледі, яғни не кілтке не деректерге тәуелді емес.

DES (Data Encryption Standard) – АҚШ-та 1977 жылдан 2001 жылға дейін деректерді шифрлау облыста мемлекеттік стандарт ретінде пайдаланған шифрлау алгоритмы. DES-ң негізгі параметрі: блок өлшемі 64 бит, кілт ұзындығы 56 бит, раунд саны – 16. DES бұл екі бұтағы бар классикалық Фейштель желісі. Алгоритм бірнеше раундта деректердің 64-битты кіру блогын 64-битты шығу блокка түрлендіреді. DES стандарты орын ауыстыруды, алмастыруды және гаммалауды араластырып пайдаланады.

Құрастырылған (композициялық) шифр - бірнеше қатарынан пайдаланған қарапайым шифрлардың комбинациясы нәтижесінде деректердің криптографиялық түрлендіруі.

ECB (Electronic CodeBook) тәртібі – блокты шифрлау алгоритмның пайдалану тәртібінің біреуі. Аудырылады – электронды код кітабі – бұл қарапайым блокша ауыстыру тәртібі. Осы тәртіпте бастапқы деректердің әрбір блогы бірдей кілтті пайдаланып басқа блоктарға тәуелсіз шифрланады. Егер хабар блок ұзындығынан артық болса, онда ол сәйкес ұзындығы бар блоктарға бөлінеді. Керек болса соңғы блок тіркелген мәндірімен толтырылады. ECB тәртібі бөлек қысқа хабарларды (мысалы, криптографиялық кілтті) беру үшін пайдалануға ұсынылады.

CBC (Chipher Block Chaining) тәртібі – шифр блоктарын тіркелу тәртібі. Блокты шифрлау алгоритмның пайдалану тәртібінің біреуі. CBC тәртіпте түрлендіру былай жүргізіледі: ашық мәтіннің әрбір блогы модуль 2 бойынша бұрынғы блоктың шифрлау нәтижесімен қосылады. Сонымен, бұрынғы блоктарының шифрлау нәтижелері келесі блоктардың шифрлауына әсер етеді.

Сұрақтар

1. Қандай шифр құрастырылған немесе композициялық шифр деп аталады?
2. Блокты шифрлау алгоритмның беріктігіне қандай факторлар әсер етеді?
3. Фейштель желісі деген не?
4. Симметриялық шифрлау DES, AES алгоритмдардың негізгі параметрлерін атып беріңіз.
5. Блокты шифрлау DES, AES алгоритмда қандай операциялар пайдаланады?
6. «Ортада кездесу» шабуыл деген не?
7. Үш еселі DES-ты пайдалану принципі қандай?
8. Қарапайым ауыстыру тәртібінде (ECB) блокты шифрлау алгоритмы қалай пайдаланады?
9. ECB тәртібінің кемшіліктері қандай?
10. Шифр блоктарын тіркелу тәртібінде шифрлау алгоритмның пайдалану ерекшелігі қандай?
11. CBC тәртібінің кемшіліктері қандай?

Әдебиеттер:

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2. Гафнер В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
5. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.