ӘОЖ 535.39

МОБИЛЬДІ ОБЪЕКТІЛЕРДЕН АШЫҚ ТЕЛЕКОММУНИКАЦИЯ АРНАЛАРЫ АРҚЫЛЫ ҚОРҒАЛҒАН ДЕРЕКТЕРДІ БЕРУ ЖҮЙЕСІН ЖОБАЛАУ

Алтынбек Жандаулет, Болатжан Қарақат
zandauletaltynbek@gmail.com, karakat990715@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық Университеті «Ғарыштық техника және технологиялар» кафедрасының 4-курс студенттері, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Молдамурат Х.

Қазіргі XXI ғасырда ақпараттық қауіпсіздік мәселесінің өзектілігі үнемі өсіп келеді және ақпаратты қорғаудың жаңа әдістерін іздеуді ынталандырады. Бүгінгі таңда ақпаратты қорғаудың жаңа әдістері мен алгоритмдерін, соның ішінде криптографиялық әдістерді іздеу және құру үнемі жүргізілуде. Өзекті міндет деп, атап айтқанда, ғарыш арналары арқылы ақпарат беру кезінде құпиялылықты қамтамасыз ету міндеті болды және болып қала беретіні сөзсіз.

Әлемнің барлық аймақтарында ұлттық қауіпсіздікке, қоғамдық қауіпсіздікке және жеке басына қол сұғылмаушылыққа нақты және болжамды қауіптердің өсуі байқалады. Ұялы желілер қоғамдық қауіпсіздікті қорғауда маңызды рөл атқарады, мысалы, құқық қорғау органдары қоңырау деректерін қолдана отырып, қылмыстық тергеу жүргізу, хабарламаларды ұстап қалу, ірі оқиғалар туралы хабарламаларды қолдау немесе денсаулыққа қауіптің таралуын бақылау үшін өз мандатын пайдаланған кезде. Жеке деңгейде алаяқтық, жеке басын ұрлау, кибершабуыл(хакерлік шабуыл) және ұялы желілер арқылы жасалатын басқа да заңсыз әрекеттер, сондай-ақ тіркелген желілер арқылы қол жетімді онлайн немесе сандық қызметтер бар. Соңғы оқиғалар, соның ішінде деректердің жоғалып кету жағдайлары, көптеген тұтынушылардың қауіпсіздігі мен құпиялылығы, мысалы, олардың өмірі туралы жеке мәліметтер қорғалғаны туралы алаңдаушылық тудырады.

Соған байланысты қазіргі уақытта шифрлеудің көптеген әдістері жасалынды, оларды қолданудың теориялық және практикалық негіздері де жасалынды. Өкінішке орай, қазіргі уақытта ғарыштық арналар арқылы ақпаратты генерациялау, шифрлеу және басқа пайдаланушыға жеткізу процестерінің бүкіл тізбегінде ақпараттың жайылып кетуіне ықпал ететін көптеген орындар бар. Берілетін ақпарат тікелей пайдаланушылардың құрылғыларында шифрленуі және дешифрленуі қажет. Қорғалған деректер арналарын пайдалану кезінде үшінші тараптар тек ақпараттық емес, шифрленген деректер ағынына қол жеткізе алады. Сондықтан ақпаратты шифрлеудің тиісті сапасын қамтамасыз ету қажет.

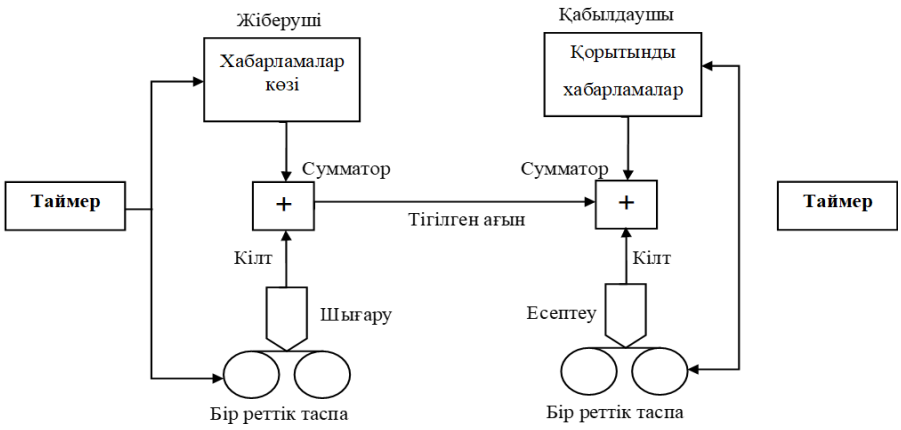
Бұл дегеніміз бір арнадан екінші арнаға желі арқылы хабарлама жіберу үшін транзакцияны бастаған екі арна өзара әрекеттесуі керек. Осы мақсатта логикалық ақпараттық арна құрылады, ол үшін деректер көзінен желідегі адресатқа өту бағыты анықталады және екі бастамашымен келісілген түрде пайдалану үшін коммуникациялық хаттама (мысалы, TCP/IP) таңдалады.

Қорғауды қамтамасыз ету үшін құпия ақпаратты жеткізуді жүзеге асыратын және жіберілген хабарламаның түпнұсқалығына кепілдік беретін транзакция бастамашыларының екеуіне де сенімді үшінші тараптың қатысуы қажет болуы мүмкін.

Жоғарыда келтірілген жалпы модельден белгілі бір қорғаныс құралын жасау кезінде келесі төрт негізгі мәселені шешу қажет:

1. Қорғауды қамтамасыз ету үшін ақпаратты түрлендіру алгоритмін жасау;
2. Алгоритммен бірге қолданылатын құпия ақпаратты жасау;
3. Осы құпия ақпаратты жеткізу және бөлісу әдістерін жасау;
4. Екі бастамашы қажетті қорғаныс деңгейін қамтамасыз ету үшін әзірленген алгоритм мен жасалған құпия ақпаратты пайдалана алатын хаттаманы таңдау.

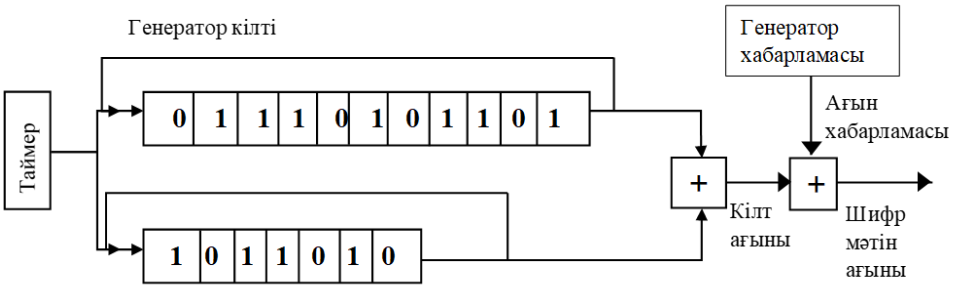
Осы кезекте Вернам шифры-симметриялық шифрлеудің ең көне тәсілдерінің бірі, абсолютті криптографиялық орнықтылығы дәлелденген жалғыз шифрлеу жүйесі болып табылады. Сонымен қатар, бұл қарапайым криптожүйелердің бірі. Хабардың биттерін кілт биттерімен ғана емес, мысалы, әріптерді де біріктіруге болады. Вернам идеясын Вижинер шифрінің қатысуымен суреттеуге болады. Бұл шифрдің кілті, Вернамның айтуы бойынша, кездейсоқ әріптер тізбегі болуы керек еді. 1.1-суретте Вернамның шифрлеу жүйесінің схемасы көрсетілген.



Сурет 1.1 – Хаос генераторы көмегімен Вернамның шифрлеу жүйесінің схемасы

Ашық мәтінді шифрлеу кезінде оның әр символы екілік түрінде ұсынылады. Шифрлеу кілті екілік түрінде де ұсынылады. Бастапқы мәтінді шифрлеу $Y=P\oplus K$ кілтінің екілік таңбаларымен ашық мәтіннің 2 екілік таңбасын модульге қосу арқылы жүзеге асырылады. Шифрды шешу модульге кілтпен шифрлеу мәтінінің 2 таңбасын қосудан тұрады.

Үлкен көлемдегі құпия кілтті алдын-ала беру мәселесін шешу үшін инженерлер мен өнертапқыштар кейбір алгоритмге сәйкес бірнеше қысқа жіптерден жалған кездейсоқ сандардың өте ұзын ағындарын құрудың көптеген схемаларын ойлап тапты. Шифрленген хабарламаны алушы жіберушімен бірдей генератормен қамтамасыз етілуі керек. Бірақ мұндай Алгоритмдер Шифр мәтініне жүйелілік қосады, оларды анықтау аналитикке хабарламаны шифрлеуге көмектеседі. Мұндай генераторларды құрудың негізгі әдістерінің бірі екі немесе одан да көп биттік таспаларды қолдану болып табылады, олардан "аралас" ағынды алу үшін мәліметтер аздап қосылады (1.2-сурет).



Сурет 1.2 – Вернамның жетілдірілген шифрлеу жүйесінің схемасы

Қортындылай кетсем, бүгінгі таңда Вернам шифрлеуі өте сирек қолданылады. Бұл қазіргі криптография әдістері пайдаланушылардың қажеттіліктерін қанағаттандыру үшін жеткілікті түрде дамығандығына байланысты. Алайда, технологияның дамуымен және қол жетімді компьютерлік қуаттардың артуымен сәтті шабуылдың ықтималдығы артып келеді. Қазіргі заманғы деректер тасымалдаушылары кездейсоқ кілттердің көп мөлшерін сақтай алады, ал қазіргі кездейсоқ сандар генераторлары дұрыс сапа шифрінде қолдануға жеткілікті кездейсоқ кілттерді шығаруға мүмкіндік береді. Мұның бәрі Вернам шифрін қолданудың өзектілігін арттыратын байқаймыз.

Қолданылған әдебиеттер тізімі

1. Асосков А.В. и др. Поточные шифры. – М.: Кудиц-Образ, 2003. – 334с.
2. Shannon C.E. Communication Theory of Secrecy Systems //Bell System Technical Journal. 1949. Vol. 28. № 4. – P. 656-715.
3. Птицын Н. Приложение теории детерминированного хаоса в криптографии – М.: МГТУ им. Н.Э. Баумана, 2002
4. Корт С.С. Теоретические основы защиты информации: – М.: Гелиос АРВ, 2014.
5. Столлингс В. Криптография и защита сетей. - М.:Вильямс, 2001.- 669 с.
6. Молдовян А.А., Молдовян Н.А. и др. Криптография. Скоростные шифры. – С.Пб: БХВ-Петербург, 2009. – 493 с.