Лекция 13 ҚҰПИЯЛЫ ЖҮЙЕЛЕР

Криптографияда пайдаланатын ақпарат теориясының негізгі қағидаларын К.Шеннон XX ғасырдын ортасында тұжырымдады. Ол көрсеткен болатын - әбден құпиялы криптографиялық жүйелердің бар болуы теориялық түрде мүмкін, оларды «бұзу» мүмкін емес. Бұл бөлімде біз Шеннон теориясының негізгі идеясымен таңысамыз және хабардың энтропиясы мен белгісіздігін қалай есептеуге болатының, тіл нормасын, хабардың артықтығын және шифр жалғыздығының қашықтығын білеміз.

Криптографияда пайдаланатын ақпарат теориясының негізгі қағидалары XX ғасырдын ортасында тұжырымдалынды. Осы зерттеулерге үлкен үлес қосты америка ғалымы К. Шеннон. Коммуникациялық арналар арқылы ақпаратты беру принциптерді зерттеу үшін К. Шеннон берілетің ақпараттың саның бағалауға ықтималдық жол ұсынды. Одан басқа, ол **әбден құпиялы криптографиялық жүйелер** («бұзу» мүмкін емес) мүмкін болатының көрсетті. Шеннон теориясының негізгі идеяларын қарастырайық.

13.1 Ақпаратты өлшеуге негізгі жолдар

Ақпаратты алу, өңдеу, беру және қорғау сұрақтары оның сандық өлшеу проблемасымен тығыз байланысты. Осындай проблеманы шешудің бірнеше түрлі жолдарын ажыратады. Олардың біреуі *статистикалық* (немесе *алфавитті*) жолы. Оның мағынасы мынадай – берілетің ақпарат көлемінің сандық бағалауы ақпарат көзінің статистикалық сипаттамаларының талдауына негізделген. Бұл тәсілде қандай да болса тіл көмегімен ақпаратты ұсыну тәсілі еске алынады.

Кейбір хабардың ақпараттық құндылығы генерацияланған хабарлар варианттарының әр түрлілігіне байланыстығы анық. Сондықтан айтуға болады, жеке хабармен берілетің ақпарат көлемі, түрлі хабарлардың жалпы N санына (немесе ақпарат көзінің күйлерінің санына) пропорционал. Тәжірибеде, бірақ, ақпараттық көлемінің өлшемі ретінде N санның өзі емес, негізі 2 бойынша оның логарифмы алынады:

$$I = \log_2 N.$$

Осы формула нәтижені битпен алуға мүмкіндік береді. Осындай өлшем ақпараттың *формальді-логикалық логарифмдік өлшемі* деп аталады, немесе Хартли бойынша ақпарат өлшемі.

Бір әріптік хабарлар үшін N ақпараттық құрылғының алфавитіндегі әріптер санына тең. Мысалы, әріптер саны екіге тең болғанда ақпарат көлемі тең

$$I = \log_2 2 = 1 \text{ бит.}$$

Орыс тілінің бір әріптерінен тұратын хабарларды генерациялайтын көзді қарастырайық (алфавитте 33 әріп). Бір әріптен тұратын жеке хабар қанша ақпарат әкелетінің анықтайық:

$$I_1 = \log_2 33 \approx 5 \text{ бит.}$$

Кейбір хабарда ақпарат көлемін анықтау үшін оның символдар санын бір символдағы ақпарат санына көбейту керек, яғни оның ақпараттық салмағына. Орыс алфавиттің төрт әріптерінен тұратын хабар қанша ақпарат әкелетінің есептейік:

$$I_4 = 4 \log_2 33 \approx 20 \text{ бит.}$$

Сонымен, алфавитті тұрғыда хабардағы ақпарат көлемі хабардың мағыныса бойынша емес, статистикалық сипаттамалары (символдар саны) бойынша бағаланады. Хартли өлшемі хабардың дұрыс сипаттамасы болып әрқашан болмайды, өйткені кез келген мүмкін хабардың тең ықтималдығын жобалайды. Ықтималдығы кіші хабарлардың құндылығы жоғары. Сондықтан, кейде ақпараттың сандық бағалауының басқа тәсілін пайдаланады. Ол нақты хабарларды генерациялау ықтималдығын еске алады, - Шеннон бойынша ақпарат өлшемі. Бұл ақпаратты өлшеу әдісті *мазмұнды жол* деп атайды.

Осы әдіске сәйкес хабарды тұтынушы алғанша ақпарат көзінің күйі кейбір белгісіздікпен сипатталады. Бұл кезде ақпаратты алу осы белгісіздікті жояды (толық немесе жарым-жартылай):

$$I = H_{\text{баст}} - H_{\text{соңғ}}$$

мұндағы $H_{\text{баст}}$ – хабарды алуға дейін хабар көзін сипаттайтын белгісіздік, $H_{\text{соңғ}}$ – хабарды алғанан кейін белгісіздік.

Ақпарат көзі күйінің белгісіздігі мына формула бойынша бағаланады:

$$H = -\sum_{i=0}^{N-1} p_i \cdot \log_2 p_i \ ,$$

мұндағы p_i – көздің i-ші күйінің ықтималдығы. Қосындының алдында «минус» таңбасы енгізілген, себебі ықтималдық шамалары дұрыс бөлшектер және теріс логарифмдер, ал белгісіздік бағалауын «плюс» таңбамен алу керек.

Мысал қарастырайық. Бір қара және бір ақ шары бар урнадан шарларды алғанда, белгісіздік болады

$$H = -\frac{1}{2}\log_2 \frac{1}{2} - \frac{1}{2}\log_2 \frac{1}{2} = -\log_2 \frac{1}{2} = -(-1) = 1 \ .$$

Белгісіздік бір битке тең болып шықты.

Басқа мысалды қарастырайық. Урнада жеті қара және бір ақ шар бар. Осы кезде белгісіздік болады

$$H = -\frac{7}{8}\log_2 \frac{7}{8} - \frac{1}{8}\log_2 \frac{1}{8} = \frac{7}{8}(\log_2 8 - \log_2 7) + \frac{1}{8}(\log_2 8) =$$

$$= \frac{7(3 - \log_2 7) + 3}{8} \approx \frac{7(3 - 2{,}8) + 3}{8} \approx 0{,}55 \ \textit{бит}$$

Белгісіздік өлшемі бірінші мысалмен салыстырғанда екі есе азайды.

Әрбір күйлердің ықтималдығы бір біріне тең болғанда белгісіздік максимал мәнін алады және осы ықтималдықтың тарқауының өсуімен азаяды. Айта кетейік, ықтималдықтар бір біріне тең болғанда $p_i = p_j, \ \forall i, j = \overline{0, N-1}$, Шеннон бойынша ақпарат өлшемі Хартли бойынша ақпарат өлшеміне тура келеді.

Көп жағдайда ақпаратты өлшеуге алфавитты жол артық көрінеді. Кейбір файлда 1,5 мегабайт ақпарат бар немесе кейбір кітаптін бір парағына 17 килобайт ақпарат кіреді деп айтқанда, дәл Хартли бойынша ақпарат өлшемі пайдаланады.

Ақпарат санның негізгі бірлігі бит. Бірақ тәжірибелік қолданылу үшін бұл тым ұсақ бірлік. Одан ыңғайлы бірлік байт (byte) болып табылады, ол сегіз битке тең. «Байт» сөзге децимал қосымшаларды «кило», «мега» және т.б. қосып одан ірі өлшем бірліктерді алуға болады. Бұл кезде есте болу керек, оларды байланыстыратын көбейткіш 1000 емес, ал $1024 = 2^{10}$.

13.2 Энтропия және белгісіздік

Сонымен, біз анықтадық, хабардағы ақпарат көлемінің өлшеуін белгісіздіктің өзгеру негізінде жүргізуге болады. К.Шеннон белгісіздік өлшемі ретінде **энтропия** ұғымын енгізді. Энтропия $H(m)$ хабардағы m ақпарат санын анықтайды және оның белгісіздік өлшемі болып табылады.

Хабарлар көзі ықтималдығы $p_1, p_2, ..., p_n$ бар түрлі хабарды $m_1, m_2, ..., m_n$ жасай алады. Бұл жағдайда хабардың энтропиясы мына формуламен анықталады

$$H(m) = -\sum_{i=0}^{N-1} p_i \cdot \log_2 p_i \ .$$

Осы формулада екілік логарифм пайдаландықтан, энтропия бит пен өлшенеді.

Энтропияның «физикалық» мағынасы - бұл белгісіздіктің сандық өлшемі. Мысал

ретінде үш хабарлар көздерін қарастырайық, олардың әрбіреуі тек екі әртүрлі m_1 және m_2 хабар генерациялайды. Бірінші көзі үшін бірінші хабардың пайда болу ықтималдығы $p(m_1)=0$ белгілі болсын, ал екінші хабардың ықтималдығы $p(m_2)=1$. Екінші көзі үшін хабарлар ықтималдықтары тең, яғни $p(m_1)=0,5$ және $p(m_2)=0,5$. Үшінші көзі үшін хабарлар ықтималдықтары келесі: $p(m_1)=0,9$ және $p(m_2)=0,1$. Хабарлар көздерінің энтропиясын анықтайық. Бірінші көзі үшін:

$$H_1 = -0 \log_2 0 - 1 \log_2 1 = 0 - 0 = 0.$$

Бірінші көзінің энтропиясы немесе белгісіздігі нөлге тең. Шынында, егер екі хабардан тек біреу ғана генерациялатыны алдын ала белгілі болса, онда ешқандай белгісіздік жоқ.

Екінші көздің энтропиясын анықтайық:

$$H_2 = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = -\log_2\frac{1}{2} = -(-1) = 1 .$$

Белгісіздік бір битке тең болып шықты. Енді үшінші көздің энтропиясын табайық:

$$H_3 = -0,9 \cdot \log_2 0,9 - 0,1 \cdot \log_2 0,1 \approx -0,9 \cdot (-0,152) - 0,1 \cdot (-3,322) \approx 0,47.$$

Үшінші көздің белгісіздігі екіншіден кіші, өйткені екі мүмкін болатын хабардан, біреуінің ықтималдығы жоғары.

Энтропия ұғымы ақпаратты беру және сақтау теориясының көп есептерінде маңызды роль атқарады. Мысалы, энтропия деректердің максимал сығу дәрежесін анықтау үшін пайдалану мүмкін. Дәл айтқанда, егер хабарлар көзі белгілі шекті энтропиясы h бар жеткілікті ұзын мәтінді n тудыратын болса, онда бұл мәтін теорияда $n \cdot h$ бит шамасына дейін сығылу мүмкін. Егер $h = 1/2$, онда мәтін екі есе сығылу мүмкін және т.б. $n\,h$ мәні шек болып табылады және тәжірибеде сирек болады.

Криптография жағынан, хабар мазмұның білу үшін энтропия ашуға қажетті символдар санын анықтайды. Егер кейбір 8-битты деректер блогы екі мүмкін болатын хабардын (мысалы, жауаптар «Иә» немесе «Жоқ») біреуін сақтайтын болса, онда бастапқы хабардың мәнің анықтау үшін бір битты дұрыс білу жеткілікті. «Иә» және «Жоқ» сөздерді шифрлау үшін қаншалық бит бөлінседе, энтропия немесе белгісіздік әрқашан бірден кем немесе бірге тең болады.

13.3 Тіл нормасы және хабардың артықтығы

Әрбір тіл үшін **тіл нормасы** r деп аталатын шаманы енгізуге болады, ол мына формула бойынша анықталады

$$r = H(m)/N,$$

мұндағы $H(m)$ – хабар энтропиясы, N – пайдаланатын тілдің символдарымен алынған хабар ұзындығы. Тіл нормасын хабардың бір символына келетін ақпарат саны ретінде қарастыруға болады. Тіл нормасы түрлі тілдер үшін және түрлі ұзындығы мен мазмұны бар хабарлар үшін әртүрлі болады. Мысалы, зерттеушілер ағылшын тілінің нормасын бір символы үшін 1,0 ден 1,5 битке дейін диапазон аралығында бағалайды. Ал орыс тілінің нормасы бір символға шамалы 1,5 бит деп саналады.

Тілдің абсолют нормасы R - символдар тізбегі тең ықтималды болғанда, тілдің бір символымен берілетін ақпараттың максимал бит саны. Алфавиты L символдан тұратын тілдің абсолют нормасы былай есептеледі

$$R = \log_2 L$$

Алфавиты 33 әріптен тұратын орыс тілі үшін тілдің абсолют нормасы

$$R_{\text{орыс}} = \log_2 33 \approx 5 \text{ бит}.$$

Сонымен, көрініп тұр, орыс тілінің абсолют нормасы нақтыдан бірталай үлкен. Мұның ешқандай таң қаларлығы жоқ, себебі барлық табиғи тілде едәуір артықтығы бар

болады. Бұл бірнеше фактілерге байланысты. Біріншіден, хабарларда алфавиттің кейбір әріптері басқалардан жиі кездеседі. Артықтықтың екінші себебі – сөздегі кейбір әріптер тіркестері жарамайды. Мысалы, орыс тілінде қатар тұратын әріптері «ц» және «й» немесе «я» және «ь» бар сөздер болмайды. Одан басқа, табиғи тілдерде сөз немесе фраза фрагментін біле отырып, жетпейтін бөлігін табуға болады. Мысалы, сәлемде

Зд.авствуй, до.огой д.уг!

жетпейтін әріпті «р» табу оңай.

Тіл артықтығын D былай бағалайды

$$D = R - r.$$

Орыс тілінің артықтығы символға 3,5 битке тең болып шығады. Демек, орыс тілінің әрбір әрпінде пайдаланбайтын ақпараттың 3,5 биты бар болады. Осыған жақын артықтық басқа табиғи тілдерде де болады, мысалы ағылшын тілде.

Хабарлардың минимал артықтығы $D = 0$ болады, егер тілдің барлық символдары тең ықтималды және хабарда бір біріне тәуелсіз кез келген ретімен кездесетін болса.

13.4 Әбден құпиялы жүйе ұғымы

Криптографиялық жүйе **әбден құпиялы** деп аталады, егер шифрланған мәтіннің талдауы ашық мәтін туралы (ұзындығынан басқа) ешқандай ақпарат бермесе.

Егер криптографиялық жүйе әбден құпиялы болмаса, онда хабардың шифрмәтінің білу сәйкес ашық мәтін туралы кейбір ақпарат береді. Қарапайым шифрлау жүйелер үшін, мысалы, бір рет ауыстыру немесе орын ауыстыру әдістер, ұстап алынған шифрланған хабар ұзындығының өсуімен шифрлау кілт немесе ашық мәтін туралы кейбір қорытынды шығаруға болады. Бұл табиғи тілдердің үлкен артықтығына байланысты. Мысалы, орын ауыстыру әдісімен шифрланған хабар ұстап алынса, онда қарсылас бастапқы хабарда қандай символдар және неше рет кездесетінің білу мүмкін. Сосын ол орын ауыстыру ережесін анықтау үшін қандай да болса күрделі талдау жүргізе алады. Егер бізге моноалфавитты ауыстыру әдісімен шифрланған хабар ДКДК белгілі болса, біз қосымша ақпаратсыз бастапқы мәтінді бірмәнді анықтай алмаймыз. Бірақ, ДКДК-ны қолға түсіріп, мұндай қорытынды шығаруға болады:

1. бастапқы хабарда алфавиттің екі әрпі ғана пайдаланған;
2. ашық мәтіннің бірінші және үшінші, және де екінші мен төртінші әріптері бірдей

болған.

Сонымен қатар болжауға болады: не Д, не К дауысты әріпті ауыстырады. Мүмкін бастапқы хабар МАМА сөзі, немесе ПАПА болу мүмкін, не тағы басқа. Оны бірмәнді дешифрлауға мүмкін емес, бірақ, шифрмәтін туралы кейбір ақпаратты біз анықтай алдық. Сонымен, ауыстыру немесе орын ауыстыру әдістер әбден құпиялы криптографиялық шифрлар болып табылмайды.

Тәжірибеде әбден құпиялы жүйенің келесі жүзеге асыруы мүмкін, ол **бір реттік таспа** (немесе **бір реттік блокнот**, немесе **Вернам шифры**) деп аталады. Шифрлау процесіне екілік деректер тап болады деп болжайық. Беретің және қабылдайтың жақта екі бірдей таспа дайындалады, мысалы, магнитті. Оларда шифрлау кілті бар. Беретің жақта таспа шифрлау құрылғыға қойылады, ал қабылдайтың жақта – дешифрлау үшін пайдаланатын ұқсас құрылғыға. Жіберуші хабарды беретін болса, ол бастапқы хабардың бір битын және магнитті таспадан бір битты модулі екі бойынша қосады. Осыдан кейін таспа келесі күйге ауыстырылады және кілттің екінші битын пайдаланып хабардың екінші битын шифрлауға болады. Осылай барлық хабар шифрланады. Қабылдайтың жақта кілті бар таспа ұқсас пайдаланылады.

Мысалы, бастапқы m хабарда келесі екілік цифрлар болсын:

m = 1100101110...

Кілттік ретінде пайдаланатын тізбек мұндай болсын деп болжам жасайық:

```
                    k = 1001100111...
```

Шифрлауды бір реттік таспа әдісі бойынша орындайық, әрбір бағанда цифрларды модулі екі бойынша қосып:

```
бастапқы мәтін              m = 1100101110...
кілттік тізбектің биты      k = 1001100111...
------------------
шифрланған мәтін            c = 0101001001...
```

Бұл процесс кіру деректер ағынына гаммана салуға ұқсайды. Бір реттік таспасы бар шифр шынында гаммалау болып табылады, бірақ, оның басқа криптожүйелерден айырмашылығы – шексіз гамма.

Бір реттік таспада барлық әріптер бірдей жиілікпен кездеседі. Сондықтан, гамманың қанша болса да таңбасы белгілі болса, біз келесі әріп қандай болатының алдын ала болжай алмаймыз. Осыдан шығады, гамма таңбаларының барлық тізбектері тең ықтималды. Демек, Вернам шифры көмегімен шифрланған хабар, кез келген сәйкес ұзындығы бар ашық мәтінге «дешифрлану» мүмкін, себебі шамаланған гамма таңбаларының тізбегінде оны басқадан айыратын ешқандай қасиеті жоқ.

Вернам шифрында кілттік деректер тасушы ретінде дәл таспаны пайдалану мүлде міндетті емес. Ең керекті, жіберуші мен алушыда өлшемі бастапқы хабардың ұзындығынан кем емес құпиялы кілт болу қажет.

Әбден құпиялы жүйелер тәжірибеде жүзеге асырылу мүмкін. Бірақ, неліктен олар барлық жағдайда пайдаланбайды? Мұнын бірнеше себебі бар. Біріншіден, жабық кілті бар шифрлау жүйедегіндей оларда кілттерді үлестіру проблемасы бар. Екіншіден, әбден құпиялы жүйеде шифрлау кілттің ұзындығы аз болғанда ашық мәтіннің ұзындығымен бірдей болу керек. Одан басқа, әрбір хабарды шифрлау үшін өз жаңа кілт қолданылу керек. Осы факторлар әбден құпиялы жүйенің жүзеге асыруын тым қымбатқа және аса қолайлы емеске әкеледі. Осындай жүйелерді тек ең маңызды байланыс (мысалы, үкімет) желілер үшін пайдалану жөн.

13.5 Жалғыздық қашықтығы

Егер криптографиялық жүйе әбден құпиялы болмаса, онда шифрланған хабар криптоталдаушыға бастапқы хабар туралы кейбір ақпарат беру мүмкін. Маман шифрмәтінді тура бір мәнді дешифрламасада, бірақ кілт немесе ашық мәтін жөнінде кейбір болжау жасай алады. Келесі дәл сол кілтпен шифрланған хабарды алғаннан кейін, криптоталдаушы өз білімін кеңейтіп, ақырында хабарды дешифрлай алу мүмкін.

Шифрланған хабарды бірмәнді дешифрлау үшін, оның ұзындығы қандай болу керек. Бұрын қарастырылған мысалда қарапайым ауыстыру әдіспен жабылған 11 символдан тұратын хабарды біз ашып оқуға әрекет жасадық. Орыс тілдің статистикалық
заңдылықтарын талдау негізінде ашық мәтіннің бірнеше қолайлы варианты таңдап алынды, бірақ олардан бір «дұрысын» таңдау үшін ақпарат жетпеді. Сірә, ұстап алынған хабардың кейбір ұзындығы болады, одан кейін хабардың ашып оқу ықтималдығы бірге жақындайды.

Шеннон шифрдың **жалғыздық қашықтығы** (немесе **бірегей қашықтығы**) U деген ұғым енгізді, ол кілтті бір мәнді қалпына келтіру үшін шифрланған хабардың қанша әріптерін ұстап алу қажеттігін көрсетеді.

Жалғыздық қашықтығын есептеу үшін кілт энтропиясын $H(K)$ білу керек. Симметриялық шифрлар үшін кілт энтропиясы шамамен кілттер санының N_K негізі 2 бойынша логарифмына тең:

$$H(K) = \log_2 N_K.$$

Мысалы, қарапайым ауыстыру шифры үшін мүмкін болатын кілттер саны барлық мүмкін ауыстыру кестелер санымен анықталады және тең $N_K = 33! \approx 8{,}68 \cdot 10^{36}$, сондықтан кілт энтропиясы тең болады

$$H(K) = \log_2 8{,}68 \cdot 10^{36} \approx 122{,}7$$

Егер бізге кейбір шифры үшін кілт энтропиясы $H(K)$ белгілі болса, онда ол үшін жалғыздық қашықтығы U мына формула бойынша есептеледі

$$U = H(K) / D,$$

мұндағы D – шифрланатын хабардың артықтығы.

Орыс тілінде хабарларға қолданылатын қарапайым ауыстыру шифры үшін жалғыздық қашықтығын есептейік:

$$U = H(K) / D = 122{,}7/3{,}5 \approx 35{,}1$$

Яғни егер ұстап алынған хабардың ұзындығы 35 символдан артық болса, онда оны бір мәнді ашып оқу мүмкін. Ал шифрланған мәтіннің ұзындығы 35 символдан кем болғанда бір мәнді ашу мүмкін емес.

Қарсыласқа кілтті анықтауды және дешифрлауды қиналту үшін, қолданылатын шифрларда жалғыздық қашықтықты көбейту қажет (шексіздікке дейін жақсы болар еді). Жалғыздық қашықтықты есептеу формуласын талдап, анықтаймыз, мұны екі тәсілмен істеуге болады.

Егер кілт энтропиясы шексіздікке тең болса, онда шифрдың жалғыздық қашықтығы да шексіздікке тең болады. Кілт ұзындығы неғұрлым ұзын болса, кілт энтропиясы соғұрлым үлкен болады. Бір реттік таспа жүйесін пайдаланғанда кілт теорияда шексіз және оның бәр символдары тең ықтималды болады, сондықтан осындай шифрдың кілт энтропиясы шексіз үлкен болады. Демек, Вернам шифрдың жалғыздық қашықтығы шексіздікке тең.

Жоғары айтылғандай, шексіз үлкен кілті бар шифрды пайдалану тәжірибелік орынды емес. Бірақ шифрлау кілттерді анда-санда ауыстыруға болады, мысалы, сеанстық кілттерді пайдаланып, яғни әрбір хабарды шифрлау үшін жаңа кілтті қолдану.

Жалғыздық қашықтықты үлкейтудің екінші тәсілі – бастапқы мәтіннің артықтығын азайту. Егер хабар артықтығы нөлге тең, онда кілт ешқашан анықталмайды, ал шифрланған хабар ашылмайды, себебі жалғыздық қашықтығы шексіздікке тең болады. Өкінішке орай, тәжірибеде бұл мүмкін емес, өйткені кез келген мағыналы хабарда кейбір нөлден өзгеше артықтығы болады.

Бірақ хабардағы артықтықты деректерді сығу арқылы азайтуға болады. Себебі деректерді сығу кезінде «сығылған» мәтіннің энтропиясы сақталындаы, ал ұзындығы азаяды. Демек, энтропия сығылған мәтінде бастапқыдан бір әріпке артық, ал артықтығы – кем. Ендеше, сығу кодтаудан кейін шифрдың жалғыздық қашықтығы өседі.

Негізгі терминдер

Тілдің абсолют нормасы – тілдегі барлық символдар тізбегі тең ықтималды болғанда, кейбір тілдің бір символымен беріле алатын ақпараттың максимал бит саны.

Тіл артықтығы – белгілі тілдегі мәтінде болатын ақпарат артықтығын белгілейтің статистикалық шама.

Тіл нормасы – хабардың бір символына келетін ақпарат саның сипаттайтын шама. **Бір реттік таспа** (немесе **бір реттік блокнот**, немесе **Вернам шифры**) – әбден құпиялы жүйені жүзеге асыруының мүмкін болатын варианты. Шексіз гаммалау сияқты жүзеге асырылу мүмкін.

Жалғыздық қашықтығы (немесе **бірегей қашықтығы**) – кілтті бір мәнді қалпына келтіру үшін шифрланған хабардың қанша әріптерін ұстап алу қажеттігін көрсететін шама.

Әбден құпиялы жүйе - шифрланған мәтіннің талдауы ашық мәтін туралы (ұзындығынан басқа) ешқандай ақпарат бермейтін криптографиялық жүйе.

Хабар энтропиясы – Шеннон енгізген шама. Статистикалық тәуелсіз хабарларды тудыратын көзінің бір элементар хабарға келетін ақпарат санын анықтайды. Ақпараттың белгісіздік немесе болжанбайтындық өлшемі болып табылады.

Сұрақтар

1. Хабар көзінің энтропиясы қалай анықталады?
2. Хабар көзінің энтропиясы нені сипаттайды?
3. Тіл нормасы нені анықтайды?
4. Тілдің абсолют нормасы қалай есептеледі?
5. Тіл артықтығы нені сипаттайды?
6. Неге табиғи тілде жазылған хабарларда әрқашан артықтық болады?
7. Әбден құпиялы криптографиялық жүйенің анықтамасын беріңіз.
8. Әбден құпиялы жүйелер болмайтын шифрлар мысалын келтіріңіз.
9. Неге бір реттік таспа шифры (Вернам шифры) әбден құпиялы жүйе болып табылады?
10. Неге әбден құпиялы жүйелер тәжірибеде ақпаратты қорғау үшін жаппай пайдаланбайды?
11. Шифр кілтінің энтропиясы қалай анықталады?
12. Шифр үшін жалғыздығының қашықтығы қалай есептеледі?