DOI 10.52209/1609-1825_2021_2_181 ӘОЖ 003.26

Ақпаратты қорғаудың криптографиялық әдістері

ШЕГЕТАЕВА Айжан Каиргельдиевна, *аға оқытушы, aizhanshegetaeva@mail.ru,*
Қарағанды техникалық университеті, Қазақстан, 100027, Қарағанды, Н. Назарбаев даңғылы, 56.

Аңдатпа. *Криптографияның мақсаты құпия хабарламалардың мазмұнын қорғалмаған (Ашық) арна арқылы беру кезінде қорғау болып табылады. Стеганографияның міндеті-құпия хабарламаларды беру фактісін жасыру, яғни жасырын (подсознание) арна құру. Ақпаратты криптографиялық түрлендіру – құпия параметр – кілтке байланысты өзара бір мәнді математикалық түрлендіру. Шифрлау нәтижесі криптограмма немесе шифрлі мәтін деп аталады. Шифр криптографиялық алгоритммен сипатталады және кілтпен бірегей анықталады. Құпия кілтті білмей шифрланған мәтінді ашу әдістері криптоанализ деп аталады. Криптоталдаудың мақсаты ашық мәтінді алу және шифр кілтінің құпия компонентін анықтау болуы мүмкін. Шифрдың сенімділігі-шифрлау кілтін білмей шифрды бұзуға болмайтындығына кепілдік беру дәрежесі-оның тұрақтылығы деп аталады (криптографиялық тұрақтылық, крипто-тұрақтылық). Криптография тарихы бірнеше мыңжылдықтардан басталады. Бұл жағдайда барлық шифрларды екі негізгі түрге бөлуге болады: ауыстыру (ауыстыру) және пермутация.*

Кілт сөздер: *криптография, криптоталдау, шифрлеу, криптожүйе, Цезарь шифры.*

Кіріспе

Ақпаратты қорғаудың қажеттілігі адамда жазуды үйренгеннен кейін бірден пайда болды. Ақпаратты қорғауды – *криптография* деп атайды, криптография құпия деректерді қорғау құралы ретінде қарастырылады:

- рұқсатсыз оқу;
- тұтастықты қасақана бұзу немесе жою;
- қажетсіз көшіру;
- фальсификация.

Криптографиялық қорғауға қойылатын негізгі талаптардың бірі, оның тең беріктігі принципі болып табылады. Яғни, егер қорғаныстық сілтемелерге бөлуге болатын болса, онда бұл сілтемелердің барлығы бірдей бұзуға төзімді болуы керек. Криптография ежелгі Египет пен Вавилонда белгілі болған деп болжанады. Криптожүйенің кеңінен танымал тарихи мысалы – Цезарь шифры деп аталады, ол ашық мәтіннің әр әрпін алфавиттің үшінші әрпімен (қажет болған кезде циклдік беріліспен) қарапайым ауыстыру болып табылды. Мысалы, "A" әрпі "D"-ға, "B" әрпі "E"-ге, "Z" әрпі "C" әріптеріне ауыстырылды.

Цезарь заманынан бері өткен ғасырлар бойы математиканың айтарлықтай жетістіктеріне қарамастан, XX ғасырдың ортасына дейін құпия жазба айтарлықтай қадамдар жасаған жоқ. Алғашқы электронды компьютерлердің пайда болуы жағдайды түбегейлі өзгертті:

- қоғамда айналымдағы ақпарат көлемі экспоненциалды заңға сәйкес өсе бастады – ол әр бес жыл сайын шамамен екі есе артады;
- белгілі бір деректерге қол жеткізу маңызды материалдық және қаржылық құндылықтарды бақылауға мүмкіндік береді; ақпарат көптеген жағдайларда тіпті есептеуге болатын құнды сатып алды;
- өңделген деректердің сипаты әр түрлі болды және тек мәтіндік мәліметтерге ғана қатысты емес;
- ақпараттық өзара әрекеттесудің сипаты күрделене түсті: жіберілген мәтіндік хабарламаларды рұқсатсыз оқудан және бұрмалаудан қорғаудың классикалық міндетімен қатар, ақпаратты қорғау саласындағы жаңа міндеттер пайда болды, мысалы, электрондық құжатқа қол қою;
- қазір ақпараттық процестердің субъектілері тек адамдар ғана емес, сонымен бірге олар жасаған бағдарламаға сәйкес жұмыс істейтін автоматты жүйелер болып табылады;
- қазіргі компьютерлердің есептеу қабілеттері жоғары күрделілігіне байланысты бұрын мүмкін емес шифрларды іске асыру мүмкіндіктерін де, оларды бұзу бойынша талдаушылардың мүмкіндіктерін де жаңа деңгейге көтерді.

Бұл өзгерістер криптографияның дамуына үлкен үлес қосты. Ғалымдар криптография мен криптоталдау мәселелерімен тығыз айналысты.

Әдіснама

Криптография (кейде криптология термині қолданылады) – бұл құпияны (криптографияны) және оны ашу әдістерін зерттейтін білім саласы – криптоталдау – Криптография математиканың бір саласы болып саналды.

Бүгінгі таңда криптография, соның ішінде құпия параметрлерді қолданатын алгоритмдер арқылы мәліметтерді түрлендіруге негізделген мүлдем басқа сипаттағы ақпараттық өзара әрекеттесуді қорғау әдістерін біріктіреді.

Ақпаратты криптография әдістерімен қорғау арнайы алгоритмдерді немесе аппараттық құралдарды және кілт кодтарын қолдана отырып, құрамдас бөліктерді (әріптер, сандар, слогдар,

сөздер) түрлендіру арқылы анық емес түрге келтіруден тұрады.

Кілт-бұл хабарламаларды шифрлау, сандық қолтаңбаны қою және тексеру, түпнұсқалық кодтарды есептеу кезінде криптографиялық алгоритм қолданатын құпия ақпарат. Бірдей алгоритмді қолданған кезде шифрлау нәтижесі кілтке байланысты болады.

Криптографиялық жүйенің мақсаты – мағыналы бастапқы мәтінді шифрлау (сонымен қатар ашық мәтін деп те аталады) және нәтижесінде мүлдем мағынасыз шифрланған мәтінді (шифрмәтін, криптограмма) алу. Бұл жағдайда қарсылас (криптоталдаушы деп те атайды) бастапқы мәтінді аша алмауы үшін жасалады.

Шифрлау (шифрды ашу) мен шифр мәтінін ашудың арасында маңызды айырмашылық бар.

Криптожүйенің ашылуы – бұл криптожүйенің көмегімен шифрланған кез-келген ашық мәтінді тиімді ашуға мүмкіндік беретін криптоталдауыштың нәтижесі. Криптожүйенің ашыла алмау дәрежесі оның тұрақтылығы деп аталады.

Шифрдың сенімділігін қосымша қамтамасыз ету – алгоритмнің құпиялылығы. Бірақ іс жүзінде, егер алгоритм әзірлеушілерге белгілі болса, пайдаланушы мен әзірлеуші бір адам болмаса, оны енді құпия деп санауға болмайды. Сонымен қатар, егер әзірлеушінің қабілетсіздігі немесе қателіктері салдарынан алгоритм тұрақсыз болса, оның құпиялылығы оны тәуелсіз сарапшыларға тексеруге мүмкіндік бермейді. Алгоритмнің тұрақсыздығы ол бұзылған кезде ғана анықталады, тіпті ол мүлдем анықталмайды.

Сондықтан криптограф алдымен голландиялық Керкхоф тұжырымдайтын ережені басшылыққа алуы керек: шифрдың беріктігі тек кілттің құпиялылығымен анықталуы керек. Басқаша айтқанда, Керкхоф ережесі-құпия кілттің мәнінен басқа барлық шифрлау механизмі априори жауға белгілі болып саналады.

Криптография басқа мақсаттарда жиі қолданылады:

- түпнұсқалықты тексеру. Хабарламаны алушы оның көзін тексере алады. Қаскүнем ешкімге ұқсай алмайды;
- тұтастық. Хабарламаны алушы жеткізу барысында хабарламаның өзгергенін тексере алады;
- авторлық құқықтан бас тартпау. Жіберуші хабарламаны жіберуден жалған бас тарта алмайды.

Шифрлау алгоритмі жасырылмаған кезде ақпаратты қорғау әдісі де бар (қатаң айтқанда, криптографияға қатысты емес), бірақ хабарламада шифрланған (онда жасырылған) ақпарат бар. Мұндай жасыру тәсілі *ақпаратты маскілеу* деп атайды.

Криптоталдау – бұл кілтсіз ашық мәтінді алу туралы ғылым. Сәтті өткізілген криптоталдау ашық мәтінді немесе кілтті ашуы мүмкін. Кілттің ашылуы криптологиялық жолмен емес, ымыраға келу деп аталады. Криптоталдау әрекеті аутопсия деп аталады. Әдетте криптоталдаудың келесі түрлері бөлінеді:

1. Тек шифрлі мәтінді пайдалана отырып ашу. Криптоталдаушының міндеті-ашық мәтінді мүмкіндігінше көп хабарламаларды ашу немесе сол кілтпен шифрланған басқа хабарламаларды шифрлау үшін пайдаланылатын кілтті алу.

2. Ашық мәтінді пайдалана отырып ашу. Криптоталдаушы бірнеше хабарламалардың шифр мәтіндеріне ғана емес, сонымен қатар осы хабарламалардың ашық мәтініне де қол жеткізе алады. Оның міндеті-сол кілтпен шифрланған басқа хабарламаларды шифрлау үшін хабарламаны шифрлау үшін пайдаланылатын кілтті алу.

3. Таңдалған ашық мәтінді қолдана отырып ашу. Криптоталдаушы бірнеше хабарламалардың шифр мәтіндері мен ашық мәтіндеріне қол жеткізіп қана қоймай, шифрлау үшін ашық мәтінді таңдау мүмкіндігіне ие.

4. Ашық мәтінді қолдана отырып, адаптивті ашу. Бұл таңдалған ашық мәтінді қолдана отырып ашудың ерекше жағдайы. Криптоталдаушы шифрланған мәтінді таңдап қана қоймай, алынған нәтижелерге сүйене отырып, келесі таңдауын жасай алады.

5. Таңдалған шифрмәтінді пайдаланып ашу. Криптоталдаушы шифрлау үшін әртүрлі шифр мәтіндерін таңдай алады және шифрланған ашық мәтіндерге қол жеткізе алады [1].

Шифр деп те аталатын криптографиялық алгоритм – шифрлау және шифрлау үшін қолданылатын математикалық функция. Әдетте бұл екі байланысты функция: біреуі шифрлау үшін, екіншісі шифрдан ашу үшін.

Қорғаныштық түрлендіру әдістеріне қойылатын негізгі талаптар:

- қолданылатын әдіс тек шифрланған мәтінмен бастапқы мәтінді ашуға жеткілікті түрде төзімді болуы керек;
- кілттің көлемі оны есте сақтау мен жіберуді қиындатпауы керек;
- ақпаратты түрлендіру алгоритмі және шифрлау және шифрлау үшін қолданылатын кілт өте күрделі болмауы керек. Қорғаныштық қайта құруға арналған шығындар ақпаратты сақтаудың берілген деңгейі кезінде қолайлы болуы тиіс;
- шифрлау қателері ақпараттың жоғалуына әкелмеуі керек. Байланыс арналары арқылы шифрланған хабарламаны беру қателерінің пайда болуына байланысты қабылдау соңында мәтінді сенімді шифрлау мүмкіндігі жоққа шығарылмауы керек;
- шифрланған мәтіннің ұзындығы бастапқы мәтіннің ұзындығынан аспауы керек;
- ақпаратты шифрлау мен шифрын шешуге қажетті уақыт пен шығындар ресурстары ақпаратты қорғаудың қажетті деңгейімен анықталады.

Зерттеу нәтижелері

Қорғаныс түрлендірулерінің көптеген заманауи әдістерін 4 үлкен топқа жіктеуге болады:

1. Қайта жүктеу.

2. Ауыстыру.
3. Аддитивті.
4. Аралас.

Пермутация және алмастыру әдістері әдетте кілттің қысқа ұзындығымен сипатталады, ал оларды қорғаудың сенімділігі түрлендіру алгоритмдерінің күрделілігімен анықталады.

Аддитивті әдістер қарапайым түрлендіру алгоритмдерімен сипатталады және олардың сенімділігі кілттің ұзындығын ұлғайтуға негізделген.

Барлық аталған әдістер симметриялы шифрлауға қатысты-шифрлау және шифрлау үшін бірдей кілт қолданылады.

Асимметриялық шифрлау кезінде бір кілт шифрлау үшін қолданылады – ашық, ал екіншісі шифрлау үшін жабық.

1. Қайта жүктеу әдісі. Бұл бастапқы мәтіннің кіріс ағыны блоктарға бөлінеді, олардың әрқайсысында таңбалар қайта орналастырылады. Қайта жүктеудің қарапайым мысалы-бастапқы мәтінді кейбір матрицаның жолдарына жазып, оны осы матрицаның бағандары бойынша оқу. Жолдарды толтыру реті және бағандарды оқу кез-келген болуы мүмкін және кілтпен орнатылады. Қайта жүктеу әдістері алгоритмнің қарапайымдылығымен, бағдарламалық жасақтаманы іске асыру мүмкіндігімен және қорғаудың төмен деңгейімен сипатталады. Бұл әдістің кемшілігі – егер сіз жүйеге шифрлау үшін бірнеше арнайы таңдалған хабарламаларды жібере алсаңыз, оны оңай ашуға болады [2].

2. Ауыстыру (алмастыру) әдісі. Бір алфавитте жазылған бастапқы мәтіннің таңбалары қабылданған түрлендіру кілтіне сәйкес басқа алфавиттің таңбаларымен ауыстырылады. Қарапайым әдістердің бірі-бастапқы таңбаларды ауыстыру векторының эквивалентімен тікелей ауыстыру. Бастапқы мәтіннің келесі таңбасы үшін оның орналасқан жері бастапқы алфавитте ізделеді. Ауыстыру векторының баламасы алфавиттің басынан алынған ығысуға бөлінеді. Шифрлау кезінде іздеу ауыстыру векторында жасалады, ал баламасы алфавиттен таңдалады. Осылайша алынған мәтіннің қорғаныс деңгейі төмен.

Ашуға қатысты неғұрлым тұрақты-бұл Вижинер кестесін қолдануға негізделген шифрлау схемасы. Кесте – k элементтерінің саны бар квадрат матрица, мұндағы k – алфавиттегі таңбалар саны.

Матрицаның бірінші жолында әріптер алфавиттегі кезектілік тәртібімен жазылады, екіншісінде – сол әріптер тізбегі, бірақ сол жаққа бір позицияға ауысумен, үшіншісінде – 2 позицияға ауысумен және т.б. оң жақтағы бос орындар солға ығыстырылған, табиғи ретпен жазылған әріптермен толтырылады.

Мәтінді шифрлау үшін кілт орнатылады, ол белгілі бір сөз немесе әріптер жиынтығы. Әрі қарай, толық матрицадан шифрлау қосалқы матрицасы таңдалады, мысалы, бірінші жол және матрицаның жолы, оның бастапқы әріптері кілттің сериялық әрпі болып табылады.

Шифрлау процесі келесі әрекеттер тізбегін қамтиды:

1. Шифрланған мәтіннің әр әрпінің астына кілт әріптері жазылады, олар кілтті бірнеше рет қайталайды.

2. Субматрица бойынша шифрланатын мәтін кіші матрацтың бірінші жолы мәтінінің әріптерін және оның астындағы кілт әріптерін қосатын сызықтардың қиылысында орналасқан әріптермен ауыстырылады.

Мәтінді түсіндіру келесі ретпен орындалады:

1. Шифрланған мәтін әріптерінің үстіне кілт әріптері рет-ретімен жазылады.

2. Вижинер кестесінің ішкі матрицасының жолында кілттің әр әрпі үшін шифрланған мәтін белгісіне сәйкес келетін әріп ізделеді. Оның үстіндегі бірінші жолдың әрпі шифрланған мәтіннің белгісі болады.

3. Алынған мәтін мағынасы бойынша сөздерге топтастырылған.

Вижинер кестесіне сәйкес шифрлаудың кемшіліктерінің бірі-кілттің қысқа ұзындығымен шифрлаудың сенімсіздігі және ұзын кілттерді қалыптастырудың күрделілігі. Мәтінді шифрлаудың сенімділігін арттыру үшін Вижинер кестесінің жетілдірілген нұсқасы қолданылады, ол келесідей:

1. Бірінші жолдан басқа барлық жолдарда алфавиттің әріптері еркін ретпен орналастырылады.

2. 10 таңдалады, біріншісін есептемегенде, 0-ден 9-ға дейінгі натурал сандармен нөмірленген жолдар.

3. Кілт ретінде шексіз сандар сериясымен көрсетілген шамалар қолданылады (мысалы, Рі саны).

Шифрлау және шифрын ашу қарапайым Вижинер кестесімен бірдей ретпен жүзеге асырылады.

3. Аддитивті әдістер. Бұл әдістерде кілт ретінде сол алфавиттің әріптерінің белгілі бір реттілігі және бастапқы мәтінмен бірдей ұзындық қолданылады.

Шифрлау бастапқы мәтіннің таңбаларын және алфавиттегі әріптер санына тең модуль кілтін қосу арқылы жүзеге асырылады.

Сол әдістің мысалы-гамма, яғни бастапқы мәтінге гамма деп аталатын кейбір кодтар тізбегін қабаттастыру. Араластыру процесі келесідей жүзеге асырылады:

1. Бастапқы мәтін мен гамма таңбалары екілік кодта ұсынылады және бір-бірінің астында орналасады.

2. Екілік белгілердің әр жұбы қабылданған алгоритмге сәйкес шифрланған мәтіннің бір екілік белгісімен ауыстырылады.

3. Шифрланған мәтіннің екілік белгілерінің алынған реттілігі таңдалған кодқа сәйкес алфавит таңбаларымен ауыстырылады.

Егер шифрлау кілті кездейсоқ таңдалса, жалған кездейсоқ сандар сенсорының көмегімен пайда болса, онда кілтті білмей ақпаратты ашу мүмкін емес.

Қорытынды

Криптография қазіргі уақытта ақпаратты қорғаудың сенімді жүйесі ретінде қызмет етеді деп қорытынды жасауға болады. Криптография да, криптоталдау да бір-бірінің білім саласының екі құрамдас бөлігі болып табылады. Біреуінің дамуындағы кез-келген ілгерілеу екіншісінің дамуына серпін береді [3].

Қазір ақпараттың құпиялылығы мен қорғалуына көп көңіл бөлінеді және оларды іздеу кванттық криптография саласында жатыр. Ол сенімділіктің абсолютті кепілдігін бере алады. Бұл технологияның мүмкіндіктері оны ірі банктер мен корпорациялармен қолданумен шектелмейді, бірақ көпшілікке қол жетімді болады.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Babash, A.V. Kriptografiya / L.V. Babash, G.II. Shankin. – M.: Solon-R, 2002.
2. Babenko, L.K. Sovremennyie algoritmyi blochnogo shifrovaniya i metodyi ih analiza: ucheb, posobie / L.K. Babenko, E.A. Ischukova. – M.: Gslios-ARV, 2006.
3. Zubov, A.Yu. Kriptograficheskie metodyi zaschityi informatsii. Sovershennyie shifryi / A.Yu. Zubov. – M.: Gelios ARV, 2005.

Криптографические методы защиты информации

ШЕГЕТАЕВА Айжан Каиргельдиевна, *старший преподаватель, aizhanshegetaeva@mail.ru,*
Карагандинский технический университет, Казахстан, 100027, Караганда, пр. Н. Назарбаева, 56.

Аннотация. *Целью криптографии является защита содержимого секретных сообщений при их передаче по незащищенному (открытому) каналу. Задачей стеганографии является сокрытие самого факта передачи секретных сообщений, т.е. создание скрытого (подсознательного) канала. Криптографическое преобразование информации – взаимно-однозначное математическое преобразование, зависящее от секретного параметра – ключа. Результат шифрования называется криптограммой или шифротекстом. Шифр описывается криптографическим алгоритмом и однозначно определяется ключом. Методы раскрытия зашифрованного текста без знания секретного ключа называются криптоанализом. Целью криптоанализа может быть как получение открытого текста, так и определение секретного компонента шифра – ключа. Надежность шифра – степень гарантии того, что шифр невозможно взломать без знания ключа шифрования – называется его стойкостью (криптографической стойкостью, криптостойкостью). История криптографии насчитывает несколько тысячелетий. При этом все шифры могут быть сведены к двум базовым типам: замене (подстановке) и перестановке.*

Ключевые слова: *криптография, криптоанализ, шифрование, криптосистема, система Цезаря.*

Cryptographic Information Security Methods

SHEGETAEVA Aizhan, *Senior Lecturer, aizhanshegetaeva@mail.ru,*
Karaganda Technical University, Kazakhstan, 100027, Karaganda, N. Nazarbayev ave., 56.

Abstract. *The purpose of cryptography is to protect the content of secret messages when they are transmitted over an unprotected (open) channel. The task of steganography is to conceal the very fact of the transmission of secret messages, i.e. creation of a hidden (subconscious) channel. Cryptographic transformation of information is a one-to-one mathematical transformation that depends on a secret parameter, a key. The result of the encryption is called a cryptogram or a ciphertext. The cipher is described by a cryptographic algorithm and is uniquely determined by the key. Methods of disclosing ciphertexts without knowing the secret key are called cryptanalysis. The purpose of cryptanalysis can be both obtaining the plaintext and determining the secret component of the cipher – the key. The strength of the cipher – the degree of guarantee that the cipher cannot be broken without knowing the encryption key – is called its strength (cryptographic strength, cryptographic strength). The history of cryptography goes back several millennia. Moreover, all ciphers can be reduced to two basic types: substitution (substitution) and permutation.*

Keywords: *cryptography, cryptanalysis, encryption, cryptosystem, Caesar's system.*

REFERENCES

1. Babash, A.V. Kriptografiya / L.V. Babash, G.II. Shankin. – M.: Solon-R, 2002.
2. Babenko, L.K. Sovremennyie algoritmyi blochnogo shifrovaniya i metodyi ih analiza: ucheb, posobie / L.K. Babenko, E.A. Ischukova. – M.: Gslios-ARV, 2006.
3. Zubov, A.Yu. Kriptograficheskie metodyi zaschityi informatsii. Sovershennyie shifryi / A.Yu. Zubov. – M.: Gelios ARV, 2005.