ISSN 1728-7901

Абай атындағы Қазақ ұлттық педагогикалық университеті
Казахский национальный педагогический университет имени Абая
Abai Kazakh National Pedagogical University

ХАБАРШЫ

«Физика-математика ғылымдары» сериясы
Серия «Физико-математические науки»
Series of Physics & Mathematical Sciences
№1(69)

Алматы, 2020

Абай атындағы Қазақ ұлттық педагогикалық университеті

ХАБАРШЫ
«Физика-математика ғылымдары» сериясы № 1 (69), 2020 ж.

Қазақстан Республикасының Ақпарат министрлігінде тіркелген
№ 4824 – Ж - 15.03.2004
(Журнал бір жылда 4 рет шығады)
2000 жылдан бастап шығады

Басуға 10.03.2020 ж. қол қойылды
Пішімі 60x84 $^1/_8$. Көлемі 57,3 е.б.т.
Таралымы 300 дана. Тапсырыс 256.

050010, Алматы қаласы,
Достық даңғылы, 13
Абай атындағы ҚазҰПУ-ің“Ұлағат” баспасы

М а з м ұ н ы
С о д е р ж а н и е

МАТЕМАТИКА. МАТЕМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ

МАТЕМАТИКА. МЕТОДИКА ПРЕПОДАВАНИЯ МАТЕМАТИКИ

Казахский национальный педагогический университет имени Абая

ВЕСТНИК
Серия «Физико-математические науки»
№ 1 (69), 2020 г.

Зарегистрирован в Министерстве информации
Республики Казахстан,
№ 4824 - Ж - 15.03.2004
(периодичность – 4 номера в год)
Выходит с 2000 года

Подписано в печать 10.03.2020 г.
Формат 60x84 $^1/_8$. Об. 57,3 уч.-изд.л.
Тираж 300 экз. Заказ 256.

050010, г. Алматы, пр. Достык, 13,
Издательство «Ұлағат» КазНПУ им. Абая

ФИЗИКА. ФИЗИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ

ФИЗИКА. МЕТОДИКА ПРЕПОДАВАНИЯ ФИЗИКИ

ABAI UNIVERSITY

BULLETIN
Ser. Physics & Mathematical Sciences

№ 1 (69)
Editor-in-Chief
Dr. Sci. **Bektemesov M.A.**

Deputy Editor-in-Chief:
Dr. Sci. **Ualiyev G.,**
Dr. Sci. (Ped.), **Bidaibekov Ye.Y.,**
Dr. Sci., Corresponding member of the NAS of RK **Kosov V.N.,**
Cand.Sci. **Bekpatshayev M.Zh.**

Responsible editorial secretary:
Cand. Sci. (Ped.) **Shekerbekova Sh.**
Cand. Sci. (Ped.) **Abdulkarimova G.A.**

***Editorial board*:**
Dr.Sci. **Alimhan K.** (Japan),
Phd.d. **Cabada A.** (Spain),
Phd.d **Kovatcheva E.** (Bulgaria),
Phd.d. **Ruzhansky M.** (England),
Dr. Sci. (Ped.), Corresponding member of the NAS of RK **Abylkasymova A.Ye.,**
Dr.Sci.(Engineering) **Amirgaliyev Ye.,**
Dr. Sci. **Berdyshev A.S.**
Dr.Sci. **Grigoriev S.G.** (Russia),
Dr.Sci. **Grinshkun V.V.** (Russia),
Dr. Sci. **Mukhambetzhanov S.T.,**
Dr.Sc. **Kabanikhin S.I.** (Russia),
Dr. Sci., Academician of the NAS of RK **Kalimoldayev M.N.,**
*Dr. Sci.***Kozhamkulov B.A.,**
Dr. Sci. **Komarov F.F.,**
(Republic of Belarus),
Dr.Sci.(Engineering) **Kulbek M.K.,**
Dr. Sci. (Ped.) **Lapchik MP** (Russia),
Dr. Sci.**Lisicin V.M.** (Russia),
Dr. Sci. (Ped.) **Mambetakunov E.M.**
(Kyrgyz Republic),
Dr. Sci. (Ped.) **Pak N.I.** (Russia),
Dr.Sc. **Sakhiev S.K.,**
Dr. Sci. (Ped.) **Sedova Ye.A.** (Russia),
Dr. Sci. (Ped.) **Sydykov B.D.,**
Dr.Sci.(Engineering) **Tuleshov A.K.,**
Dr.Sci. **Ualiyev Z.G.,**
Cand.Sci. **Khamraev Sh.I.**

Registered in the Ministry of Information of the Republic of Kazakhstan,
№ 4824 - Ж - 15.03.2004
(Periodicity: 4 issues per year)
Published since 2000

Signed to print 10.03.2020 г.
Format 60x84 1/8. Vol. 57,3 p.
Printing 300 copies. Order 256.

Publishing and Editorial:
050010, 13 Dostyk av.,
Almaty, Kazakhstan
Publisher "Ulagat"
Abai University

ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ. БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ. ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ

Экономикалық – экономикалық жағынан елге, халыққа пайдалы жағы;
Қоршаған орта – табиғатты қорғау немесе зиян келтірмеу жақтарына үлес қосу;
Саяси – дамыған мемлекеттердің қатарына қосылып, беделімізді, саяси мүмкіндігімізді арттыру;
Құқықтық – заңдағы жаңашылдықтарды, құқықтар мен міндеттерді білу;
Этникалық – ұлттық құндылықтарды жаңғырту деген ойлар туындады [5].

Кейстер әдісі

1. Проблеманы анықтау
2. Шешудің жолдарын іздестіру
3. Шешу жолдары бойынша салдарын болжау
4. Ең тиімді жолын таңдап алу

Бұл әдіс арқылы мұғалімдер мен ғалымдар туындаған мәселенің шешу жолдары мен проблемаларын анықтап, ортақ пікірге келді.

Қорытындылай келе, жаратылыстану бағыты бойынша 10-11 сыныптарда информатика пәнін оқыту жаңартылған мазмұндағы жаңа әдіс-тәсілдерді қамти отырып өткізілуі тиіс. Нәтижесінде оқушы алған білімін өмірде пайдалана алуы керек деп есептеймін. Информатика пәні бойынша оқытылатын тақырыптар оқушыға түсінікті, анық және нақты болған жағдайда ғана оқыту мен оқудағы нәтижеге қол жеткізе аламыз. Оқудың табыстылығы пәннің ерекшелігіне сәйкес жүйелі түрде тиімді әдістерді таңдай білетін ұстаздың шеберлігі мен құзіреттілігіне байланысты болатыны анық.

Сөзімнің соңында Махатма Гандидің мына сөзімен аяқтағым келіп тұр: «Егер сен болашақты өзгерткің келсе – ол өзгерісті өз уақытында жаса» деген екен. Бүгінгі таңда еліміздің білім беру жүйесіндегі оқыту мен оқудағы білім мазмұнын жаңарту жағдайында болып жатқан үлкен өзгерістер еліміздің болашағына, оны жүзеге асыруда еңбек етіп жүрген Біз бен Сіздерге толағай табыстар әкелетініне сенемін.

Пайдаланылған әдебиеттер тізімі:

1 Қазақстан Республикасының Білім туралы заңы.- Астана, 2000.
2 Қ.Р. Білім беруді дамытудың 2011-2020 жылдарға арналған мемлекеттік бағдарламасы. – Астана, 2010 – 6 б.
3 Абдуллина Г. Интерактивті оқыту таным белсенділігінің қазіргі бағыты // Ұлт тағылымы. - №2 - 2009 - 36-39б.
4 «Жаратылыстану пәндерін оқытудағы интербелсенді әдістер» Әдістемелік құрал / Құраст. Картабаева Д.А., Каракушекова Ф.Н. – Алматы, 2017. -104 б.
5 Сындарлы оқыту-сапалы білім бастауы: (деңгейлік курс білім алушыларының іс тәжірибесінен) - Алматы, 2013 – 170 б.

МРНТИ 50.41
УДК 004.054

Ф.Р. Гусманова[1], Г.А. Абдулкаримова[2]

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[2] Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан

БЛОКТЫҚ ШИФРЛАУДЫҢ ДАМУЫНА ШОЛУ

Аңдатпа

Жаппай ақпараттандыру жағдайында ақпараттық қауіпсіздік пен ақпаратты қорғау проблемасы өзекті болып тұр. Жұмыста блоктық шифрлаудың дамуына шолу жасалған. Блоктық шифр - симметриялы шифрдың бір түрі. Блок шифрінің ерекшелігі - бірнеше байттан тұратын блокты бір итерацияда өңдеу. Блок криптожүйелері хабарлама мәтінін бөлек блоктарға бөліп, кілтті қолдана отырып, осы блоктарды түрлендіреді. Блоктық шифрлауға қатысты базалық ақпарат келтірілген, талдаудың негізгі нұсқалары көрсетілген. Осы тақырып бойынша білім алушылардың ғылыми-зерттеу жұмысымен айналысуға мүмкіндік бар екені негізделген. Блоктық шифрларды зерттеу бойынша халықаралық конкурстарға шолу жасалынған.

Электроникада қолдануға болатын сұлба келтірілген, ал программалау үшін да генерациялайтын алмастыру кестесі генерацияланды және ашылып жазылды. Осы екі тәсіл де эквивалент болып табылғандықтан, компьютерде шифрланған файлдың электрондық құрылғыда шифрын ашуға болады және керісінше.

Түйін сөздер: ақпараттық қауіпсіздік, криптожүйе, криптографиялық алгоритм, кілт, қорғау.

Аннотация

Ф.Р. Гусманова[1], Г.А. Абдулкаримова[2]
[1] Казахский национальный университет им. аль-Фараби, г. Алматы, Казахстан
[2] Казахский национальный педагогический университет им. Абая, г. Алматы, Казахстан

ОБЗОР РАЗВИТИЯ БЛОЧНОГО ШИФРОВАНИЯ

В условиях всеобщей информатизации, существенно обострилась проблема информационной безопасности и защиты информации. В работе дан обзор развития блочного шифрования. Блочный шифр является разновидностью симметричного шифра. Его особенностью является обработка за одну итерацию блока нескольких байт. Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа. Представлена базовая информация, касающаяся блочного шифрования, показаны основные варианты анализа. Отмечена возможность научно-исследовательской работы студентов по данной тематике, выполнен обзор международных конкурсов по исследованию блочных шифров. Приведена схема, которую можно применить в электронике, а для программирования генерирована и расписана таблица замены. В данном случае оба этих подхода являются эквивалентными, это означает, что зашифрованный файл на компьютере, расшифровывается на электронном устройстве и наоборот.

Ключевые слова: информационная безопасность, криптосистема, криптографический алгоритм, ключ, защита.

Abstract

OVERVIEW OF THE BLOCK ENCRYPTION DEVELOPMENT

Gusmanova F.R. [1], Abdulkarimova G.A. [2]
[1] Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

In the conditions of universal Informatization, the problem of information security and information protection has significantly worsened. This work provides an overview of the block encryption development. Block cipher - a kind of symmetric cipher. A feature of the block cipher is the processing of a block of several bytes in one iteration. Block cryptosystems break the message text into separate blocks and then convert these blocks using a key. Basic information related to block encryption is presented, and the main analysis options are shown. The possibility of students' research work on this topic was noted, and the review of international competitions on block ciphers research was performed.

A diagram is shown that can be applied in electronics, and a replacement table is generated and painted for programming. In this case, both of these approaches are equivalent, meaning that an encrypted file on a computer is decrypted on an electronic device and vice versa.

Keywords: information security, cryptosystem, cryptographic algorithm, key, protection.

Кіріспе

Ғаламтордың кеңінен тарауымен байланысты ақпаратты жіберу мәселесі едәуір жеңілдеді, әйтсе де, жіберушіден алушыға жету жолында оны қорғау мәселелерінің қажеттілігі артуда. Блоктық шифрлар бекітілген ұзындықтағы биттер тізбегі (нөлдер мен бірлерден тұратын) түрінде берілген ашық мәтінді блок бойынша түрлендіреді [1].

1971 жылы Хорест Фейстель шифрлаудың әр түрлі алгоритмдерін жүзеге асыратын екі құрылғыны патенттеді, кейіннен ол «Люцифер» (ағылш. *Lucifer*) деп аталды [2]. Осы құрылғылардың бірі кейіннен «Фейстель» желісі (ағылшл. *Feistel cipher, Feistel network*) деп аталған құрылғыны пайдаланды. Сол кезде Хорест Фейстель Дон Копперсмитпен бірге IBM-де жаңа криптожүйелерді құрумен айналысты. «Люцифер» жобасы тәжірибелік болды, бірақ содан кейін DES (ағылш. *Data **e**ncryption **s**tandard*) алгоритмі үшін негізі болды. 1973 жылы «Scientific American» журналында Фейстельдің «Криптография және желілік қауіпсіздік» мақаласы жарияланды. Мақалада шифрлаудың кейбір маңызды аспектілері ашылды және «Люцифер» жобасының бірінші нұсқасының сипаттауы келтірілді. «Люцифер» жобасының бірінші нұсқасында Фейстель жүйесі пайдаланылған жоқ.

Уитфилд Диффи мен Мартин Хеллманның «Криптографиядағы жаңа бағыттар» (1976 ж.) мақаласы криптографиялық жүйелерде революция туғызды және ашық кілтті криптографияның негізін салды. Кейіннен әзірленген Диффи-Хеллман алгоритмі екі жаққа да ортақ қауіпсіз байланыс каналы бойынша құпия кілтті алуға мүмкіндік жасады. Әйтсе де, бұл алгоритм аутентификациялау проблемасын шеше алмады. Пайдаланушылар қосымша ресурстарсыз ортақ құпия кілтті кіммен генерациялайтынына сенімді бола алмайды. Осы мақаланы толығымен талдағаннан кейін Массачусет технологиялық институтының оқымыстылары Рональд Ривест, Ади Шамир және Леонард Адлеман ашық кілті бар криптографиялық жүйелер моделін жүзеге асыру мүмкіндігі бар математикалық функцияны іздеуге кірісті. 40 мүмкін нұсқаларды қарастырып, олар үлкен жай сандарды табу қарапайымдылығы мен екі үлкен жай сандардың көбейтіндісін көбейткіштеріне жіктеу күрделілігінің арасындағы

айырмашылыққа негізделген, кейіннен RSA деп аталған алгоритмді тапты. Жүйе осы алгоритмді құрушылардың аттарының бірінші әріптерінен құралған аббревиатурамен аталды [3].

DES 56-биттік кілтті қабылдады, дегенмен есептеу техникасының дамуымен 2^{56} өлшемінен асып кетті және DES қабылдаушы ны таңдау үшін RSA компаниясымен жоба қарастырылды. Сонымен қатар, DES архитектурасы аппараттық жүзеге асырылуға бағытталған, ал шектеулі ресурстармен берілген платформаларда алгоритмдерді жүзеге асыру қажетті өнімділікті қамти алмайды. Rijndael шифры – блоктарды шифрлаудың симметриялы алгоритмі (блок өлшемі – 128 бит, кілт 128/192/256 бит) конкурста жеңіске жетті. Конкурстың атымен байланысты оны көбінесе AES (Advanced Encryption Standard) деп атайды.

Заманауи блоктық криптожүйелер программалық және программалық-аппараттық жүзеге асыру әдістеріне бағытталған. Блоктық криптожүйелер блоктық (топтық) шифртүрлендірулерді береді. Блоктық шифрлар биттермен үлкен көлемдегі манипуляциялардан алыстауға мүмкіндік беретіндіктен және компьютерге ыңғайлы мәліметтер блоктарымен амалдар орындауға болатындықтан олар ағындық шифрларға қарағанда жеңіл жүзеге асырылады.

Блоктық шифрлар ақпараттың бүтін блоктарын (4-тен 32 байтқа дейін) бір тұтас ретінде шифрлайды – бұл толық іріктелетін шабуылға түрлендіру беріктігін едәуір арттырады және әр түрлі математикалық және алгоритмдік түрлендірулерді пайдалануға мүмкіндік береді.

Блоктық криптожүйе М ашық мәтінді M_1, . M_2, ... блоктар тізбегіне бөледі және әрбір блокты K кілтінің көмегімен бір қайтымды E_k түрлендіруінің көмегімен шифрлайды: $E_k(M) = E_k(M_1), E_k(M_2)$. Олардың кез келгенін кілт элементтерімен және ашық мәтінмен, сонымен қатар олардың шамаларының туындыларымен жүргізілетін операциялар тізбегі ретінде қарастыруға болады.

Шифрлау алгоритм элементтерін таңдау жеткілікті түрде көп, әйтсе де, «элементар» операциялар жақсы криптографиялық қасиеттерді меңгерулері керек және ыңғайлы техникалық және программалық жүзеге асыруға мүмкіндік беруі керек. Негізінен келесі операциялар пайдаланылады:

- екілік векторларға модуль 2 бойынша биттік қосу (операцияның белгіленуі – $\oplus$; XOR)

- белгілі бір модуль бойынша бүтін сандарды қосу: мысалы, 2^{32} модулі бойынша қосу, операцияның белгіленуі – $\boxplus$

егер $a + b < 2^{32}$ болса, онда $a \boxplus b = a + b$;

егер $a + b \geq 2^{32}$ болса, онда $a \boxplus b = a + b - 2^{32}$,

мұндағы + бүтін сандарды қосу;

- белгілі бір модуль бойынша бүтін сандарды көбейту:

$ab(modn) = res\left(\frac{ab}{n}\right)$ – бүтін сандардың көбейтіндісін (ab) n санына бөлгендегі қалдық;

- екілік векторлардың биттерінің орын ауыстырып қою;

- екілік векторлардың элементтерін кестелік алмастыру.

Шифрлау алгоритмдерінің практикалық беріктігі операцияларды тізбектерге біріктіру ерекшеліктерінен де тәуелді болады. АҚШ пен Ресейдегі сәйкес DES–алгоритмі мен ГОСТ-28147-89 шифрлау стандарттары ретінде қабылданған шифрлаудың блоктық алгоритмдері блоктық жүйелерге мысалдар болып табылады.

Тікелей криптографиялық түрлендіру (шифрлау) ашық мәтін блогын сол ұзындықтағы шифрмәтінге аударады. Кері криптографиялық түрлендіру (шифрды ашу) шифрмәтін блогын ашық мәтіннің бастапқы блогына аударады. Құпия кілттің бар болуы - тікелей криптографиялық түрлендірудің орындалуының да, кері криптографиялық түрлендіруінің орнылдалуының да қажетті шарты болып табылады. Көптеген блоктық шифрлардың блок разрядтылығы 64 битті құрады.

Тікелей криптографиялық түрлендіру келесі қасиетті қамтиды: ашық мәтіннің әртүрлі блоктары шифрмәтіннің әртүрлі блоктарында орналасады. Кері түрлендіруде сәйкестік сақталады. Тікелей түрлендіруді блоктың бекітілген өлшемімен хабарлар жиынындағы орын ауыстыру ретінде қарастыруға болады. Орын ауыстыру нәтижесі құпиялы сипатта болады, ол құпия компонентпен – кілтпен қамтамасыз етіледі.

Фейстель желісінің негізінде DES алгоритмі жобаланған болатын 1977 жылы АҚШ үкіметі DES стандартын берілгендерді шифрлаудың стандартты әдісі деп мақұлдайтын FIPS 46-3 стандартын қабылдады. Алгоритмнің итеративті құрылымы қарапайым программалық және аппараттық жүзеге асыруды құруға мүмкіндік берді.

Кейбір мәліметтерге сәйкес ССРО-да 1970 жылдары МҚК (КГБ) Фейстель желісін пайдаланатын блоктық шифрды дайындады және осы шифр 1990 жылы ГОСТ 28147-89 ретінде қабылданды.

1987 жылы FEAL және RC2 алгоритмдері дайындалды. Blowfish (1993), TEA (1994), RC5 (1994), CAST-128 (1996), XTEA (1997), XXTEA (1998), RC6 (1998) және т.б. сияқты алгоритмдер пайда болған 1990 жылдары Фейстель желілері кеңінен пайдаланылды.

1997 жылы 2 қаңтарда NIST институты DES-ті алмастыратындай, берілгендерді шифрлаудың жаңа алгоритмін дайындау бойынша конкурс жариялады. Жаңа блоктық шифр AES (ағылш. *Advanced Encryption Standard*) деп аталды және 2002 жылы 26 мамырда бекітілді. AES-те Фейстель желісінің орынына алмастыру-орын ауыстыру желісі пайдаланылды.

Фейстель желісі немесе Фейстель конструкциясы блоктық шифрларды құру әдістерінің бірі болып табылды. Желі Фейстель ұяшықтары деп аталатын ұяшықтардан тұрады. Әрбір ұяшықтың кірісіне берілгендер мен кілт түседі. Әрбір ұяшықтың шығысында өзгертілген берілгендер мен өзгертілген кілт алынады. Барлық ұяшықтар бір типті және желі көп рет қайталанылатын құрылымды береді деп айтады. Кілт шифрлау / шифрды ашу алгоритмдеріне байланысты таңдалынады және бір ұяшықтан екіншісіне өткен кезде өзгеріп отырады. Шифрлау және шифрды ашу барысында бір операциялар орындалады; тек кілт реті ғана ерекшеленеді. Операциялардың қарапайымдылығынан Фейстель желісі программалық сияқты, аппараттық та жеңіл жүзеге асырылады. Көптеген заманауи блоктық шифрлар (DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA және т.б.) Фейстель желісін негізі ретінде пайдаланады. Алмастыру-орын ауыстыру желісі (AES және т.б.) Фейстель желісіне балама болып табылады.

Фейстель конструкциясы мәтінді мәтіннің бөліктерінің бірінен есептелген мән басқа бөліктеріне салынатын қайтарымды түрлендіру әдісі деп аталады. Желі құрылымы көбінесе келесі түрде орындалады: шифрлау және шифрды ашу үшін бір алгоритм пайдаланылады – айырмашылығы тек кілт материалын пайдалануда.

Екілік түрде (нөлдер мен бірлер тізбектері түрінде) және компьютер жадысында немесе басқа да құрылғыда (мысалы, файлда) берілген қандай да бір ақпаратты шифрлау талап етілсін.

Шифрлау алгоритмі:

Ақпарат бірдей (бекітілген) ұзындықтағы блоктарға бөлінеді. алынған блоктар алгоритм кірісіне түсетіндіктен *кіріс блоктары* деп аталады. Кіріс блогының ұзындығы бір мезгілде шифрлауға қабілетті таңдалынған шифрлау алгоритмінің өлшемінен (блок өлшемі) кіші болса, онда блок қандай да бір тәсілмен ұзартылады. Ереже бойынша блок ұзындығы екінің дәрежесі болып табылады, мысалы, 64 битті немесе 128 битті құрайды.

Блоктық шифрлау алгоритмінде берілгендерді өңдеудің тізбектелген қадамдарының бірі криптографияда раунд деп аталады. Фейстель шифрларында және шифрлар архитектурасы бойынша оған жақын – берілгендердің шифрланатын блогының бір немесе бірнеше бөлігі берілген функцияны қолдану жолымен жетілдірілетін шифрлаудың бір қадамы.

Таңдалынған блок бір өлшемдегі екі– «сол жақ» (L_0) және «оң жақ» (R_0) ішкі блокқа бөлінеді.

«Оң жақ» R_0 ішкі блок K_0 раундтық кілтті пайдалана отырып F функциясымен өзгеріледі:

$$x = F(R_0, K_0).$$

Нәтиже модуль 2 бойынша «сол жақ» L_0 ішкі блокпен қосылады:

$$x = x \oplus K_0.$$

Нәтижесі келесі раундта «оң жақ» R_1 ішкі блок рөлінде пайдаланылады:

$$R_1 = x.$$

Ағымдық раундтың «оң жақ» R_0 ішкі блогы келесі раундта (раудтың бастапқы мезетінде өзінің өзгерілмеген түрінде) «сол жақ» L_1 ішкі блок рөлінде пайдаланылады:

$$L_1 = R_0.$$

Қандай да бір математикалық ереже бойынша K_1 раундтық кілт – келесі раундта пайдаланылатын кілт есептеледі.

Аталған операциялар $N - 1$ рет орындалады, мұндағы N – таңдалынған шифрлау алгоритміндегі раундтар саны. Бұл жерде бір раундтан (кезең) басқасына өту арасында кілттер өзгереді: K_0 кілті K_1 кілтімен, K_1 кілті K_2 кілтімен және т.с.с алмастырылады.

Шифрды ашу

Ақпарат шифрын ашу шифрлау сияқты орындалады, бұл жерде тек кілттер кері ретпен орналасады, яғни біріншіден N-ге емес, керісінше N-шіден біріншіге қарай жүзеге асырылады.

Алгоритмдік сипатталуы

Ашық мәтін бірдей екі бөлікке бөлінеді: (L_0, R_0)

Әрбір раундта

$$L_i = R_{i-1} \oplus f(L_{i-1}, K_{i-1})$$

$$R_i = L_{i-1}$$

есептеледі, мұндағы, i – раунд нөмірі, $i = 1, \dots, N$; N – шифрлаудың таңдалынған алгоритміндегі раунд саны; f – қандай да бір функция; K_{i-1} – $i-1$-ші раундтағы кілт (раундтық кілт).

(L_N, R_N) – N раундтың орындалу нәтижесі болып табылады. N раундта, шифрды ашу үшін де сол процедураны пайдалану мүмкін болу үшін L_N мен R_N ішкі блоктарының орындары ауыспайды. Кілттерді пайдалану реттері ауыстырылады ($K_0, \dots, K_{N-1}, K_N$ орнына $K_N, K_{N-1}, \dots, K_0$):

$$L_{i-1} = R_i \oplus f(L_i, K_{i-1})$$

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

Аздаған өзгерістің көмегімен шифрлау және шифрды ашу процедураларын орындауға болады.

Артықшылығы:

- пайдаланылатын f функциясынан тәуелсіз алгоритмнің қайтымдылығында;
- қаншалықты күрделі болса да f функциясын таңдау мүмкіндігінде.

Математикалық сипаттау

Мысалы, кіріске түсетін берілгендер блогы (кіріс блогы); A – қандай да бір инволютивті түрлендіру (немесе инволюция) – өзіне өзі кері болып табылатын өзара бірмәнді түрлендіру, яғни әрбір $(\forall)X$ үшін келесі өрнек ақиқат болсын:

$$AAX = A^2X = X, (\forall)X$$

Y – шығысында (нәтиже) алынатын берілгендер блогы.

A түрлендіруін X кіріс блогына түрленліруді бір реттік қолданғанда Y шығыс блогы алынады:

$$Y = AX$$

A түрлендіруін алдыңғы Y түрлендіру нәтижесіне қолдану кезінде келесі қатынасты аламыз:

$$AY = AAX = X, (\forall)X$$

X кіру блогы бірдей ұзындықтағы L және R ішкі блоктарынан тұрсын:

$$X = (L, R)$$

Екі түрлендіруді анықтаймыз:

$G(X, K)$ – X берілгендерін K кілтпен шифрлау:

$$G(X, K) = (G(L, R), K) = (L \oplus F(K, R), R)'$$

$T(L, R)$ – L және R ішкі блоктарының орындарын ауыстыру:

$$T(L, R) = (R, L)$$

Келесі белгілеулерді енгіземіз:

G түрлендіруін бір реттік қолдану:

$$\tilde{X} = \left(\tilde{L}, \tilde{R}\right) = GX$$

G түрлендіруін екі реттік қолдану:

$$\tilde{\tilde{X}} = \left(\tilde{\tilde{L}}, \tilde{\tilde{R}}\right) = G^2X$$

Шифрды ашу барлық түрлендірулерді кері ретпен қолдану арқылы жүргізіледі. Түрлендірудің әр қайсысының инволюнтивтілігінен к нәтижесінде кері рет бастапқы нәтижені береді:

$$X = G_1TG_2T \dots G_{m-1}TG_mT(Y_m) = G_1TG_2T \dots G_{m-1}T(Y_{m-1}) = \dots = G_1T(Y_1) = X$$

Фейстель желілерінде пайдаланылатын функциялар.

Түрлендірудің екі блогы бар ($f(L_i, K_i)$ функциясы)

- алмастыру блогы (s-блок, ағылш. s -box);
- орын ауыстыру блогы (p-блок, ағылш. p -box).

Бекітілген ұзындықтағы берілгендер блогын кез келген екілік түрлендіру s-блогы түрінде жүзеге асырылады. N үлкен болған жағдайда N-разрядты s-блокты құрудың күрделілігіне бпйланысты практикада қарапайымдау болып келетін конструкция қолданылады.

Блок термині түпнұсқада «функция» терминінің орнына пайдаланылады, осыған байланысты блоктық шифр жайында қарастырылады да, s және p блоктар цифрлық микросұлбалар (цифрлық блоктар) болады деп ұсынылады.

S-блок.

Алмастыру блогы келесі бөліктерден тұрады:

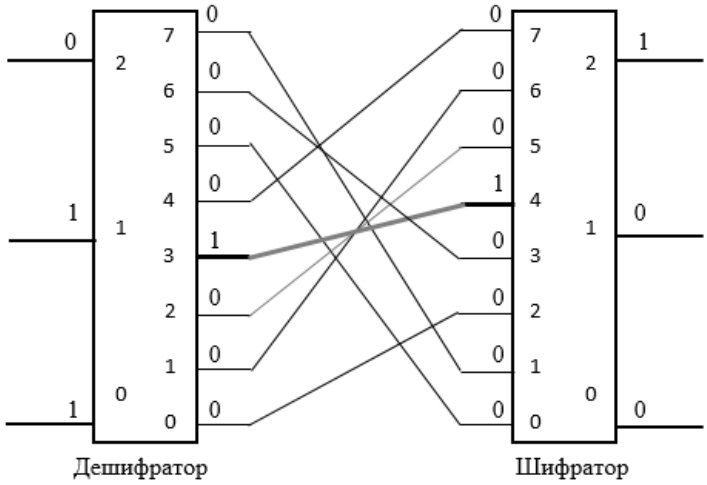
- дешифратор – n-разрядты екілік сигналды 2^n негізі бойынша бірразрядты сигналға түрлендіргіш;
- коммутатор жүйесі – ішкі қосу (мүмкін болатын барлық қосулар саны $2^n!$);
- шифратор – бірразрядты 2^n-реттік сигналды n-разрядты екілік сигналға түрлендіргіш.

n өте үлкен болған жағдайда n-разрядты s-блокты талдау қиынға соғады, қосу мүмкіндіктер саны (2^n) көп болғандықтан осындай блоктарды практикада жүзеге асыру да қиын болады. Практикада алмастыру блогы күрделірек жүйелердің бөлігі ретінде пайдаланылады.

Жалпы жағдайда s-блоктың кіріс / шығыс сандары беттеспеуі мүмкін, бұл жағдайда коммутация жүйесінде дешифратордың әрбір шығысынан бір ғана қосылудың шығуы міндетті емес, бұл жерде екі немесе одан да көп, немесе мүлдем шықпауы да мүмкін. Осындай мәселе шифратор кірісі үшін де ақиқат болады.

Электроникада төменде келтірілген сұлбаны тікелей қолдануға болады. Программалауда алмастыру кестесін генерациялайды. Осы екі тәсіл де эквивалент болып табылады, яғни компьютерде шифрланған файлдың электрондық құрылғыда шифрын ашуға болады және керісінше.

S-блок сұлбасы



Келтірілген 3-разрядты s-блок үшін алмастыру кестесі

Комбинация	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Кіріс	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*
Шығыс	*010*	*110*	*101*	*100*	*111*	*000*	*011*	*001*

Артықшылықтары:

- функцияның едәуір бөлігі заманауи компьютерлердің аппараттық деңгейімен қолдауына байланысты программалық жүзеге асыруының қарапайымдылығы (мысалы, 2 модулі бойынша қосу («хог»), 2^n модулі бойынша қосу, 2^n модулі бойынша көбейту және т.б.);
- Фейстель желісінде тұрғызылған алгоритмнің жақсы меңгерілуі.

Кемшілігі:

Бір раундта тек қана кіріс блогының жартысы шифрланады.

Қорытынды.

Ақпаратты шифрлаудың қажеттілігі мен ұсынылған шифрлар санының жеткілікті түрде үлкен болуынан блоктық шифрларды стандарттауға немесе қолдануға ұсыныс білдіретіндей бағытта бірнеше ірі конкурстар жарияланды. Мұның нәтижесінде АҚШ-тағы және барлық әлемдегі шифрлау стандарты сияқты DES қабылдаушысын іздеуге бағытталған AES жобасы болды. Конкурсқа қатысушыларға қойылатын талаптар қарапайым болды: 128-биттік блок, 128-, 192- және 256-биттік құпия кілт, шифр 3- DES-тен кем болмауы керек, бірақ жылдамдығы оған қарағанда артығырақ болуы керек. Конкурсқа 20-ға жуық өтініш түсті, оның 15 шифры конкурсқа толығымен сәйкес келді. Бірінші кезеңнен кейін әр түрлі платформаларда тиімді жұмыс істейтінін және жақсы сенімділік көрсеткен бес шифр іріктеліп алынды. Олар толығымен зерттелініп, ешқандай кемшілігі жоқ деп мақұлданды. Әйтсе де, конкурс шарты бойынша бір ғана шифр таңдалыну керек болғандықтан, шешімнің айқындығымен және элеганттылығымен ерекшелінген бельгиялық Rijndael жұмысы таңдалынып алынды.

Осыдан кейін тағы екі конкурс - европада NESSIE (2000 ж.) және Жапонияда CRYPTREC ұйымдастырылды, бұл конкурстарда блоктық шифрлар ғана емес, сонымен қатар басқа да алгоритмдер зерттелінді [3].

42 өтініш түскен NESSIE (англ. New European Schemes for Signatures, Integrity, and Encryptions, электрондық қолтаңба, тұтастылық және шифрлауға арналған жаңа европалық алгоритмдер) жобасының негізгі мәселелері – мықты криптографиялық алгоритмдерді анықтау болды. Конкурсқа жіберілген алгоритмдердің ішінде конкурсқа ең көп қатысушылар Жапониядан болды. NESSIE конкурсының AES конкурсынан айырмашылықтарының бірі – шифрланатын мәліметтер блогының өлшеміне қандай да бір шектеу қойылмайды, сондықтан да конкурста 64-, 128-, 160- және 256-биттік блоктық шифрлар қарастырылды. NESSIE конкурсындағы алгоритмдер бағаланатын басты критерийлер ол – мәліметтердің құпиялылығы, тұтастылығы және аутентификациясы. NESSIE жобасы зерттеушілер, дайындаушылар және алгоритмдерді стандарттауға дейін тексеретін және салыстыратық серіктестер арасында көпір болды.

CRYPTREC (ағылш. Cryptography Research and Evaluation Committees) жобасы 2000 жылы өкіметтік және индустриалдық пайдалану үшін шифрлау әдістерін бағалау және ұсыну мақсатында жапон өкіметімен ұсынылды. Жоба мақсаты – электрондық мемлекеттің қауіпсіздігін бағалау және мониторинг жүргізу, шифрларды ұсыну, сонымен қатар, криптографиялық модульдерді бағалау критерийлерін орнатады. Жыл сайын наурыз айында CRYPTREC қызметі бойынша жылдық есеп беріліп, жарияланып отырады.

Блоктық шифрлаудың даму тарихымен танысу криптографияны меңгеру барысындағы – мәліметтерді құпиялылығының (ақпаратты басқа тұлғалардың оқу мүмкіндіктерінің болмауы, тұтастығының (ақпараттың байқаусыз өзгертілуінің мүмкін еместігі) және аутентификациялаудың (авторлықтың немесе объектінің қандай да бір қасиеттерінің түпнұсқасын тексеру)) әдістері туралы ғылым, сонымен қатар, авторлықтан бас тарту мүмкін еместігінде.

Криптография дамуының тарихи аспектілерімен студенттердің танысуы арқылы өзінің ой-өрісін кеңейту, ғылымның жүйелік байланысын орнату және математикалық пәндерді меңгеруге кәсіби бағытталған және осы салада мамандықты игеру сияқты мәселелер жүзеге асырылады.

Пайдаланылған әдебиеттер тізімі:

1 Гусманова Ф.Р., Абдулкаримова Г.А. Ақпаратты қорғаудың криптографиялық әдістерін оқытудың өзекті аспектілері. // Абай атындағы ҚазҰПУ Хабаршысы. «Физика-математика» сериясы №4(68), 2019, С.201-208

2 Пестунов А.И. Блочные шифры и их криптоанализ // Вычислительные технологии Т.12, №4, 2007 г. С.42-50

3 Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009 – 576 с. ISBN 978-5-9775-0319-8.