Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Ақпаратты шифрлеу алгоритмдері: симметриялық және асимметриялық



Ақпаратты қорғаудың маңызы

Қолжетімділік

Ақпарат рұқсат етілген пайдаланушыларға қажет кезде қолжетімді болуы керек. Жүйе үздіксіз жұмыс істеуі және деректерге тез қол жеткізуді қамтамасыз етуі тиіс.

Бүтіндік

Деректер өзгеріссіз, толық және дұрыс күйінде сақталуы қажет. Рұқсатсыз өзгерістер мен бұрмалаулардан қорғалуы керек.

Конфиденциалдық

Ақпарат тек рұқсат етілген тұлғаларға ғана қолжетімді болуы керек. Құпиялылықты сақтау негізгі қағида болып табылады.

Соңғы жылдары киберқылмыстар мен ақпараттық шабуылдардың саны қарқынды өсуде. Деректерді ұрлау, шпиондық қызмет және жүйелерді бұзу әрекеттері күн санап көбейіп келеді. Осыған байланысты ақпаратты шифрлеу қазіргі заманғы қауіпсіздіктің маңызды құрамдас бөлігіне айналды.



?Ақпаратты шифрлеу дегеніміз не

Шифрлеу – бұл түсінікті ақпаратты түсініксіз форматқа түрлендіру процесі. Бұл криптографиялық әдістер арқылы жүзеге асырылады және деректердің .қауіпсіздігін қамтамасыз етеді

Шифрлау операциясы ашық мәтінді (plaintext) шифрмәтінге (ciphertext) айналдырады. Бұл процесс арнайы алгоритм және құпия кілт арқылы іске асырылады.

Дешифрлау операциясы керісінше процесс – шифрмәтінді қайтадан ашық мәтінге түрлендіреді. Тек дұрыс кілті бар адам ғана бұл операцияны орындай алады.

Шифрлеу технологиясы рұқсатсыз қол жеткізу, деректерді ұрлау және ақпаратты бұрмалаудан қорғайды. Бұл қазіргі цифрлық әлемде өте маңызды қауіпсіздік қабаты болып табылады.



Ақпаратты шифрлеу алгоритмдерінің екі негізгі түрі

Криптографияда шифрлеу алгоритмдері кілттерді қолдану тәсіліне қарай екі үлкен санатқа бөлінеді. Әр түрдің өзіндік ерекшеліктері, артықшылықтары және қолданылу аясы бар.

Симметриялық шифрлеу

Шифрлау мен дешифрлауда бірдей құпия кілтті қолданады. Классикалық және кең таралған әдіс.

- Бір кілт екі операция үшін
- Жылдам және тиімді
- Кілтті қауіпсіз тарату қажет

Асимметриялық шифрлеу

Ашық және жабық кілттер жұбын пайдаланады. Қазіргі криптографияның негізі.

- Екі түрлі кілт: ашық және жабық
- Қауіпсіз кілт алмасу
- Күрделі математикалық негіз

Екі әдіс те қазіргі ақпараттық қауіпсіздікте маңызды рөл атқарады және көбінесе бірге қолданылады.

Симметриялық шифрлеу: негізгі түсінік



Бір кілт принципі

Симметриялық шифрлеудің негізгі ерекшелігі – ақпаратты шифрлауда және дешифрлауда бірдей құпия кілтті қолдану. Жіберуші мен алушы бірдей кілтке ие болуы керек.

Артықшылықтары

- Өте жоғары жылдамдық
- Аз есептеу ресурстары қажет
- Үлкен көлемдегі деректерге тиімді

Негізгі мәселе

Кілтті қауіпсіз жолмен тарату – симметриялық шифрлеудің басты қиындығы. Егер кілт қауіпсіз емес арна арқылы жіберілсе, оны ұстап алу мүмкіндігі бар.

Тарихи мысал: Цезарь шифры

Цезарь шифры – ең ежелгі және қарапайым шифрлеу әдістерінің бірі. Біздің заманымыздан бұрынғы I ғасырда Рим императоры Юлий Цезарь өзінің әскери хабарламаларын шифрлау үшін қолданған.

Алфавит таңдау

Латын немесе басқа алфавиттің барлық әріптері қолданылады

Жылжыту мәні

Цезарь 3 позицияға жылжытуды қолданған (A→D, B→E және т.б.)

Шифрлеу процесі

Әр әріпті белгіленген санға алға жылжыту арқылы өзгерту

Дешифрлау

Кері бағытта жылжыту арқылы түпнұсқа мәтінді алу

Мысалы, "HELLO" сөзі 3 позицияға жылжытылса "KHOOR" болады. Бұл шифр өте қарапайым болғанымен, криптография тарихында маңызды орын алады және шифрлеудің негізгі принциптерін көрсетеді.



DES (Data Encryption Standard)

Тарихи маңызы

1977 жылы АҚШ-тың Ұлттық стандарттар бюросы (NBS) ресми шифрлеу стандарты ретінде қабылдаған алғашқы криптографиялық алгоритм.

Техникалық сипаттамалар

- 56 биттік симметриялық кілт
- 64 биттік блоктармен жұмыс
- 16 раундтық шифрлеу процесі
- Feistel желісі құрылымы



Қазіргі жағдайы

Компьютерлік қуаттың артуына байланысты DES қазір әлсіз деп саналады. 1998 жылы арнайы жабдық арқылы бір тәулікте бұзылды.

Triple DES (3DES) DES-ті үш рет қолдану арқылы қауіпсіздікті арттыру әрекеті болды, бірақ ол да баяу болып шықты.



AES (Advanced Encryption Standard)

AES – қазіргі заманғы ақпараттық қауіпсіздіктің алтын стандарты. 2001 жылы АҚШ үкіметі DES-ті алмастыру үшін ресми түрде қабылдаған.

1

Rijndael алгоритмі

Бельгиялық криптографтар Жоан Дамен мен Винсент Риймен әзірлеген. Халықаралық конкурста жеңіске жетті.

2

Икемді кілт ұзындығы

128, 192 және 256 биттік кілттерді қолдайды. Ұзын кілт неғұрлым жоғары қауіпсіздікті қамтамасыз етеді.

3

Блоктық шифр

128 биттік блоктармен жұмыс істейді. Деректерді тұрақты өлшемді блоктарға бөліп өңдейді.

4

Қазіргі қолданыс

Wi-Fi қауіпсіздігінен бастап банктік транзакцияларға дейін кең ауқымда қолданылады.

AES әлемдік деңгейде мойындалған және қорғаныс, қаржы, денсаулық сақтау және басқа да маңызды салаларда қолданылады. Оның қауіпсіздігі мен тиімділігі өте жоғары деңгейде.

Симметриялық шифрлеудің артықшылықтары

Жоғары жылдамдық

Симметриялық алгоритмдер өте жылдам жұмыс істейді. Қарапайым математикалық операциялар қолданылады, сондықтан есептеу уақыты аз. Нақты уақыт режимінде деректерді шифрлауға өте қолайлы.

Үлкен деректер көлемі

Терабайттық ақпаратты тез шифрлау мүмкіндігі бар. Бұл үлкен файлдар, дерекқорлар және бұқаралық ақпарат ағындары үшін өте маңызды. Видео, аудио және үлкен мұрағаттарды өңдеуге тамаша.

Аз ресурс тұтыну

Процессорға, жадқа және энергияға аз жүктеме түседі. Қарапайым құрылғыларда да тиімді жұмыс істейді. Ұялы телефондар мен IoT құрылғылары үшін өте қолайлы.

Іске асыру қарапайымдығы

Алгоритмдер салыстырмалы түрде қарапайым және түсінікті. Әртүрлі программалау тілдерінде жеңіл іске асырылады. Көптеген дайын кітапханалар мен құралдар бар.

Осы артықшылықтары арқасында симметриялық шифрлеу әлі күнге дейін кең қолданылады, әсіресе үлкен көлемді деректерді қорғауда.

Симметриялық шифрлеудің кемшіліктері

Кілтті тарату мәселесі

Ең үлкен қиындық – құпия кілтті екі тарапқа да қауіпсіз жеткізу. Кілтті ашық арналар арқылы жіберу мүмкін емес, өйткені оны ұстап алу қаупі бар.

- Физикалық жеткізу керек болуы мүмкін
- Құпия кездесулер немесе арнайы курьерлер қажет
- Көп алушылар болған жағдайда күрделене түседі

Масштабталу қиындығы

N пайдаланушы бір-бірімен байланыс жасағысы келсе, N×(N-1)/2 кілт қажет. Мысалы, 100 пайдаланушы үшін 4,950 кілт керек болады!

Кілттің бір рет ұрланауы

Егер кілт бір рет ұрланса немесе жоғалса, сол кілтпен шифрланған барлық деректер қауіп төндіреді. Өткен және болашақ хабарламалар ашылуы мүмкін.

Аутентификация мәселесі

Симметриялық шифрлеу жіберушінің сәйкестігін растай алмайды. Кілті бар кез келген адам хабарлама жібере алады.

Осы шектеулер асимметриялық шифрлеудің пайда болуына себепкер болды.

Асимметриялық шифрлеу: негізгі түсінік

Асимметриялық шифрлеу 1970 жылдары криптографияда революция жасады. Бұл жүйе симметриялық шифрлеудің негізгі мәселесін – кілтті қауіпсіз тарату қиындығын – шешті.

Ашық кілт (Public Key)

Барлығына ортақ, еркін таратылатын кілт. Кез келген адам бұл кілтті біле алады және пайдалана алады.

- Ақпаратты шифрлау үшін қолданылады
- Электрондық қолтаңбаны тексеру үшін
- Қауіпсіз емес арналар арқылы таратуға болады

Жабық кілт (Private Key)

Құпия, тек иесінде сақталатын кілт. Оны ешкіммен бөліспеу керек және қауіпсіз жерде сақтау қажет.

- Ақпаратты дешифрлау үшін қолданылады
- Электрондық қолтаңба жасау үшін
- Ешқашан басқа адамдарға берілмейді

Шифрлеу схемасы

Алушының **ашық кілтімен** шифрлау → тек оның **жабық кілтімен** дешифрлау мүмкін

Қолтаңба схемасы

Жіберушінің **жабық кілтімен** қолтаңба → оның **ашық кілтімен** тексеру

RSA алгоритмі

RSA – ең танымал және кең қолданылатын асимметриялық шифрлеу алгоритмі. 1977 жылы MIT-тің үш ғалымы – Рон Ривест, Ади Шамир және Леонард Адлеман ойлап тапқан. Алгоритмнің аты олардың тегінің бас әріптерінен құралған.

01

Екі үлкен жай санды таңдау

p және q деген екі үлкен жай сан таңдалады (әдетте жүздеген цифрлы)

02

n санын есептеу

n = p × q болады, бұл модуль деп аталады

03

Эйлер функциясы

φ(n) = (p-1) × (q-1) есептеледі

04

Ашық кілт экспонентасы

e саны таңдалады (көбінесе 65537), φ(n)-ге өзара жай

05

Жабық кілт экспонентасы

$d = e^{-1} \bmod \varphi(n)$ есептеледі

06

Кілттер жасалды

Ашық кілт: (e, n), Жабық кілт: (d, n)

Қауіпсіздік негізі: Үлкен санды екі жай санның көбейтіндісіне жіктеу (факторизация) өте қиын есептеу мәселесі. Қазіргі компьютерлермен 2048 биттік санды жіктеу практикалық тұрғыда мүмкін емес.

ЭЦҚ (электрондық цифрлық қолтаңба)

Электрондық цифрлық қолтаңба – асимметриялық криптографияның ең маңызды практикалық қолданысы. Ол құжаттың түпнұсқалығын, бүтіндігін және жіберушінің сәйкестігін растайды.

Құжат дайындау

Қол қоюға арналған электрондық құжат немесе хабарлама

Хэш есептеу

Құжаттың бірегей "баспасын" жасау (SHA-256 немесе басқа хэш-функция)

Жабық кілтпен шифрлау

Хэшті қол қоюшының жабық кілтімен шифрлау – бұл қолтаңба

Жіберу

Құжат пен қолтаңбаны алушыға жіберу

Тексеру

Алушы ашық кілтпен қолтаңбаны тексеріп, құжаттың өзгермегенін растайды

Заңдық күші

Көптеген елдерде ЭЦҚ қолмен қойылған қолға тең заңдық күшке ие

Теріске шығаруға болмайды

Қол қойған адам кейіннен бас тарта алмайды

Уақыт белгісі

Қолтаңба қашан қойылғанын дәл анықтауға болады

Асимметриялық шифрлеудің артықшылықтары



Қауіпсіз кілт алмасу

Ашық кілтті еркін тарата аласыз – ол қауіпсіз емес арналар арқылы жіберілсе де мәселе туғызбайды. Жабық кілт ешқашан тасымалданбайды, сондықтан ұрлану қаупі жоқ.



Аутентификация мүмкіндігі

Жіберушінің сәйкестігін дәл анықтауға болады. ЭЦҚ арқылы хабарламаның шынайы қай адамнан келгенін растай аласыз. Бұл маңызды транзакциялар үшін өте қажет.



Жақсы масштабталу

Әр пайдаланушыға тек бір кілт жұбы қажет. N пайдаланушы үшін тек 2N кілт керек (симметриялық жүйеде N^2-ге жуық кілт қажет болатын).



Теріске шығарылмайтындық

Жабық кілтімен қол қойған адам кейіннен "бұл мен емеспін" деп айта алмайды. Бұл электрондық коммерция және заңды транзакциялар үшін өте маңызды.

Осы артықшылықтары арқасында асимметриялық шифрлеу қазіргі Интернеттің қауіпсіздігінің негізі болып табылады.

Асимметриялық шифрлеудің кемшіліктері

Төмен жылдамдық

Симметриялық алгоритмдерге қарағанда 100-1000 есе баяу жұмыс істейді. Күрделі математикалық операциялар (үлкен сандармен дәрежелеу, модулярлық арифметика) көп уақыт алады.

- RSA шифрлеу/дешифрлау ресурс көп тұтынады
- Өнімділік маңызды жүйелерде проблема тудыруы мүмкін

Үлкен деректерге қолайсыз

Мегабайттық немесе гигабайттық файлдарды асимметриялық алгоритммен шифрлау практикалық тұрғыда мүмкін емес. Әдетте тек кішкентай деректерді (кілттерді, хэштерді) шифрлауға қолданылады.

Кілттің үлкен өлшемі

Қауіпсіздікті қамтамасыз ету үшін өте ұзын кілттер қажет. Қазіргі уақытта 2048-4096 биттік кілттер стандарт болып табылады.

- Симметриялық 128 бит ≈ Асимметриялық 3072 бит
- Кілттерді сақтау және тасымалдау қиынырақ

Күрделі басқару

Кілттер инфрақұрылымын басқару қиын. Сертификаттар, сертификаттау орталықтары (CA), кілттердің қолданыс мерзімі – барлығын дұрыс басқару керек.

Осы себептер бойынша практикада асимметриялық және симметриялық шифрлеу бірге қолданылады.

Гибридтік шифрлеу жүйелері

Гибридтік шифрлеу екі әдістің артықшылықтарын біріктіреді: асимметриялық криптографияның кілт алмасу қауіпсіздігі мен симметриялық криптографияның жылдамдығы.

1. Сессиялық кілт генерациясы

Кездейсоқ симметриялық кілт жасалады (мысалы, AES-256 кілті). Бұл кілт тек бір байланыс сессиясы үшін қолданылады.

1

2. Кілтті асимметриялық шифрлеу

Сессиялық кілт алушының ашық кілтімен шифрланады (RSA немесе ECC қолданып). Қауіпсіз емес арналар арқылы жіберуге болады.

2

3. Деректерді симметриялық шифрлеу

Негізгі деректер (файл, хабарлама) сессиялық кілтпен жылдам шифрланады (AES алгоритмімен). Үлкен көлемдегі деректерге тиімді.

3

4. Алушы дешифрлейді

Алушы өзінің жабық кілтімен сессиялық кілтті алады, содан кейін сол кілтпен деректерді ашады.

4

Артықшылықтары

- Асимметриялық кілт алмасудың қауіпсіздігі
- Симметриялық шифрлеудің жылдамдығы
- Кез келген көлемдегі деректерді өңдеу
- Практикалық және тиімді шешім



TLS/SSL протоколы мысалы

TLS (Transport Layer Security) – бұл Интернетте қауіпсіз байланысты қамтамасыз ететін негізгі протокол. Веб-браузерде көрсетілетін HTTPS қосылымдарында қолданылады. TLS гибридтік шифрлеудің керемет мысалы.

Client Hello

Клиент (браузер) серверге қосылады және қолдайтын шифрлеу әдістерін ұсынады. TLS нұсқасы мен қолдайтын cipher suite тізімін жібереді.

Server Hello + Сертификат

Сервер өзінің сертификатын (ашық кілті бар) жібереді және cipher suite таңдайды. Сертификаттың растығын CA (сертификаттау орталығы) растаған.

Кілт алмасу

Клиент pre-master secret жасайды және оны серверден алған ашық кілтпен шифрлайды (RSA) немесе Diffie-Hellman алмасуын жүргізеді.

Сессиялық кілттер генерациясы

Екі тарап та бірдей симметриялық кілттерді (session keys) есептейді. Әрі қарай барлық деректер AES немесе ChaCha20 алгоритмімен шифрланады.

Қауіпсіз деректер алмасу

Веб-беттер, формалар, логиндер – барлығы симметриялық кілтпен жылдам шифрланып тасымалданады.

Маңызды факт: Әр HTTPS сессиясы үшін жаңа уникалды сессиялық кілттер генерацияланады. Бұл "forward secrecy" деп аталатын қосымша қауіпсіздік қабатын қамтамасыз етеді.

Қазіргі заманғы қолдану салалары

Электрондық пошта (PGP/GPG)

Pretty Good Privacy және GnuPG хаттарды шифрлау мен электрондық қолтаңба қою үшін гибридтік криптографияны қолданады.

- RSA немесе ECC асимметриялық кілттер
- AES симметриялық шифрлеу хат мазмұны үшін
- Жеке тұлғалар мен компаниялар арасында кең таралған

VPN және корпоративтік желілер

Виртуалды жеке желілер қашықтан қауіпсіз қосылу үшін шифрлеу қолданады.

- IPsec, OpenVPN, WireGuard протоколдары
- Асимметриялық аутентификация + симметриялық туннель
- Қызметкерлердің қашықтан жұмысын қорғау

Мобильді қосымшалар

Смартфондардағы қосымшалар деректерді қорғау үшін шифрлеуді белсенді пайдаланады.

- WhatsApp, Signal – end-to-end шифрлеу
- Банктік қосымшалар – транзакциялар қорғанысы
- Бұлттық сақтау қосымшалары

Блокчейн және криптовалюталар

Bitcoin, Ethereum және басқа криптовалюталар криптографияға негізделген.

- ECDSA (Elliptic Curve DSA) қолтаңбалар
- Хэш-функциялар (SHA-256)
- Ашық және жабық кілттер қаражатты басқару үшін

IoT құрылғылары

Заттар интернеті құрылғылары шектеулі ресурстарда шифрлеу қолданады.

- Жеңіл криптографиялық алгоритмдер
- Ақылды үй жүйелері
- Денсаулық сақтау құрылғылары

Бұлттық қызметтер

AWS, Azure, Google Cloud – барлық бұлттық провайдерлер шифрлеуді қолданады.

- Деректерді сақтау кезінде (at rest) шифрлеу
- Тасымалдау кезінде (in transit) шифрлеу
- Клиенттік кілттерді басқару (BYOK)

Ақпараттық қауіпсіздіктің заманауи қатері

Криптография статикалық ғылым емес – ол үнемі дамып, жаңа қатерлерге бейімделіп отырады. Ең үлкен қауіп қазір кванттық есептеулерден келіп отыр.

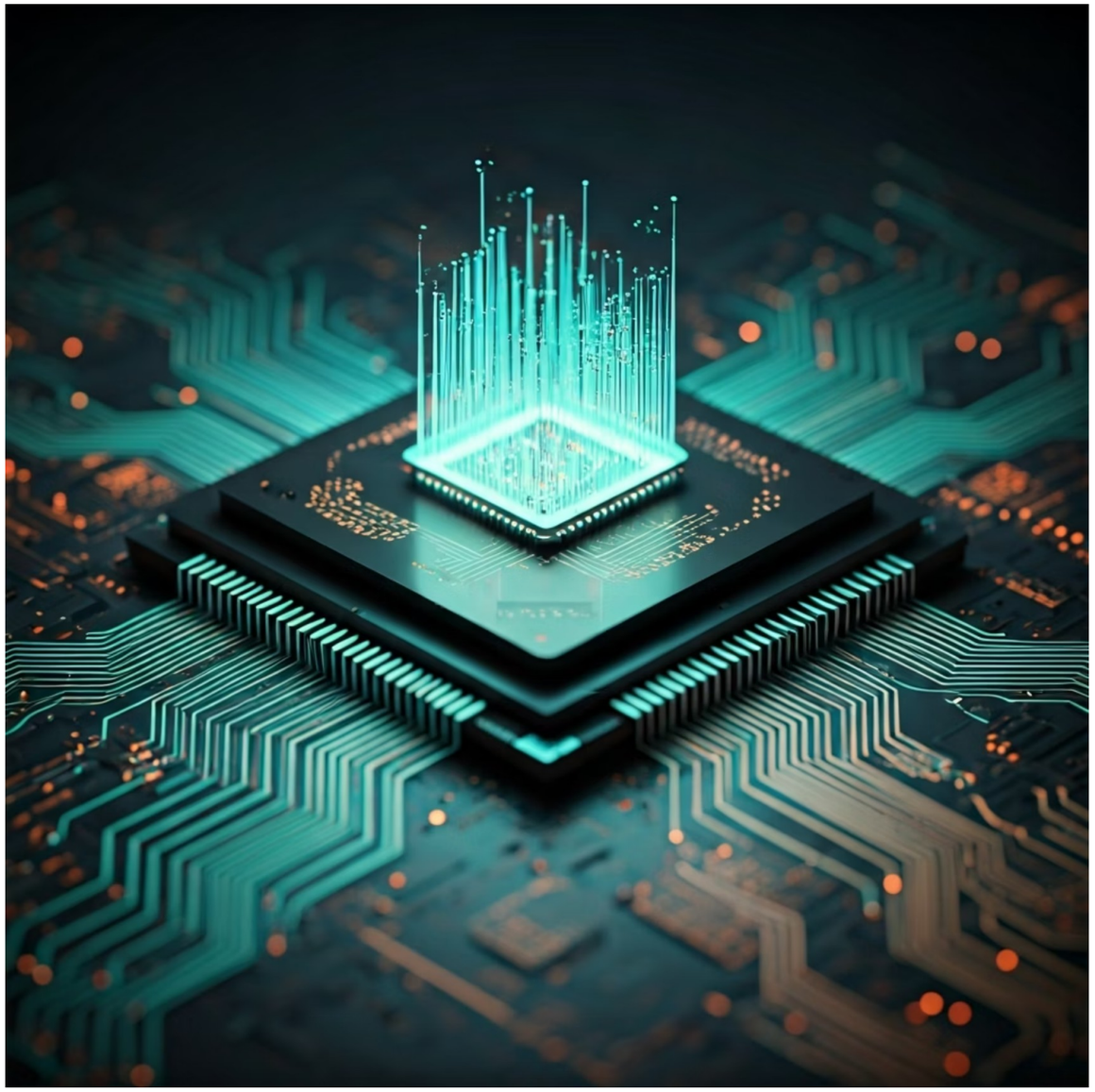
Кванттық компьютерлердің қаупі

Кванттық компьютерлер Шор алгоритмін қолдана отырып, RSA мен ECC сияқты қазіргі асимметриялық алгоритмдерді тиімді бұза алады.

- Үлкен сандарды факторизациялау экспоненциалды емес, полиномдық уақытта шешіледі
- 2048 биттік RSA кілтті кванттық компьютер бірнеше сағатта бұзуы мүмкін
- Дискреттік логарифм мәселесі де шешілетін болады

Қазіргі жағдай

Әлі толық қуатты кванттық компьютерлер жоқ, бірақ жылдам дамып келеді. Google, IBM, Қытай ғалымдары үлкен прогресске жетуде.



"Harvest now, decrypt later"

Қауіпті тенденция: шабуылдаушылар қазір шифрланған деректерді жинап, болашақта кванттық компьютермен ашуды жоспарлауда.

Уақыт шектеулі: Сарапшылар 10-15 жылдан кейін кванттық компьютерлер қазіргі криптографияны бұза алады деп болжайды.

Кванттық криптографияның негіздері

Кванттық криптография – бұл кванттық механика заңдарына негізделген принципиалды жаңа қауіпсіздік тәсілі. Математикалық күрделілікке емес, физика заңдарына сүйенеді.

1

Кванттық кілт алмасу (QKD)

Quantum Key Distribution – кванттық каналдар арқылы кілттерді абсолютті қауіпсіз тарату әдісі.

- Фотондардың поляризациясын немесе фазасын қолдану
- Физика заңдары бойынша тыңдауды анықтау мүмкін
- Белгілі протокол: BB84 (Bennett-Brassard 1984)

2

Қауіпсіздік принципі

Кванттық күйді өлшеу оны өзгертеді (Heisenberg белгісіздік принципі). Егер біреу байланысты тыңдаса, бұл бірден анықталады.

Шабуылдаушы фотонды ұстап, өлшеп, қайта жіберсе, оның кванттық күйі өзгереді және заңды пайдаланушылар мұны байқайды.

3

Практикалық іске асыру

Кванттық криптография әлі шектеулі, бірақ жұмыс істейді:

- Оптикалық талшық желілері арқылы 100-400 км қашықтыққа
- Қытай спутниктер арқылы кванттық байланыс жүргізуде
- Банктер мен үкіметтер тестілеуде

Шектеулер: Қымбат жабдық, қысқа қашықтық, баяу жылдамдық – әзірге кванттық криптография кең таралуға дайын емес.

Болашаққа көзқарас: Постквантық криптография

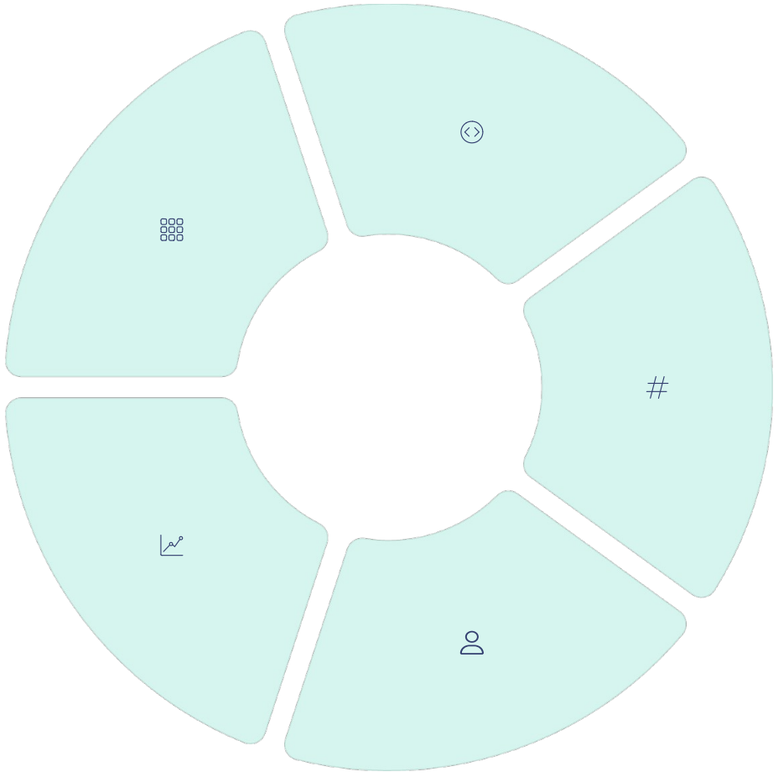
Постквантық криптография – классикалық компьютерлерде жұмыс істейтін, бірақ кванттық компьютерлерге төзімді алгоритмдер. Бұл қазіргі инфрақұрылымаға бейімделген практикалық шешім.

Lattice-based

Тор құрылымдарындағы қиын мәселелерге негізделген. NTRU, Kyber, Dilithium алгоритмдері.

Isogeny-based

Эллиптикалық қисықтардың изогениялары. SIKE алгоритмі (2022-де бұзылды).



Code-based

Қате түзету кодтарына негізделген. McEliece криптожүйесі 40+ жыл бойы бұзылмаған.

Hash-based

Хэш-функцияларға негізделген қолтаңбалар. SPHINCS+, XMSS алгоритмдері.

Multivariate

Көпөзгермелі теңдеулер жүйелерін шешу қиындығына негізделген.

NIST стандарттау процесі

АҚШ-тың Ұлттық стандарттар және технологиялар институты (NIST) 2016 жылдан бері постквантық алгоритмдерді бағалауда.

2022 жылғы нәтижелер:

- CRYSTALS-Kyber (шифрлеу)
- CRYSTALS-Dilithium (қолтаңба)
- FALCON (қолтаңба)
- SPHINCS+ (қолтаңба)



Ақпаратты шифрлеу алгоритмдерінің даму тарихы

Б.з.д. 500 ж. – Ежелгі Греция

Скитала – таспаны таяқшаға орап жазатын транспозициялық шифр. Спарталықтар әскери хабарламаларда қолданған.

Б.з.д. 58-51 ж. – Цезарь шифры

Юлий Цезарь қарапайым ауыстыру шифрын әскери хабарламаларда пайдаланды. Криптография тарихындағы ең белгілі мысал.

1467 ж. – Альберти дискісі

Леон Баттиста Альберти полиалфавитті шифрді ойлап тапты. Қазіргі криптографияның бастауы.

1918 ж. – Enigma машинасы

Артур Шербиус электромеханикалық роторлы шифрлау машинасын жасады. Екінші дүниежүзілік соғыста немістер қолданды.

1945 ж. – Claude Shannon жұмысы

"Криптография математикалық теориясы" – қазіргі криптографияның ғылыми негізі қаланды.

1976 ж. – Диффи-Хеллман

Асимметриялық криптографияның бастамасы. Ашық кілт идеясы революция жасады.

1977 ж. – RSA алгоритмі

Ривест, Шамир, Адлеман коммерциалды асимметриялық алгоритмді жариялады. Әлі күнге дейін кең қолданылады.

1997 ж. – AES конкурсы

NIST DES орнына жаңа стандарт іздеді. 15 кандидаттан Rijndael жеңіске жетті.

2001 ж. – AES стандарты

Advanced Encryption Standard ресми шифрлеу стандарты болды. Қазір барлық жерде қолданылады.

2009 ж. – Bitcoin пайда болды

Блокчейн технологиясы криптографияны жаңа деңгейге көтерді. ECDSA қолтаңбалар негізі.

2016 ж. – Постквантты стандарттау

NIST кванттық қауіпке дайындықты бастады. Жаңа дәуір басталды.

2024 ж. – Болашаққа қадам

Постквантты стандарттар жарияланды. Кванттық криптография дамуда. Жасанды интеллект криптоанализде қолданылуда.

Ақпаратты шифрлеудің заңнамалық және этикалық аспектілері

Криптография тек техникалық мәселе емес – ол құқықтық, саяси және этикалық сұрақтарды тудырады. Жеке құпиялылық пен мемлекеттік қауіпсіздік арасындағы тепе-теңдік қиын мәселе.

Құпиялылық құқығы

Дүниежүзілік адам құқықтары декларациясының 12-бабы жеке өмірге қол сұқпауды кепілдейді. Шифрлеу – бұл құқықты іске асырудың құралы.

- Еуропада GDPR жеке деректерді қорғауды талап етеді
- Шифрлеу – деректерді қорғаудың ең тиімді әдісі
- Компаниялар пайдаланушылар деректерін шифрлеуге міндетті

Мемлекеттік бақылау

Көптеген үкіметтер терроризммен күрес және қылмысты анықтау үшін шифрланған байланысқа қол жеткізуді талап етеді.

- "Backdoor" (артқы есік) талаптары
- Заңды ұстап алу (lawful interception)
- Криптографияны әлсірету ұсыныстары



Этикалық дилемма

Күшті шифрлеу қылмыскерлер мен террористерге де қолжетімді. Бірақ оны әлсірету барлық адамдардың қауіпсіздігін төмендетеді.

> **Техникалық шындық:** "Тек жақсылар үшін" backdoor жасау мүмкін емес. Кез келген әлсіздік шабуылдаушылар табады.

Халықаралық айырмашылықтар

Әртүрлі елдер шифрлеуді әртүрлі реттейді:

- АҚШ, ЕО: салыстырмалы түрде еркін
- Қытай, Ресей: қатаң бақылау
- Кейбір елдер күшті шифрлеуді тыйым салады

Қазақстандағы ақпараттық қауіпсіздік пен шифрлеу

Қазақстан ақпараттық қауіпсіздік саласын белсенді дамытуда және өз криптографиялық стандарттарын құруда.

1

Ұлттық қауіпсіздік стратегиясы

Қазақстан Республикасының 2026 жылға дейінгі кибер қауіпсіздік тұжырымдамасы ақпараттық инфрақұрылымды дамытуды көздейді.

2

Техникалық реттеу комитеті

Қазақстанда криптографиялық құралдарды сертификаттау және қолдану тәртібі белгіленген. Ақпараттық технологиялар комитеті басқарады.

3

ҰЭҚ (Ұлттық электрондық цифрлық қолтаңба)

Қазақстанда электрондық үкімет қызметтері үшін міндетті. ГОСТ стандарттарына негізделген криптографиялық жүйе.

4

Қазақстандық криптоалгоритмдер

Ұлттық криптографиялық стандарттар әзірленуде. ГОСТ Р 34.10, ГОСТ Р 34.11 және басқа ресейлік стандарттар қолданылады.

5

Білім беру бағдарламалары

ҚазҰУ, Satbayev University, ҚБТУ-да ақпараттық қауіпсіздік мамандары даярланады. Криптография курстары оқытылады.

Астана Хаб және инновациялар

Қазақстан халықаралық технологиялық орталыққа айналуды мақсат етуде. Кибер қауіпсіздік өнімдерін әзірлеу қолдау табуда.



Танымал криптографтар мен олардың еңбектері



RSA үштігі

Рон Ривест, Ади Шамир, Леонард Адлеман – 1977 жылы RSA алгоритмін жасаған. Шамир Тьюринг сыйлығын алды (2002).



Диффи-Хеллман

Уитфилд Диффи және Мартин Хеллман – асимметриялық криптографияның негізін қалаушылар (1976). Тьюринг сыйлығы (2015).



Ралф Меркл

Диффи-Хеллманмен бірге ашық кілт криптографиясын дербес ойлап тапқан. Merkle tree – блокчейнде қолданылады.



Клод Шеннон

"Криптографияның атасы" – 1945-49 жж. ақпарат теориясы мен криптографияның математикалық негізін қалады.



Дамен мен Риймен

Жоан Дамен және Винсент Риймен – бельгиялық криптографтар, Rijndael/AES авторлары (1998-2001).



Брюс Шнайер

Танымал қауіпсіздік сарапшысы, "Applied Cryptography" кітабының авторы. Blowfish және Twofish алгоритмдерін жасаған.

Бұл ғалымдардың еңбектері қазіргі цифрлық әлемнің қауіпсіздігін қамтамасыз етуде. Олардың жасаған алгоритмдері күнделікті миллиардтаған транзакцияларды қорғайды.

Қауіпсіздік инциденттері мен шифрлеудің рөлі

1

2013 – Эдвард Сноуден ашуы

АҚШ-тың NSA және Британияның GCHQ арнайы қызметтері әлемдік байланысты кең ауқымда тыңдап отырғаны анықталды. PRISM, XKeyscore бағдарламалары ашылды.

Нәтижесі: Күшті шифрлеуге деген сұраныс күрт өсті. WhatsApp, Signal, Telegram end-to-end шифрлеуді енгізді.

2

2014 – Heartbleed (OpenSSL осалдығы)

OpenSSL кітапханасында сыни қате табылды. Миллиондаған сервер осал болды, жеке кілттер және құпия деректер ұрланды.

Сабақ: Ашық бастапқы кодтың маңыздылығы және криптографиялық кітапханаларды мұқият тексеру қажеттілігі.

3

2017 – WannaCry ransomware

Windows-тағы EternalBlue осалдығын пайдаланып, ransomware 150+ елде жүздеген мың компьютерді шифрлады. Денсаулық сақтау, банктер зардап шекті.

Қорғаныс: Дұрыс резервтік көшірмелер мен шифрлеу зардапты азайтуға көмектесті.

4

2018 – Cambridge Analytica скандалы

Facebook пайдаланушыларының деректері рұқсатсыз жиналып, саяси мақсаттарда қолданылды. 87 миллион адам әсер етті.

Шешім: Деректерді шифрлеу және қатаң қол жеткізу бақылауының маңыздылығы.

5

2021 – Colonial Pipeline шабуылы

АҚШ-тағы майпроводын басқаратын жүйе ransomware шабуылына ұшырады. Компания $4.4 млн. төлеуге мәжбүр болды.

Салдары: Критикалық инфрақұрылымды қорғаудың стратегиялық маңызы дәлелденді.

6

2023 – MOVEit Transfer осалдығы

Кең қолданылатын файл тасымалдау бағдарламасындағы осалдықты пайдаланып, миллиондаған адамның деректері ұрланды.

Қорытынды: Файлдарды тасымалдау кезінде end-to-end шифрлеу міндетті.

Ақпаратты шифрлеу саласындағы инновациялар

Гомоморфикалық шифрлеу

Революциялық технология: деректерді дешифрламай-ақ өңдеуге мүмкіндік береді. Мысалы, шифрланған сандарды қосуға немесе көбейтуге болады.

Қолданылуы:

- Бұлттық есептеулерде құпиялылық
- Медициналық деректерді сақтау
- Қаржылық талдаулар
- Машиналық оқыту шифрланған деректермен

Қиындықтары:

Өте баяу (қарапайым AES-тен мыңдаған есе). Практикалық іске асыру әлі күнге дейін шектеулі.



Әзірлеушілер:

- Microsoft SEAL кітапханасы
- IBM HElib жобасы
- Google Private Join and Compute

Блокчейн және криптография

Блокчейн технологиясы криптографияны негізге алады және жаңа қолдану аясын ашты.

Хэш-функциялар

SHA-256 блоктарды байланыстыруда. Тізбекті бұзу практикалық тұрғыда мүмкін емес.

Цифрлық қолтаңбалар

ECDSA транзакцияларды растауда. Жеке кілт – қаражатты иелену дәлелі.

Merkle tree

Деректерді тиімді тексеруге мүмкіндік береді. Биткоинде транзакцияларды ұйымдастыруда қолданылады.

Zero-knowledge proof

Ақпаратты ашпай-ақ оның бар екенін дәлелдеу. Zcash, Monero жасырын транзакцияларда пайдаланады.

Қорытынды: Ақпаратты шифрлеудің болашағы

Шифрлеу технологиясы тоқтамай дамып келеді. Болашақта бірнеше негізгі тренд байқалады:

Постквантты дәуірге өту

Келесі 5-10 жылда барлық жүйелер постквантты алгоритмдерге көшуі керек. Бұл үлкен ауыстыру жұмыстары болады.

Гомоморфикалық шифрлеудің жетілуі

Жылдамдық артып, практикалық қолданыс кеңейеді. Құпиялылықты сақтаған есептеулер стандарт болады.

Жасанды интеллект интеграциясы

AI криптоанализде және жаңа алгоритмдер табуда қолданылады. Бірақ шабуылдаушылар да AI пайдаланады.

IoT және шектеулі құрылғылар

Жеңіл криптография дамиды. Миллиардтаған IoT құрылғылары қауіпсіздікті қажет етеді.

Заңнама мен технологияның үйлесімі

Халықаралық стандарттар қажет. Құпиялылық пен заңды талаптар арасында баланс іздеу жалғасады.

Негізгі принциптер өзгермейді

- Криптография қауіпсіздіктің негізі болып қала береді
- Үнемі дамып отырған ғылым
- Математика мен компьютерлік ғылымның түйісуі
- Адам факторы әлі де маңызды (кілттерді дұрыс басқару)



Шифрлеу – бұл тек технология емес, бұл цифрлық дәуірдегі еркіндік пен қауіпсіздіктің кепілі.