Дәріс 10.

Интернеттегі мәліметтерді қорғау. Цифрлық қолтаңба.

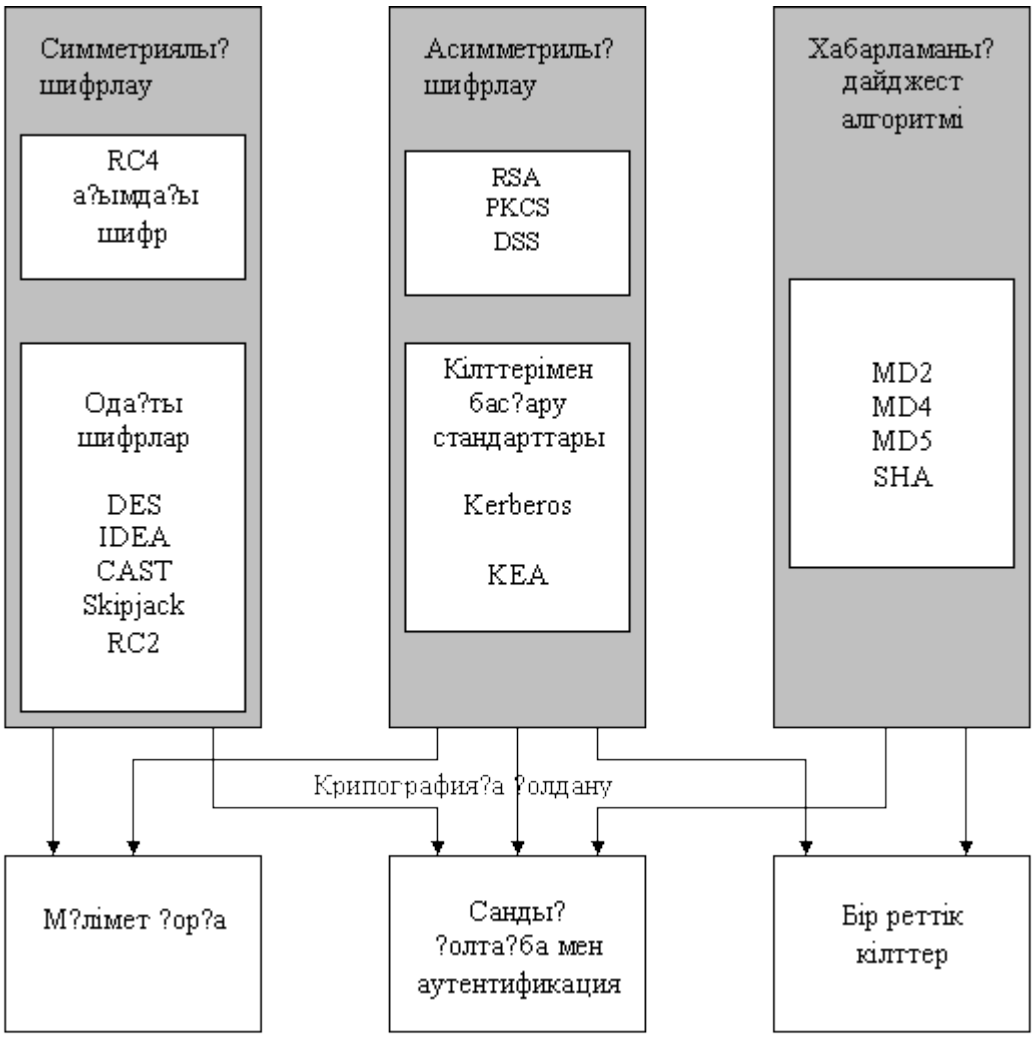
Криптография және Интернет. Симметриялық және асимметриялық кілттер.

Цифрлық қолтаңбаның механизмі. Қауіпсіздік проблемалары.

Нақты мысал қарастырайық. Фирмасының директоры В фирмасының директорына өте қажетті бір құжатты электрондық почта арқылы жіберді делік. Қарап отырсақ мұнда қандай коммуникация қауіпсіздігі пайда болады. В фирмасының директоры бұл хатты алғаннан соң келесідей сұрақтар пайда болады. Шыныменде осы хатты А фирмасының директоры жіберді ма? (Жіберуші идентификациясы). Бұл сұрақтың туындау себебі, бұл құжатты А фирмасының директоры ретінде басқа біреудің де жіберуі мүмкін. Бұл құжатты жіберу кезінде жолдан ұстап өзгертулер енгізген жоқ а? (жіберу аутентификациясы). Бұл құжатты қабылдаушыдан басқа адамдар оқыған жоқ па? (құпияның сақталуы). Бәрімізге белгілі құпияны сақтау үшін мәліметтерді шифрлау арқылы жетуге болады. (жіберу конфиденциялы). Берілген 3 мақсаттарды шифрлау базасы арқылы шешуге болады, онымен криптография айналысады.

Криптография – (Грекшеден аударылғанда Cryptos – құпия деген мағынаны береді) – бұл ғылым және шифрлау технологиясы мәліметтерді өзгертуге және авторлық құқықты сақтайды. Криптография тек қана тексттерді шифрланған формаға аударып қана қоймайды, сонымен қатар, жүйеде жұмыс жасап отырған кезде қолданушының аутентификациясын және идентификациясының берілуін қадағалап отырады. Криптография ең басты қауіпсіз комуникация болып табылады. Біз жүйеде жұмыс жасаған кезде тек қана адамдармен сөйлесіп қана қоймаймыз, сонымен қатар басақада қызметтер барысында араласатынымыз бізге мәлім. Мысалға, біз қандай да бір серверден программа көшіретін болсақ, біз үшін осы сервер шығарушы – фирманың сервері ма, әлде біздің компьютерімізге вирус болып түсетін пираттық фирманың сервері емес па деген ойлар келеді.

Бұл тарауда кейбір стандарт шифрлауы және ақпарат қорғау негіздері сипатталған. 5-1 суретте осы тараудың материалы схемалы түрде ұсынылған.



Сур. 5-1. *Криптографиялық әдістер мен шифрлар*

Шифрлау әдістері

Ортақ мағынада екі шифрлау түрі мүмкін: *симметриялық* (немесе классикалық) және *асимметриялық* (немесе ашық кілтпен шифрлау).

Симметриялық шифрлау

Симметриялық шифрлаудың идеясы математикалық формула түрімен жазылады:

Шифр мәтін = функция (ашық текст, кілт)

Қарсы жақ функция түрі

Ашық мәтін = қарсы жақ функция (Шифр мәтін, кілт)

5-2 суретте симметриялық шифрлау кезінде ақпаратты өзгертуі көрсетілген.

Тіпті тік және кері функция таныс кезінде ашық текстті білімсіз кілтпен қайта құру мүмкін емес. Симметриялық шифрлауде сонымен қатар құпиялы кілтпен шифрлау деп атайды, өйткені құпиялы кілт жіберушіде және қабылдаушыда болуы керек. Келесі бөлімдерде маңызды шифрлаудың симметриялық алгоритмі немесе шифрлар қарастырылған. Шифрдың екі түрі болады: *одақты* және *ағымдағы*. Біріншілер шифртекст одағына (ортақ айтқанда, басқа көлемде) кіретін мәлімет одағын (кейбір көлемді) өзгертеді. Екіншілер – ашық мәтінді шифртекст тактына бір бит бойынша.

DES

DES (Data Encryption Standard) — 56 бит ұзындығымен кілтті қолдана 64 бит бойынша одақты өңдейтін шифр одағы. Ол енді жеткілікті зерттелген. Тестталған және өте тұрақты болып танылған. DES жұмыс режимінің екі негізгісі болады: (Electronic Code Bonk) және CBC (Cipher Block Chaining). Бірінші режимде DES 56-биттік кілтті қолдана 64 бит тактын өңдейді. Сонымен, әрбір одақ басқалардан тәуелсіз шифрланады. CBC режимінда кезекті 64 биттік одағын оған шифрлау үшін «Немесе шығару» алдыңғы одақ операциясы қолданылады. Бұл ашық мәтіннің әртүрлі орындарында болатын 64-битті бірдей одақ әртүрліге шифрланады.

DES аппараттық жүзеге асыру үшін жарамды өте жылдам алгоритм өңделді. DES қолданатын шетке шығару өнімі АҚШ үкіметімен сұранды. ANSI АҚШ ұлттық стандарт шифрлау көмегімен DES қабылданды.

DES алгоритм сенімділігі аз болып көрінгенде triple-DES – модификациясы қолданылады. Жалпы айтқанда Triple-DES бірнеше нұсқауы болады. Ең қарапайым – қайта шифрлау. Екіншіден – алынған шифртекст ашық мәтін бірінші кілтте DBS алгоритммен және ақырында мәліметтер екінші қадамнан алынған – үшіншіде шифрланады. Барлық үш кілт бір-бірінен тәуелсіз таңдалады.

IDEA

IDEA (International Data Encryption Algorithm) — 128 бит кілт ұзындықты тағы бір шифр одағы. Бұл Европаолық стандарт (ETH, Цюрих-тан) 1990 жылы ұсынды. IDEA алгоритмі жұмыс жылдамдығы және анализ тұрақтысы бойынша DES алгоритміне орын бермейді.

CAST

CAST— бұл 128-битті кілтті АҚШ-та және 40-битті экспорт нұсақауында қолданалатын шифр одағы. CAST Northern Telecom (NORTEL) компаниясымен қолданылады.

Skipjack/ Capstone

Skipjack шифрі

АҚШ Ұлттық қауіпсіздік агентімен (National Security Agency, NSA) өңделген Skipjack шифрі 80-биттік кілттер қолданады. Capstone жобасының бөлігі, оның мақсаты – АҚШ үкіметінің талаптарын қанағаттандыратын криптографиялық станларт өңдеуі түсінікті. Capstone өзіне төрт негізгі компонентті қосады:

- Skipjack шифрі;
- DSS (Digital Signature Standard) стандарт негізінде сандық қолтаңба алгоритмі;
- SHA (Secure Hash Algorithm) алгоритм негізінде хеш-функция;
- Барлық жоғарыда айтылғандарды жүзеге асыру микросхемасы (мысалы, осы микросхемада негізделген Fortezza — PCMCIA-плата).

Skipjack жүзеге асыруында паттентелген Capstone микросхемасы қолданылады, оның алгоритмі құпияланған. Қырғын талас «агенстваның делдалы» (escrow agencies) үшін Skipjack кілттер қарастырылған тізгін бойынша жүргізіледі, олар сот талабы бойынша хабарламаны дешифрлауы мүмкін.

RC2 және RC4

RC2 және RC4 Рон Райвеслмен өңделген, USA Data Security компаниясының негізгілердің бірі және осы компаниямен патенттелген. Олар әртүрлі ұзындықты кілттерді қолданады, ал шетке шығару өнімдерінде DES орын ауытырады. RC2 шифрі – 64 бит одақ ұзындығымен одақталған; RC4 - ағымдағы. Жабдықтаушы пікірі бойынша RC2 және RC4 өнімділігі DES алгоритмінен гөрі азырақ емес тиісті болады. 40 бит (және төмен) ұзындық кілтін қолданған кезде шетке шығару шектеулері осы шифрларға таратылмайды.

Ассиметриялық шифрлау

Ассиметриялық шифрлу біздің жүз жылдығымызда 70-жылдарда өңделген. Негізгі идеясы кілттің жұп қолдануында қорытындылайды. Бірінші – *ашық кілт* (public key) – барлығына рұқсатталған және кілт иесіне хабарламаны кім жібереді, сонымен

қолданылады. Екінші – *жеке кілт* (private key) – тек қана иесіне таныс. Ең қызығы асимметриялық шифрлауда екі кілт ереже бойынша өзара ауыспалы. Яғни, жеке кілтте шифрланған ақпаратты тек қана ашық кілтепн, немесе кері қолданып шифрлауды ашуға болады. Бұл қасиет келесі бөлімде айтылатын концепция сандық қолтаңбасы негізінде жатады. Асмметриялық шифрлаудың беріктігі болжауда негізделген, екі қарапайым туындысы болатын өте үлкен натурал санының бөлгішін іздеу көп еңбектің процедурасы.

Осы болжаудың математикалық дәлелі болмайды, бірақ ол тәжірибемен расталған. Ашық кілтпен криптографияның негізгі идеясы 5-3 суретте көрсетілген.

3 суреттің үстіңгі бөлігінде қабылдаушының ашық кілт қолдануымен мәтіннің шифрлануы көрсетілген. Қабылдаушы хабарламаны оқу үшін өзінің жеке кілтін қолданады. Бұл тек мекенжай хабарламаның шифрын ашуын кепілдейді. Суреттің төменгі бөлігінде асимметриялық шифрлаудың басқа әдісі көрсетілген – жіберушінің жеке кілтімен шифрланған және жіберушінің ашық кілтімен шифрды ашу. Егер ашық мәтін қабылдаушыға алдын-ала танылса, онда осы әдіс негізінде сандық қольтаңба құрылады, өйткені хабарламаның мұндай түрі (алдын-ала анықталған ашық мәтінмен) жеке кілтін білетін бір жіберушіден ғана келуі мүмкін.

RSA

RSA шифр атауында онышығарған фамилиясы кодталған: Рона Рай вест (Ron Rives!), Ади Шамир (Adi Shamir) және Леонард Элдемал (Leonard Aldeman) — RSA Data Security компаниясының негіздеушілері. RSA өте танымал ғана емес, сонымен жалпы танымал шифр. RSA математикалық дәлелі мынандай: екі қарапайым туындысы болатын өте үлкен натурал санының бөлгішін іздеу көп еңбектің процедурасы. Сонымен қатар ашық кілт бойынша оңың жеке жұп кілтін есептеуге өте қиын. RSA шифрі жеткілікті ұзындық кілт кезінде барлық жақты зерттелген және күшті болып танылған. Мысалы, 512 бит күштілікті қамтамасыздандыру үшін жетпейді, ал 1024 бит мүмкін нұсқау болып есептеледі. Кейбірі RSA процесс күштілігінің өсуімен толық асып кету шабуылына тұрақтылықты жоғалтады. Бірақ процессордың күштілігін артуы тұрақтылықты көбейтетін аса ұзын кілттерді қолдануға рұқсат етеді.

PKCS ашық криптографияның стандарты

PKCS (Public Key Cryptography Standards) стандарты Microsoft, Apple Digital Equipment, Sun Microsystems және Lotus қоса RSA Laboratories және біріккен компаниялармен ұсынылған. PKCS отбасында көптеген әртүрлә стандарттар (оның көбісі PKCS болашақта қосу үшін дайындалады), олардың әрбіреуі бөлек аймақты сипаттайды (кесте 5-1). (PKCS 2 және PKCS 4, PKCS 1-де біріктірілген).

Кесте 5-1. PKCS стандарты

Аты	Сипаттама
PKCS 1	RSA ашық кілт көмегімен шифрлау
PKCS 3	Диффи-Хеллман (Diffe-Hellman) хаттамасының алмасуы және кілттердің келісуі
PKCS 5	Құпиялы кілтті қолданумен шифрлау
PKCS 6	X.509 көптеген сертификаттардың болуымен формат сертификаты
PKCS 7	Шифртекст және сандық қолтаңбасы болатын хабарлама синтаксисі
PKCS 8	Жеке кілтердің форматы
PKCS 9	Басқа PKCS қолданатын мәлімет құрылымы
PKCS 10	Сертификацияға синтаксис сұранымы
PKCS 11	Криптографиялық функцияларды қолданатын құрылыс үшін API сипаттайды, мысалы смарт-карта үшін

DSS стандарты

DSS (Digital Signature Standard) стандарты АҚШ үкіметімен қабылданды.Қолданбалы кілт ұзындығы 512-ден 1024 бит шамасында түрлендіреді. DSS сандық жазбаны құру үшін, бірақ ақпаратты жабу үшін арналған. DSS стандартында кейбір қорғау орындары табылды, нәтижесінде ол кең таратылады.

Дайджест хабарламаның алгоритмдері

Шифрлауды қолдану туралы айтуды бастамай тұрып, мысалы аутентификация немесе сандық жазба үшін дайджест хабарламасының алгоритмін есептеуді қарастыру пайдалы. Олар ассиметриялық шифрлау алгоритмдарымен бірге сандық жазба жүйесінің негізіне салынған.

Біріншіден *хэш-фукциясын* (hash function) қарастырайық. Ол кіруге айналмалы бит санын алады және шығу кезінде бекітілген ұзындық – жол хэш-код береді. Егер хэш-фукцияға қаратуға өте қиын болса, онда хэш-кодты *дайджест хабарламасы* (message digest) деп атайды. Дайджест хабарламасының есептеу алгортмі бірегей хэш-кодты болжайды.

MD2, MD4 және MD5

MD2, MD4 және MD5 — Рон Райвестпен өңделген дайджест хабарламасының алгоритмі. Олардың әрбіреуі 128-битті хэш-кодты өңдейді. MD2 алгоритмі — өте баяу, ал MD4 — өте жылдам. MD5 алгоритмі MD4 модификациямен есептеуге болады, қауіпсіздікті арту үшін жылдамдықпен құрбан етеді. Толық ақпаратты сіз RFC 1321 (MD2), RFC 1320 (MD4) И RFC 1319 (MD5)-тен таба аласыз.

SHA

SHA (Secure Hash Algorithm) — бұл 160-битті хэш-кодты өңдейтін, дайджест хабарламасының есептеу алгортмі. SHA алгоритмі АҚШ (Capstone жобасының бөлігі ретінде) үкіметімен қабылданды. Ол MD4 және MD5-тен сенімді қайталағыш хэш-код қайта құрылған әртүрлі кіру кезеңімен ықтималдықты кемітетін ұзын хэш-код өндіреді.

Шифрді қолдану

Жоғарыда жазылған әдіс негізімен шифрді қолдану әдісінің көптеген қызықтары өңделді. Оның кейбіреуі келсі бөлімдерде жазылған.

Ақпараттар мен канал байланыстарын қорғау

Қорғау құралдарының қолдануы канал байланыс бойынша ақпарат жібері кезінде жасырынды кепілдейді. Мысалы, Netscape компаниясының 2 және 3 версиялары SSL (Secure Socket Layer) және Microsoft компаниясының PCT (Private Communication Technology) транспорттық деңгейде ақпаратты қорғауға рұқсат етеді. SSL және PCT криптографиялық қосымша ретінде ғана танымал емес. Олар транспорттық деңгейдің интерфейсін қолданатын программистер үшін API ұсынады. SSL және PCT төменгі тарауда жазылған.

Сандық қолтаңба

Сандық қолтаңба (digital signature) — бұл ақпарат ішіндегі біртұотастықты және оның нағыз жіберушіні тексері әдісі. Ол ассиметриялық және хэш-функциялар көмегімен жүзеге асырады. Сандық қолтаңба ассиметриялық шифрға қарауға негізделген, сонымен қатархабарламаның ішіндегі байланыстыққа қолжазба және кілт жұбының өзін: осы элементтің біреуін өзгерту нағыз қолтаңбаның рұқсатнамасын

мүмкін емес жасайды. Сандық қолжазбаның алгоритм жұмысы 5-4 суретте көрсетілген.

Жіберуші дайджест хабарламасын (суретін сол жақ үстіңгі бұрышта) табады. Оны өзінің жеке кілтімен шифрлайды және хатпен бірге жібереді. Қабылдаушы хабарламаны алып жіберушінің ашық кілтімен дайджест шифрді ашады. Бұдан басқа қабылдаушының өзі қабылданған хабарламадан дайджеситті тауып, оны шифр ашумен салыстырады.

RSA негізінде сандық қолтаңба

RSA шифр сонымен қатар сандық қолтаңбаны өңдеу және тексеру үшін қолданады. Хабарламаға қолтаңба жазу үшін жіберуші оны өзінің жеке кілтімен шифрлейді және хабарламамен бірге қолжазбаны жібереді. Жіберушінің ашық кілтпен қолжазбаны шифрді алу және қабылдаған хабарламамен нәтижені салыстырады. Егер хабарлама жалған болса, онда алынған және шифрі ашылған хабарлама сәйкес келу керек.

Жіберуші ақпаратты жабу үшін RSA қолдану кезінде қабылдаушының хабарламасын ашық кілтпен шифрлейтінін байқайық (жіберушінің жеке кілті қолданатын сандық қолтаңба ерекшелігінде).

DSS сандық қолтаңбаның стандарты

DSS (Digital Signature Standard) стандарты – бұл АҚШ үкіметімен кепілденетін қолдануымен ассиметриялық шифр. Мұнда кілттің ұзындығы 512-ден 1024 битке дейін қолданылады. DSS стандарт тек қана сандық қолтаңба таңдау үшін, бірақ мәліметтің жабылуы үшін емес қолданылады. Ол ұлттық стандарт және технология институтымен (National Institute of Standards and Technology, NIST) өңделген DSA (Digital Signature Algorithm) алгоритмінде пайда болды.

DSA/DSS RSA негізінде таралған сандық қолтаңбаны ауыстырадыма – сұрақ, бұған тек қана уақытпен ғана жауап беруге болады. Сыншылар DSA/DSS көптеген кемшіліктер бар болуын көрсетті, оның кейбіреуі жойылған. Бір проблема қалды - DSA қолтаңбаны тексеру кезінде процессор (және уақытымен) қорларын есептеуге оның құрылуынан гөрі талап етеді.

Уақыт белгілерінің қызметтер

Сандық қолтаңбаны қолдай отырып, уақыт белгілерінің қызметтері (Time Stamping Service) концепциясына сәйкес сенімді делдал, қолтаңбаға уақыт белгілерін қосу. Осылай сенімді делдал сол фактті растайды, көрсетілген абонент құжатты көрсетілген күн мен уақытқа қол қояды.

Аутентификация

Аутентификация көмегімен сіз ақпарат алмасу кезінде ол өзін кім болатынын шынайы пайдаланушы немесе процесс екеніне сенімді бола аласыз. Аутентификация әдістері көп. Кейде оны бірегей құрам бойынша әкелді, пайдаланушыға немесе процессорға болатын, мысалы, саусақ іздері бойынша. Немесе кейбір бірегей ақпараттың пайдаланушының немесе процессордың білімі бойынша. Сандық қолтаңба жағдайында жіберушінің жеке кілтті болады. SSL және PCT тек қана жасырын ақпаратты қамтамасыздандырмайды, сонымен қатар аутентификация қызметтерін ұсынады.

Аутентификация тағы бір ортақ әдісі - Microsoft.NTLM Challenge/Response хаттамасы, OS/2 операционды жүйе үшін LAN Manager бірінші версия негізінде өңделген. Клиент сервермен қосылады, ал ол клиентке сұраным жібереді. Клиент пайдаланушы паролінің хэш-код негізінде жауапты таңдайды және оны серверге жібереді.Сервер Microsoft Windows NT басқарумен пайдаланушы паролі туралы ақпаратымен иегеретін хэш-кодты тәуелсіз тауып алуды біледі және клиенттің түзету жауабын жүргізеді. Сервер қатаң түрде айтқанда басқа доменде болуы мүмкін: Бұл жағдайда пайдаланушының сұранымын тексеру үшін рұқсатқа тексеріс Windows NT құрамы қолданылады. Тамаша құжатталған API Microsoft NTLM Challenge/Response қолдануын жеңілдетеді. Сонымен программистке криптографиялық алгортимді нақты оқуға қажет емес. Бірақ ең бастысы пайдаланушы пароль осы тарауда «Поставщик услуг безопасности в Windows NT» бөлімінде – нақтылық ашық түрде байланыс каналдары бойынша ешқашанда жіберілмейді.

Authenticode

Authenticode — Microsoft Internet Explorer 3.0. бірінші қолданылған Microsoft компаниясының жаңа баласы. Бұл технология бағдарламалық кодтан енгізілген туындысын пайдаланушы құралдарымен тексеру мүмкін, және өзінің бағдарламаларын жабдықтауды рұқсаттайтын API.

Authenticode технологиясын қолдана отырып нағыз жібеушіге сол сияқты жинақтылыққа Интернет кодынан енгізілгенін тексеруге болады. Мұнда ассиметриялық криптография қолданатыны анық. Сертификациялық қызметт ретінде Verisign шығады. Бағдарламалық қамтамасыздандыру пайдаланушылары мен өндірушілері біреудің сертификаттарын тексеруге және өзінің сертификаттарын алуға болады.

Internet Explorer браузері Интернет жүйесінен енгізілетін бүкіл код тексерілгенде пайдаланушыға мұндай деңгей қауіпсіздігін таңдауға рұқсаттайды. Ассиметриялық шифрді қолдана пайдаланушы кез-келген алынған бағдарламалық кодтан нағыздың өзін тексереді. Windows Trust Verification Service бағдарламасының көмегімен клиент қауіпсіздіктің басқа деңгейін береді, мысалы нақты компаниядан түсетін қауіпті емес, немесе теріс тексерісті талап ететін барлық кодты есептеу.

Бір реттік кілттер

Шифр алгоритмінің – симметриялық және асимметриялықтың қай түрін қолдану қажет? Тәжірибеде екі әдіс қолданылады. Асимметриялық симметриялықтан едәуір баяу. Сондықтан жіберуші кездейсоқ құпиялы кілтті өңдейді және оның құрамымен хабарламаны (симметриялық алгоритммен) шифрлайды. Хат қабылдаушының (ашық кілтпен алгоритм) ашық кілтімен шифрланған құпиялы кілтпен бірге жіберіледі. Осындай кездейсоқ бейнемен өңделген кілт *бір реттік* (message key) деп атайды.

Ұқсас жағдай хабарламаны бірнеше қабылдаушыларға қатар тарату қажет болғанда туындайды. Асимметриялық тізбек щифрлау кезінде хабарламаны әрбір абонент үшін оның ашық кілтін қолдана бөлек шифрлау қажет болады. Бұл көп уақытты үнемдейді. Бұның орнына хабарламаны кездейсоқ өңделген құпиялы кілтпен шифрлап және содан кейін тек қана құпиялы кілтті әрбір қабылдаушының ашық кілтімен шифрлау қажет.

SET хаттамасы

SET (Secure Electronic Transaction) хаттамасы Интернетте мүмкіндіктер мен сауда қызмет рамкасын кеңейтуін рұқсат етеді. SET ерекшелігі Microsoft, Netscape, IBM және GTE қатысуымен, Visa және MasterCard компанияларымен бірге өңделді. SET ерекшелігінің соңғысы үш томна тұрады: бизнес – сипаттама, хаттама және программист басшылығының сипаттамалары. SET – бұл технология несие карталары туралы Интернет арқылы және API Интернетте сауда қосымшаларын өңдеу үшін қорғалған жіберу. SET хаттамасында ақпаратты шифрлау үшін DES, ал құпиялы кілтті және несие картасының номерін шифрлау үшін – RSA қолданылады.

SSL хаттамасы

Winsock хаттамасы 3-ші тарауда жазылған. SSL (Secure Socket Layer) хаттамасы оны толықтырады: ол клиентке сервер мәліметімен алмасатын қорғау мәліметін және аутентификацияны қолдануға рұқсат береді. Сеанс байланысы инициализация кезінде SSL хаттамасы симметриялық сеанс кілтін (session key) жәнешифрлау алгоритмін байланыстыру қажет. Симметриялық кілт мәліметті шифрлау және шифрды ашу үшін қолданады. Сол уақытта (сеансты орнату) клиент пен сервердің аутентификациясын орындауға болады. Байланыс сеанс параметірі біткенде шифрлауды қолдан клиент және сервер ақпартпен қауіпсіз алмаса алады. Сеанс орнату уақытында SSL хаттамасы ашық кілтпен RSA қолдайды: RC2, RC4, IDEA, DES және Triple-DES — ақпаратты шифрлау үшін; MD5 — дайджест хабарламасы үшін.

Соңғы, үшіншіні SSL версиясын Netscape сияқты браузерлер, сол сияқты Microsoft қолдайды.

PCT хаттамасы

PCT (Private Communication Technology) хаттамасы клиент-сервер қосымшалары үшін қорғауды қамтамасыз етеді. Идея – клиент және сервыер

арсында бөтен ақпарт алмасуынан жасырады. Сервер әрқашан сенімді, ал клиенттер - әрқашан емес болып саналады.

PCT функционалды SSL-ға ұқсас. SSL сияқты PCT сеанс байланысын орнату кезінде клиент құпиялы кілтпен симметриялық олгоритім шифрлаумен (ол мәлімет шифрлау үшін қолданылады) үйлестіреді. SSL-дан негізгі айырмашылық PCT аутентификацияны шифрлаудан айырады және сондықтан сенімді механизім аутентификациясы ие болуы мүмкін және АҚШ экспорт шектеуімен сай келеді (ескертейін, АҚШ үкіметі 40 биттан артық ұзындық кілтімен шетке шығару жүйе шифрлауын тиым салады). Басқа да айырмашылықтар бар. PCT аса тиімді, өйткені аз хабарламаны қолданады және олар SSL салыстыруы бойынша өте қысқа. Кілтпен басқару үшін RSA, Диффи-Хеллман және Fortezza алгоритмдерін қолдайды: DES, RC2 және RC4 - мәлімет шифрлау үшін, USA және KSA – сандық қолтаңба үшін.

PCT 3 немесе жоғары Microsoft Internet Explorer версиясында, сонымен қатар 2 Microsoft Internet Information Server (IIS) версиясынан жоғары жүзеге асырылған. Басқа компаниялар, мысалы Spyglass және Open Market PCT қолдауы туралы мәліметі.

Транспорт деңгейінің қауіпсіздігі

IETF жұмыс тобында - Transport Layer Security (транспорт деңгейінің қауіпсіздігі) құрылды, ол SSL, PCT және Secure Shell Remote Login негізделген транспорттық деңгейдің бірлік интерфейс қорғауын құруға талпынады. Microsoft компаниясы SSL версия 3 және PCT версия 2 болашақ біріктіруін есептей бұл бастауды қолдайды.

Сертификаттар

Ассиметриялық шифрлау құпияда жеке кілттің сақталуын талап етеді. Осыдан басқа ашық кілт және нақты адам, процесс немесе объект салыстыруымен сенімді әдіс қажет.

Ашық кілт шынында Джон Доу-ға жататынын қалай білуге болады? (егер, мысалы, Джейн Доу өзінің ашық кілтін Джон Доу кілті сияқты әлеуметтесе, онда Джона Доу үшін барлық хабарламаны оқып шыға алады). Қандай да бір жүйеде пайдаланушы мен оның кілтін тиімді байланыстыратын *сертификат* (certificate) – объект көмектеседі. Сертификат басқа да ақпаратты, мысалы аяқталу күнін ұстайды. Оны сертификацияланған қызмет (certificate authority, CA) береді және қол қояды, бірақ бұл проблеманы толық шешпейтінін байқаңыз.

CA-ның өзімен біз ашық кілттің шынайы екенін қалай тексереміз? Әрине, тағы бір CA (тағыда, тағыда) қосып, даусыз сенімді CA-ға дейін жетпегенше. Менандай тізбек рұқсатталған: CA корпоротивті, оған барлық компанияның қызметкерлері, өте жоғары деңгей CA аймағы, мемлекеттік CA және т.б. сенеді.

Сертификат серверлері

Сертификаттар каталог қызмет объектілері сияқты немесе осы сервер үшін арнайы ерекшелігінде сақталады. Microsoft, сол сияқты Netscape құрылған сертификат сервер БҚ болады. Уақыттан уақытқа сертификатты шақыру қажет.

Ол үшін олрды CA-мен басылған айдатылған сертификат тізіміне (certificate revocation list, CRL) енгізеді (CRL сақтау толықтығымен бұл кітаптан шығатын сұрақ қатарын тигізеді.

X.509

X.509 — бұл формат және синтаксис сертификатын сипаттайтын стандарт. Қатаң айтқанда X.509 аутентификация қызметін сипаттайды (бірақ қолданылмайтын криптографиялық алгоритм), бірақ X.509 сертификат синтаксисімен ассоцияланады. Аутентификация және мәлімет қорғауға байланысты әртүрлі стандарттар, мысалы, SSL, Secure HTTP (S-HTTP, 14 тарауда жазылған). Privacy Enhanced Mail (PEM, 9 тарауда жазылған) X.509 сертификатын қолданады. Кең таралған X.509 сертификаты электронды коммерция ортада қабылдап алады. Бірінші X.509 версиясы 1988 жылы қаланды. Ағымдағы версия – үшінші.

Сертификаттің басты міндеті – пайдаланушы және оның ашық кілтпен арасында бір мағыналы сәкес орнату. X.509 сертификат стандартының кейбір өрісі:

- X.509 номер версиясы;
- Аутентификация қызметінің идентификатор алгоритмі;
- сертификат берген мекеменің аты;
- сертификаттың аяқталу мерзімі;
- пайдаланушының ашық кілт туралы мәлімет.

Кілттермен басқару

Жоғарыда айтылғандай, жеке кілттерді жасырын сақтау керек, сертификаттармен басқару қажет, алсимметриялық алгоритм шифрлауымен қолдану кезінде құпиялы кілт және олармен алмасуды қауіпсіз басқару қажет. Kerberos – барлық осы міндетті орындайтын қосымшалардың бірі.

Kerberos

Kerberos хаттамасында Массачусетс технологиялық институтпен (Massachusetts Institute of Technology, MIT) өңделген, бірнеше функциялар жүзеге асырылған. Оның біреуі – мәлімет негізінде сақталған жеке кілттерді сақтау. Бұл кілттер тек қана Kerberos және оның иелеріне таныс. Тағы бір фукция – құпиялы кілтпен алмасатын екі абонент арасында сенімді делдал. Сол мағынада сенімді екі жақ оның сенімділігінде күдіктенбейді. Сонымен қатар Kerberos аутентификация қызметін және кілтті жіберуді ұсынады. Оның ішінде DES алгоритм шифрлауда қолданылады.

Kerberos қорғаудың үш түрі бар. Қандай деңгей оның қажеттілігін пайдаланушы өзі шешеді. Kerberos желілік шығарма орнату кезінде аутентификацияны жүргізеді, және ары қарай клиенттер осы желілік мекенжайдан

дұрыс түсетін барлық ақпаратты есептей алады. Кейбір* пайдаланушылар (немесе қосымшалар) Kerberos әрбір хабарламаның дұрыстығын тексеріп, бірақ оның ішіндегісін шифрламай қояды. Бұл *қауіпсіз хабарлама* (safe messages) деп аталатын. Жоғары деңгей қаупсіздігі кезінде ірбір хабарлама дұрыстылыққа тексеріледі және шифрланады.

Kerberos билет (ticket) ерекшелеу қызмет принципі бойынша жұмыс істейді. Мысалы, пайдаланушы клиент жүйесінде тіркеледі. Оған өзінің атын енгізуге ұсынады, ал содан кейін Kerberos аутентификация серверіне сұраным жібереді. Ол осындай есіммен пайдаланушының бар болуын тексереді және дұрыс жауап жағдайында қездесоқ кілтті өңдейді. Содан соң ол ағымдағы уақытты, уақыт өмірінің билетін, клиенттің IP-мекенжайын ұстайтын және жаңа ғана өңделген сеанстты кілтті құрады. Одан әрі аутентификация серверіне ғана таныс осы ақпарат кілтті шифрлайды. Мұндай билет пайдаланушының жеке кілтімен шифрланады және клиентке жіберіледі. Сосын клиенттік жұмыс станция пайдаланушының паролін сұрау жасайды, билетті шифрды ашуға болатын және билетті сақтайтын DES кілтімен оны өзгертеді. Ол аутентификация серверіне жеке пайдаланушын қолдау үшін керек болады.

Диффи-Хеллман алгоритмі

Диффи-Хеллман (Diffe-Hellman) алгоритмі кілтпен алмасу үшін кең қолданады. Ол қорғалмаған канал байланыс бойынша ақпарат алмаса екі абонентке тәуелсіз бірдей кілтті есептеуге рұқсат етеді. Диффи-Хеллман алгоритмі оны дұрыс қолдануы кезінде (ұзындық кілтімен сәйкес) табанды болып саналады. Бұл алгоритм АҚШ-та патенттелген, бірақ 1997 жылы патент мерзімі өтіп кетті.

KEA алгоритмі

KEA (Key Exchange Algorithm) алгоритмі кілтпен алмасу үшін ғана жарайды, бірақ ақпаратты қорғау үшін емес. Ол Диффи-Хелман модифициаланған версия алгоритмінда негізделген және 1024-биттік кілтті қолданады.

SKIP хаттамасы

SKIP (Simple Key Management for Internet Protocols) — Бұл Sun Microsystems компаниясымен өңделген кілтпен басқару хаттамасы. SKIP оңай жүзеге асырылады. Оның ішінде ашық кілт сертификаты негізінде кілтті есептеу әдісі сипатталған. Бірақ SKIP қолдануы алгоритм шифрлауын және хешты таңдауға нақты шектеулер салынады. SKIP хаттамасы IPSec (Internet Protocol Security) ерекшелігін маңызды емес компонент сияқты мәлімделген – 3 тарауды қараңыз.

ISAKMP хаттамасы

ISAKMP (Internet Security Association and Key Management Protocol) хаттамасы IPSec міндетті қолдауға жатады. SKIP oil хаттамасымен салыстыру бойынша алгоритм шифрлауын және хештауды өте иілгіш қолдануға рұқсат етеді.

Криптоталдау және шабуыл

Криптоталдау — бұл білімсіз кілт ақпартының ашық текстіне шифр текстін қайта құру туралы ғылымы. Кез-келген шифр сенімді, оның сенімділігі соншалық, кілтті өңдеу немесе оларды тарату өте баяу орын.

Алгоритм шифрінің көбісі бәсекеленбеген дауыссыз болатын, бірақ қатаң дәлелі болмайтын жобалауда негізделген. Жоғарыда айтылғандай, мұндай болжаулардың біпеуі мынандай: екі қарапайым туынды болатын іздеу бөлімі үлкен натурал саны өте қиын.

Есептеу техника күштілігінің өсуімен тіпті шабуыл толық асып кету (келесі бөлімде сипатталған) мүмкін емес болмайды.

Бұл кілттің ұзындығын үлкейтуді мәжбір етеді, ол АҚШ, ФБР және ҰҚА (ұлттық қауіпсіздігінің агенттігі) үкіметінің қызығушылығына қарсы болады, кез-келген хабарлама мүмкіншілікті дешифрлауға болады.

Есептеу техникасының қуатының өсуімен қатар тіпті, толып кетудің шабуыл да (келесі тарауда жазылған) мүмкін еместей көрінбейді.

Бұл кілт ұзындығын үлкейтуге мәжбүр етеді, ол АҚШ өкіметінің, жекеше алғанда ФБР мен ҰҚА (Ұлттық Қауіпсіздік агенттіліші) көзқарастарына қайшы келеді, олар өз есебінен кез-келген хатты шифрсіздеуге тілек білдіреді. Заң бойынша максимальды ұзындықтарын шектеп, өздерін ыңғайлы сезінеді.

ТОЛЫҚ ТОЛЫП КЕТУ

Толық толып кетумен шабуыл (brute force attack) барлық мүмкін кілттерді сынап көруге негізделген. Бірақ мәселе сонда, кілт ұзындығы өскен сайын есептеу көлемі де экспоненциалды түрде өсіп отырады. Кейбіреулер есептеу техникасының қуаты өскен сайын шифрлар беріксіз болады деп жорамалдайды. Бірақ, екінші жағының, бұл өте ұзын кілттерді қолдануға мүмкіндік береді.

Шифрмәтінге шабуыл

Шифрмәтінге шабуыл (cipher-text-only attack) шабуыл жасаушыда тек шифрмәтіні бар деп жорамалдайды. Ал тәжірибе жүзінде, ол хат мазмұны жөнінде кейбір мәліметтерге сүйеніп, оларды қолдану мүмкін.

Ашық мәтін бойынша шабуыл

Ашық мәтін бойынша шабуыл (chosen-plain-text attack) жасаушының өзі тағайындаған кез-келген мәтінді шифрлау мүмкіндігі бар деп жорамалдайды. Мұндай жолмен, шабуыл жасаушы кілтті шешпекші болады. RSA шифрі мұндай шабуылдарға сезімтал келеді.

Белгілі мәтін бойынша шабуыл

Бұл жағдайда ашық мәтін бөлігі немесе барлығы оған сәйкес шифрмәтінді ілуі жорамалданады. Осыған сүйене отырып, ол кілтті табуға талпынады.

Уақыт бойынша шабуыл

Бұл шабуылдың жаңа түрі. Шабуыл жасаушы модульді потенциялау амалына қажет уақытты өлшейді (берілген модуль бойынша дәріжеге шығарады), және

осы ақпаратты қолдануға тырысады. Диффи-Хеллман RSA ширі шабуылдың бұл түріне қарсы тұра алмайды.

«Делдал» шабуылы

Шабуылшы ақпарат алмасып жатқан екі абонент арасына енеді. Егер кілт алмастыру кезінде енсе, ол келесі хаттарды шифрсізде мүмкіндігіне ие болады. Өзін тауып алмас үшін, ол хаттарды дұрыс шифрлеп, мекенжайларына жөнелту арқылы ұзақ уақыт бойы жасыруы мүмкін. Ұқсас шабуылдардан қарапайым қорғану тәсілі – сандық жазбаны қолдану.

Кілтті шешу

Алгоритм беріктігіне қарамастан, қолданушы (немесе құрушы) толық немесе жекелей шешуге тап болатын беріксіз кілттерді пайдалану арқылы әлсіздетуі мүмкін. Мысал - Netscape Navigator бета-версиясының қорғанысын жүзеге асыру. Мұнда шифрлауға арналған кілт бөлігі, ағымды уақытта негізделген.

Тағы бір мысал — Microsoft Windows for Workgroups 3.11, пароль файлын қолданды. Қолданушы жүйеде тек бір рет тіркелген, ал басқа компьютерлер қорларына енуге рұқсат қажет болғанда, ол әр түрлі парольдар енгізуге мәжбүр болған. Windows for Workgroups бірінші версиясының мәселесі – қолданушы аты кілттің бір бөлігі ретінде қолданған. Осылай, шабуыл жасаушы парольдар файлын шифрлеуге мүмкіндік беретін кілттің мәнді бөлігін алып отырған. Бұл жүйе қазір жаңартылған.

Криптография және API

Бұл бағдарламаушыларға олар жасап жатқан тіркемелерге қауіпсіздік құралдарын қосуға мүмкіндік беретін API бөлімі көрсетілген. Кейде тіркеме мен API арасында шектеу жүргізу қиынға соғады. Алдыңғы бөлімнен, сіз SSL — хаттамасы – транспортты деңгейдегі бағдарламаушыларға API, ал одан жоғары деңгейде – мәліметтерді қорғауды қамтамасыз ететін тіркеме басып табылады.

Ақпарат және байланыс арналарын қорғау

Қорғаныс құралдары байланыс арналары бойынша берілу кезінде ақпараттың жасырушынышылығын қамтамасыз етуге мүмкіндік береді. Мысалы, 2,3 версиясының SSL және PCT ақпаратты транспортық деңгейде құрайды. SSL-де PCT-де криптографиялық қосымша ғана емес, транспортты деңгейде жазатын бағдарламалаушыларға API болып табылады.

Windows NT-де қауіпсіздік қызметтерін жеткізуші

NT Security Service Provider Interface (NT SSPI) — 3,5 версия Windows NT-де алғашқы жүзеге асырылған API. Ол қосымшамен жүйе қауіпсіздігінің ядросы арасындағы қабықша болып табылады. Бұл қауіпсіздік үлгісін оңайлықпен жаңартып, қосымшаны жобалауды жеңілдетеді. Мысалы, қосымша кейде қорғалған байланысты орнатып, ққолданылатын сұлба жайлы ештеңе білшісі келмегені мүмкін немесе ол әрбір хаттама қол қюды талап етеді. Алғашқы

рет SSPI LAN Manager және NTLM (Microsoft желілері үшін) MSN-диалектісінде, көптеген өндірушілер басқа қауіпсіздік қызметтерін жеткізушілеріне қаралады.

Microsoft-тан криптографиялық API

SSPI крипотграфиялық амалдардың негізді жиынын бейнелеу кезінде, криптографиялық API (CryptoAPI) есептердің кең ауқымды ширегін Microsoft CryptoAPI қосымшларды әртүрлі қосымша крипографиялық тәсілдерді қолдану арқылы хаттарды шифрлеуге немесе жазуға мүмкіндік береді, сонымен қатар хаттарды, шешіп, жазбаларын тексеруге мүмкіндік береді. Тәсілдер CryptoAPI-ге қосылатын криптографиялық қызметтер жеткізушілерімен жүзеге асырылады (cryptography service provider, CSP). Бұл жаңа CSP-ға қосымшаның минималды модификациясын қажет болғандықтан, өте қолайлы.

I версияның CryptoAPI «RSA» деп аталатын CSP базасымен беріледі:

- 40-биттік RC2 және RC4;
- 512-биттік RSA;
- MD2 және MD5;
- 160-биттік SHA.

2 версиядағы CryptoAPI-ға сертификаттар қосылған Ол 3 версиядағы X.509 сертификатымен, сонымен қатар PKCS 7 және PKCS 10 ен жұмыс істей алады.

Microsoft компаниясы CryptoAPI-ді платформа-аралық ретінде жасап, оны Windows-жүйесінде ғана емес, басқа жерлерге де таратпақшы. Ол үшін Microsoft KSA компаниясының CryptoAPI-ді заңдастырып, оны өз өнімдерінің құрамында шығаруға мүмкіндік береді

Microsoft Wallet және PFX

Microsoft Wallet сандық қалтасы жеке ақпаратты берік сақтауға арналған, ол PFX (Personal Information Exchange) — одан мәліметтердің қауіпсіз берілуі үшін арналған. Wallet жасырын ақпаратты сақтауға арналған, мысалы, әлеуметтік сақтандыру номері, несие карталары мен сертификаттар номері. Microsoft Wallet алғашқы версиясы 1990 жылы жарық көрді, ол 2.1 версиясы қазіргі уақытта да Internet Explorer 4.0. құрамында беріледі. Қалта қолданушы компьютеріндегі мәлемтті сақтауға арналған. Номға бөтен кісілерді рұқсатын шектеі айдан анық. Ол үшін PFX арналған — ол ақпаратты сақтау және оны қалтадан алып шығару механизмдердің көшірме жазбасы. PFX қызметтерінің бірі — сандық қалтаны мобильді түрге келтіру, қолданушы оны жұмыс компьютерінен үйге және керісінше тасымалдауға мүмкіндігі болуы қажет. Microsoft Wallet — криптографиялық тіркеме екендігі анық, ендеше PFX – API болып табылады. Парольдерді қорғауға қосымшаны өздігінен қарап шығуға мүмкіндік беретін, тек оның дұрыстығын тексеретін API құрылған. PPX бейнесі болашақ стандарт негізі ретінде W3C (World Wide Web Consortium) жіберілген.

Authenticode

Бір жағынан, Authenticode технологиясы бағдарламалық код келіп түскен мекеме немесе жеке адамды тексеруге мүмкіндік береді. Екінші жағынан – құраушылар мен мекемелерге өз бағдарламалық кодын жазуға мүмкіндік беретін API бейнеленеді. Authenticode мұндай құралдарымен алынған код бүтіндігін тексере алады (зақымдардың болмауы).

Authenticode технологиясы асимметриялы шифрлеуге негізделіп өз кодын жазатын мекемелер мен субъектілердің ашық кілттерін алу және басқарауға арналған Verisign қызметін қолданады. Authenticode PKCS 10 (сертификатталған сұраныстар), X..50Э (сертификатталған ерекшелігі) және SHA және MD5 (хештау) алгоритмдеріне негізделген.

Java API тобы

Бұл API тобы әлі даму үстінде. Қайтадан пайда болған Java API бұрыңғы тіркемелермен жұмыс істеп мәліметтер базасымен өзара әсерлеседі. JDBC (Java Database Connectivity) интерфейсі мәліметтер базасы мен өзара әсерлесу SQL-құрылғыларына қол жеткізуге мүмкіндік береді. Java IDL – объективті-бағыттаушы интерфейс болып табылады. Java RMI - Java-объекттер арасында таратылған өңдеу құралы. Java Server API — серверлерге рұқсат және сервелет (servlet) деп аталатындарды құрау – сервер мүмкіндігін кеңейтетін апплеттер. Java Management API ұйымдық желілерді басқаруға арналған апплеттер құруға мүмкіндік береді, Java Media API — мультимедиялық қосымша. Java Security API криптографиялық құралдарды, мәліметтерді қорғау, сандық қотаңба мен аутентификацияларды бейнелейді, JavaBeans API объекттің бар үлгілерімен өзара әсерлесуін жүзеге асырады, мысалы, COM CORBA, OpenDOC және OLE.

болады., ал оның шифрын екі пардағы кілттер арқылы ашуға болады. Құжатты шифрлап жеке кілт арқылы жіберсе, оның шифрын публикалық кілт арқылы ашуға болады, және де керісінше. Жеке кілт тек қана иесіне белгілі оны басқа біреуге беруге болмайды, осы уақытта публикалық кілт барлық корреспонденттерге ашық жария етіледі.

Қос кілттер – жеке және публикалық – оларды аутентификация және құпияны сақтау үішн қолдануға болады.

Екі адамның мәлімет алмасуы үшін екі қос кілттер болуы қажет.

Шифрлау кезінде қос кілттің арқасында сіз публикалық кілтті корреспонденттерге жіберіп отыру қажет емес. Бұл кілтті жүйеге ашық жазып қою сізге ыңғалы болады. Сол кезде барлық адамдар осы кілтті өздеріне жазып алып, сіздерге құпиялы мәліттерді жібере алады.

Симметриялық және асимметриялық кілттер арқылы шифрлау.

Әрбір уақытта ассиметриялық шифрлау симметриялық шифрлаудан эффективалық жағынан жеңіліп қалады,сондықтанда көптеген адамдар шифрлау жүйесінде ассиметиялық және дәстүрлі симметриялық шифрлау жүйесін қолданады. Ашық кілтпен шифрлау симметриялық кілт қолданылады, бұл жіберілген мәліметті ширлау үшін қолданылады.

Цифрлық қолтаңба

Цифрлық қолтаңбаның механизмін түсндіру үшін, бір жақты хэш функияны енгізу қажет. Біржақты хэш функция бұл функция, шығарылған мәліметтің ұзындығын белгілі ұзындыққа айналдрады, оны жіберу дайджесті деп атайды. 16 байттық хэш функцяны шығару кезінде сіз 16 байттық мәлімдеме аламыз.

Хештау – бұл біржақты, т.б, шифрлауға қарағанда қайтарымсыз. Дайджест боынша шығарылған мәлімдемені қайтаруға болмайды, бірақ оған идентификация жасауға болады. Нақты бір мысал қарастырайық.Мысалы А хэш функция арқылы дайджестті қандайда бір код ретінде ады делік (код 1). Одан соң ол А өзінің жеке кілтін пайдаланып, сол документтің аналогының қолтаңбасы болатын дайджестті шифрлайды. Содан соң А ашық текстті және цифрлық қолтаңбалы В жібереді. В абоненті оны публикалық кілт арқылы шифрлап ашады да, бұл хаттың А келеніне сенімді болады. Осылай аутентиикация орындалады. Содан соң бұл хаттың жолда өзгертілмегені жөнінде тексеру қажет. Соңында В шифрлау арқылы дайджестті алады – код 1. Содан кейін А сияқты В –да хэш – функцияны пайдаланып, дайджестті қандайда бір код ретінде алады – код 2. Егер код1 және код 2 бір біріне сай келсе, сонда ғана В бұл тексттің жолда өзгертілмегеніне көзін жетізеді.

Осындай жағдайда, цифрлық қолтаңба және электрондық қолтаңба – бұл әдіс жіберушінің аутентификациясы немесе авторлық қолтаңба, бұл мәліметтің мазмұнының өзгертілмеуіне себеп. Цифрлық қолтаңба шифрлау арқылы қойылуыда мүмкін, сонымен қатар ашық жіберуде орындалуы мүмкін.

Бақылау сұрақтары:

Интернетте мәліметті жіберу кезінде қандай мәліметті қорғау механизмі қолданылады.

2. Жіберуші идентификациясы, жіберу аутентификациясы, құпияны сақтау мәндері қандай?

3. Симметриялық және ассиметриялық шифрлаудың мәні қандай? 4.Цифрлық қолтаңба механизмінің алгоритмі қандай?