Лекция 6 КРИПТОГРАФИЯЛЫҚ ХЕШ-ФУНКЦИЯЛАР

6.1 Хеш-функция ұғымы

Хеш-функция (hash function) - бұл кез келген ұзындығы бар жол үшін кейбір бүтін мәнді немесе кейбір тіркелген ұзындығы бар басқа жолды есептейтің математикалық немесе басқа функция. Математикалық түрде былай жазуға болады:

$$h = H(M),$$

мұндағы M – бастапқы хабар (кейде болашақ үлгісі деп аталады); h – нәтиже, хеш-функция мәні деп аталады (және де хеш-коды немесе хабар дайджесы – ағыл. *message digest*).

Хеш-функцияның мағынасы болашақ үлгінің сиппаты белгісін - хеш-функция мәнің анықтау. Әдетте бұл мәнде тіркелген өлшемі болады, мысалы, 64 немесе 128 бит. Хеш-кодты әрі қарай кейбір есепті шешу үшін талдауға болады. Мысалы, хеширлау деректерді салыстыру үшін қолданылу мүмкін: егер екі деректер массивінде хеш-коды әртүрлі болса, массивтер міндетті түрде әртүрлі; егер бірдей болса – массивтер де бірдей. Жалпы жағдайда бастапқы деректер мен хеш-коды арасында бір мәнді сәйкестік жоқ, өйткені хеш-функция мәндерінің саны кіру деректер варианттарынан әрқашан кем. Сондықтан, бірдей хеш-кодты беретің кіру хабардың бірнеше көптігі бар (осындай жағдайды *коллизия* деп атайды). Коллизияның болу ықтималдығы хеш-функцияның сапасын бағалауда үлкен роль ойнайды.

Хеш-функциялар қазіргі криптографияда жиі қолданылады.

Ең қарапайым хеш-функция «модулі 2 бойынша қосынды» операцияны пайдалануымен құрастырылу мүмкін: кіру жолды аламыз, модулі 2 бойынша барлық байтты қосамыз және байт-нәтижені хеш-функция мәні ретінде қайтарамыз. Хеш-функция мәнің ұзындығы бұл жағдайда, кіру хабардың өлшеміне тәуелсіз, 8 бит болады.

Мысалы, цифрлық түрге айналдырған бастапқы хабар келесі болсын (он алтылық форматта):

3E 54 A0 1F B4

Хабарды екілік түрге ауыстырайық, байттарды бір бірінің астында жазайық және әрбір бағанда биттерді модулі 2 бойынша қосайық:

```
 0011 1110
 0101 0100
 1010 0000
 0001 1111
 1011 0100
----------
 0110 0101
```

Нәтиже ($0110\ 0101_{(2)}$ немесе $65_{(16)}$) хеш-функцияның мәні болып табылады.

Бірақ мұндай хеш-функцияны криптографиялық мақсаты үшін пайдалануға болмайды, мысалы, электронды қолды құрастыру үшін, өйткені бақылау қосындыны өзгертпей қол қойылған хабардың мазмұның өзгерту оңай.

Сондықтан қарастырылған хеш-функция криптографиялық қолдануға келмейді. Криптографияда хеш-функция жақсы деп саналады, егер бірдей хеш-функция мәні бар екі

болашақ үлгіні жасауға қиын болса, және де егер функция шығуының кіруден анық тәуелділігі жоқ болса.

Криптографиялық хеш-функцияларға қойылатын талаптарды тұжырымдайық:

- хеш-функция кез келген өлшемі бар хабарларға қолданылу болу керек;
- функция мәнің есептеуі жеткілікті тез орындалу керек;
- хеш-функция мәні белгілі болғанда, сәйкес болашақ үлгіні M табу қиын (мүмкін емес) болу керек;
- хабар M белгілі болғанда, осындай хеш-функция мәні бар басқа хабарды M' табу қиын болу керек;
- қандай да болса кездейсоқ әртүрлі бірдей хеш-функция мәні бар жұп хабарды табу қиын болу керек.

Айтылған талаптарға қанағаттандырылатын хеш-функцияны жасау оңай емес. Есте сақтау қажет, функция кіруіне кез келген өлшемі бар деректер түседі, ал хеш-нәтижесі олар үшін бірдей болмау керек.

Қазіргі уақытта тәжірибеде хеш-функция ретінде кіру хабарды блок блокпен өңдейтің және кіру хабардың әрбір M_i блогы үшін хеш-мәнің h_i есептейтің функциялар қолданылады

$$h_i = H(M_i, h_{i-1}),$$

мұндағы h_{i-1} – кіру деректердің бұрыңғы блогы үшін хеш-функцияны есептеу нәтижесі.

Нәтижесінде хеш-функцияның шығуы h_n кіру хабардың барлық n блоктарының функциясы болып табылады.

6.2 Хеш-функцияны құрастыру үшін шифрлау блокты алгоритмды пайдалану

Хеш-функция ретінде симметриялық шифрлаудың блокты алгоритмын пайдалануға болады. Егер пайдаланатын блокты алгоритм криптографиялық берікті болса, онда оның негізіндегі хеш-функция да сенімді болады.

Хеш-кодты алу үшін блокты алгоритмды пайдалануының ең қарапайым тәсілі - CBC тәртіпте хабарды шифрлау. Бұл жағдайда хабар, ұзындығы шифрлау алгоритмның блок ұзындығына тең блок тізбегі ретінде беріледі. Қажет болғанда, керекті ұзындығы бар блокты алу үшін соңғы блок оң жағынан нөлмен толтырылады. Хеш-мәні мәтіннің соңғы шифрланған блогы болады. Сенімді блокты шифрлау алгоритмды пайдаланғанда алынған хеш-мәннің келесі қасиеті болады:

- шифрлау кілтті білмей, берілген ашық ақпарат массивы үшін хеш-мәнің есептеу мүмкін емес;
- шифрлау кілтті білмей, берілген хеш-функцияның мәні үшін ашық деректерді іріктеп алу мүмкін емес.

Осылай құрастырылған хеш-мәнің әдетте *еліктеу ендірме* немесе *аутентификатор* деп атайды және хабардың тұтастығын тексеру үшін пайдаланылады. Сонымен, еліктеу ендірме – бұл ашық деректерге және құпиялы кілттік ақпаратқа тәуелді бақылау комбинациясы. Еліктеу ендірменің пайдалану мақсаты ақпарат масивінде барлық кездейсоқ немесе әдейі өзгертулерді табу. Кіру хабарды өңдегенде хеш-функциямен алынған мәні хабарға қосылады, егер хабар дұрыстығы белгілі болса. Алушы хабардың еліктеу ендірмесін есептеп және алынған хеш-кодпен салыстырып хабар тұтастығын тексереді. Хеш-коды қауіпсіздік тәсілмен берілу керек, мысалы, еліктеу ендірмені жіберушінің жабық кілтімен шифрлау, яғни қолды жасау. Алынған хеш-кодты симметриялық шифрлау алгоритмы мен де шифрлауға болады, егер жіберуші мен алушыда симметриялық шифрлаудың ортақ кілті болса.

Көрсетілген еліктеу ендірмені алу және пайдалану процесі ресей стандартында ГОСТ 28147-89 бейнеленген. Стандарт берілетің хабар тұтастығын тексеру үшін, тіркелу тіртібінде барлық хабарды шифрлаудың шығуында алынған блоктың, кіші 32 битын пайдалануын ұсынады. Еліктеу ендірмені құрастыру үшін осы түрімен симметриялық шифрлаудың кез келген блокты шифрын пайдалануға болады.

Хеш-кодты жасау үшін блокты шифрдың басқа пайдалану тәсілі келесі болу мүмкін. Бастапқы хабар блоктар ретімен өңделеді. Соңғы блок қажет болса нөлмен толтырылады, кейде соңғы блокқа екілік сан түрінде хабар ұзындығын қосады. Әрбір кезеңде бұрынғы кезеңде алынған хеш-мәнің шифрлаймыз, кілт ретінде хабардың ағымды блогын аламыз. Соңғы алынған шифрланған мәні ақырғы хеш-нәтижесі болады.

Сонымен, егер M хабардың блокты f шифры көмегімен K кілтте кәдімгі шифрлау схемасын біз былай жазсақ $E=f(M, K)$, онда h хеш-кодты алу схемасын былай көрсетуге болады

$$h_i = f(h_{i-1}, M)$$

Бастапқы h_0 хеш-коды ретінде кейбір константаны алады. Шифрлау қарапайым ауыстыру тәртібінде өтеді. Айтылған тәсілді пайдаланғанда блок өлшемі кілт ұзындығымен сәйкес келеді және хеш-мәнің өлшемі бұл блок ұзындығы.

Блокты шифрдың қарапайым ауыстыру тәртібінде пайдалануының тағы бір тәсілі бар: хабар элементі бұрынғы кезеңде алынған хеш-мәнімен шифрланады:

$$h_i = f(M, h_{i-1})$$

Толық айтқанда, хеш-функцияны құрастыру үшін блокты шифрдың тағы бірнеше пайдалану схемалары болу мүмкін.

M_i – бастапқы хабардың блогы; h_i – i-ші кезеңдегі хеш-функцияның мәні; f – қарапайым ауыстыру тәртібінде пайдаланылатын блокты шифрлау алгоритмы; $\oplus$ модулі 2 бойынша қосу операциясы болсын. Онда мысалы, хеш-функцияны құрастырудың келесі схемалары болу мүмкін:

$$h_i = f(M_i, h_{i-1}) \oplus M_i,$$
$$h_i = f(M_i, h_{i-1}) \oplus h_{i-1} \oplus M_i,$$
$$h_i = f(h_{i-1}, M_i) \oplus h_i,$$
$$h_i = f(h_{i-1} \oplus M_i, M_i) \oplus h_i$$

Осы барлық схемаларда хеш-мәннің ұзындығы шифрлаудағы блок ұзындығына тең. Бұл схемалар тәжірибеде қолданылу мүмкін.

Блокты алгоритм негізінде жобаланған хеш-функцияның негізгі кемшілігі салыстырмалы кішкентай жұмыс жылдамдығы. Хеширлаудың жылдамдырақ алгоритмдары бар, олар криптоберіктік талаптарға сай жобаланған (олардың ең кең таралғаны - MD5, SHA-1, SHA-2 және ГОСТ Р 34.11-94).

6.3 Хеш-функцияны құрастыру алгоритмдарды шолу

Қазір хеш-функцияны есептеу үшін ұсынылған және тәжірибелік пайдаланады түрлі арнайы алгоритмдар. Ең танымал алгоритмдар MD5, SHA-1, SHA-2 және SHA-ң басқа версиялары, және де ресей алгоритмы ГОСТ Р 34.11-94.

MD5 алгоритмы XX ғасырдың 90-ші жылдары шықты. «MD» символдары көрсетеді *Message Digest* – хабардың қысқаша мазмұндамасы. Алгоритм авторы – Р.Ривест (R.Rivest). MD5 пайдалану нәтижесінде кез келген хабар үшін 128-битты хеш-мәні құрастырылады. Кіру деректер 512 битты блоктармен өңделеді. Алгоритмда элементар логикалық операциялар пайдаланады (инверсия, конъюнкция, модулі 2 бойынша қосу, циклдық ығысу және т.б.), және де кәдімгі арифметикалық қосу. Осы элементар функциялардың комплекстік қайталауы нәтиженің жақсы араластыруын қамтамасыз етеді. Сондықтан кездейсоқ таңдап алынған хабарларда бірдей хеш-коды болмайды. MD5 алгоритмның келесі қасиеті бар: алынған хеш-мәннің әрбір биты кіру әрбір биттын функциясы болып табылады. 128-битты хеш-мәні үшін MD5 ең күшті хеш-функция деп саналады.

SHA (*Secure Hash Algorithm* – қауіпсіз хеш-алгоритм) алгоритмы АҚШ-ң ұлттық стандарттар және технологиялар институтында (NIST) жасалынған және американ

федерал ақпараттық стандарт ретінде 1993 жылы жарияланған болатын. SHA-1 алгоритмда бастапқы хабардың 512 битты блоктармен өңдеу нәтижесінде 160-битты хеш-мәні құрастырылады. MD5 алгоритмдағыдай SHA-1 алгоритмда да қарапайым логикалық және арифметикалық операциялар пайдаланады. MD5-тен SHA-1-ң ең маңызды айырмашылығы мынадай: SHA-1-ң хеш-коды MD5-ң хеш-кодынан 32 битке ұзын. Екуінің де күрделігі бірдей болғанда SHA-1-ң беріктігі жоғары.

2001 жылы АҚШ-ң ұлттық стандарттар және технологиялар институты стандарт ретінде, хеш-коды SHA-1-ден ұзыңырақ үш хеш-функцияны қабылдады. Осы хеш-функцияларды жиі SHA-2 немесе SHA-256, SHA-384 және SHA-512 деп атайды (яғни атында хеш-код ұзындығы берілген). Бұл алгоритмдарда өңделетін блок ұзындығы да үлкен (SHA-256-да блок ұзындығы – 512 бит, SHA-384 және SHA-512-де блок ұзындығы – 1024 бит).

Ресейде хеш-функция үшін стандарты ГОСТ Р34.11-94. Оның құрылымы SHA-1,2 немесе MD5-тен қатты ерекшеленеді. ГОСТ Р34.11-94 жасайтын хеш-код ұзындығы 256 бит. Алгоритм бастапқы хабарады 256 битты блоктармен оң жақтан солға қарай рет-ретімен өңдейді. Алгоритм параметрі бастапқы хаширлау векторы – ұзындығы 256 бит кез келген тіркелген мәні. ГОСТ Р34.11-94 алгоритмда ауыстыру операциялар, ығысу, арифметикалық қосу, модулі 2 бойынша қосу пайдаланады. Көмекші функция ретінде қарапайым ауыстыру тіртібінде ГОСТ 28147-89 алгоритмы пайдаланады.

Негізгі ұғымдар

Hash function – хеш-функция.

ГОСТ Р34.11-94 – хеширлау функцияға ресей стандарты.

Хеш-функция – кез келген ұзындығы бар жол үшін кейбір бүтін мәнді немесе кейбір тіркелген ұзындығы бар басқа жолды есептейтің математикалық немесе басқа функция.

Хеш-коды – хеш-функцияның жұмыс нәтижесі, кіру деректер массивының кейбір сипатты «белгісі».

Сұрақтар

1. Криптографияда нені хеш-функция деп атайды?
2. Хеш-функциялар қандай мақсаты үшін пайдаланады?
3. Хеш-функцияларға қойылатын негізгі талаптарды айтып беріңіз.
4. Криптографиялық хеш-функцияның мысалдарын айтып беріңіз.
5. Криптографиялық хеш-функцияны құрастыру алгоритмға қандай ресей стандарты бар?
6. Хеш-функцияны құрастыру үшін блокты шифрлау алгоритмды қалай пайдалануға болады?