15-ДӘРІС
ШИФРЛАРДЫҢ БЕРІКТІЛІГІ

Дәрістің мақсаты

Криптографиялық беріктілік ұғымын жүйелеу, теориялық және практикалық беріктілікті ажырату, кілт кеңістігі, есептеу күрделілігі, алгоритм құрылымы және іске асыру қауіпсіздігінің шифр сенімділігіне әсерін түсіндіру.

Криптографиялық беріктілік

Шифрдың беріктілігі – қарсыласқа қолжетімді ақпарат пен есептеу ресурстары жағдайында қорғалатын мәліметті немесе құпия кілтті қалпына келтірудің қиындығын сипаттайтын қасиет. Беріктілік бір ғана кілт ұзындығымен анықталмайды; алгоритмнің математикалық құрылымы, қолдану режимі және іске асыру сапасы да маңызды.

Теориялық беріктілік

Теориялық немесе ақпараттық беріктілік есептеу қуатына тәуелсіз қауіпсіздік ұғымымен байланысты. Бір реттік блокнот қажетті шарттар орындалғанда ақпараттық-теориялық қауіпсіздіктің классикалық мысалы болып саналады. Бірақ мұндай жүйеде кілтті басқару практикалық жағынан күрделі.

Практикалық беріктілік

Практикалық немесе есептеуіш беріктілік шабуылды орындауға қажет уақыт, жады, операция саны және басқа ресурстардың қолжетімді шектен жоғары болуына сүйенеді. Қазіргі криптографияның басым бөлігі дәл осы есептеуіш қиындық қағидасына негізделеді.

Кілт кеңістігі

Егер кілт n биттен тұрса және барлық кілт тең ықтималды болса, мүмкін кілттер саны 2^n. Толық перебордың ең нашар жағдайдағы жұмысы барлық кілттерді тексерумен байланысты, ал орташа жағдайда шамамен кеңістіктің жартысы қарастырылуы мүмкін.

$$|K| = 2^n$$

Дегенмен үлкен кілт кеңістігі алгоритмде құрылымдық әлсіздік жоқ дегенді білдірмейді.

Шабуыл модельдері

Модель	Қарсыласқа белгілі ақпарат
Тек шифрмәтін	Бір немесе бірнеше шифрмәтін
Белгілі ашық мәтін	Ашық мәтін мен сәйкес шифрмәтін жұптары
Таңдалған ашық мәтін	Белгілі ережелер шегінде таңдалған кірістердің шифрмәтіндері
Таңдалған шифрмәтін	Белгілі ережелер шегінде таңдалған шифрмәтіндерге байланысты нәтижелер

Криптоталдау және толық перебор

Толық перебор алгоритм құрылымын пайдаланбай, кілт кеңістігін тексеруге сүйенеді. Криптоталдау, керісінше, алгоритмнің математикалық, статистикалық немесе іске асыру қасиеттерін пайдаланып, толық іздеуден тиімдірек жол табуға ұмтылады. Шифрды бағалауда ең жақсы белгілі шабуылдардың күрделілігі ескеріледі.

Қауіпсіздік маржасы

Қауіпсіздік маржасы – алгоритм параметрлері мен белгілі шабуылдардың мүмкіндіктері арасындағы қорды сипаттайтын жалпы ұғым. Мысалы, көпраундты шифрда зерттеушілер азайтылған раунд нұсқаларына шабуыл табуы мүмкін, ал толық нұсқада қосымша раундтар қор ретінде қалады. Бұл бағалау алгоритмге тәуелді.

Алгоритмнің ашықтығы

Криптографиялық жүйенің қауіпсіздігі алгоритмнің құпия болуына ғана сүйенбеуі тиіс. Қазіргі криптографияда алгоритм ашық талдауға ұсынылып, негізгі құпия ретінде кілт сақталады. Ашық талдау алгоритмнің әлсіздіктерін ертерек анықтауға мүмкіндік береді.

Іске асыру қауіпсіздігі

Математикалық тұрғыдан берік алгоритм қате іске асырылса әлсіз болуы мүмкін. Кілтті дұрыс сақтамау, кездейсоқ мәндерді сапасыз генерациялау, параметрлерді қайта пайдалану немесе жанама арнадан ақпараттың шығуы жалпы жүйенің беріктілігін төмендетеді. Сондықтан алгоритм және оны іске асыру бөлек те, бірге де бағаланады.

Қауіпсіздік деңгейін бағалау

Бағалау кезінде кілт өлшемі, блок немесе параметр өлшемдері, белгілі шабуылдардың күрделілігі, қолдану режимі, кілт басқару, бағдарламалық және аппараттық іске асыру, стандарттар мен зерттеу нәтижелері қарастырылады. Бір көрсеткіш бойынша ғана қорытынды жасау жеткіліксіз.

Криптографиялық жүйенің толық беріктігі

Нақты ақпараттық жүйеде беріктілік тізбектің ең әлсіз бөлігімен шектелуі мүмкін. Берік шифр, бірақ әлсіз парольден алынған кілт; дұрыс алгоритм, бірақ кілттің ашық сақталуы; сенімді математика, бірақ қате протокол – барлығы жалпы қауіпсіздікті төмендетеді. Сондықтан криптографиялық қорғаныс жүйелік тұрғыдан қарастырылады.

Қорытынды

Шифрдың беріктілігі теориялық қасиеттердің, есептеу күрделілігінің, кілт кеңістігінің, белгілі криптоталдау әдістеріне төзімділіктің және дұрыс іске асырудың жиынтық нәтижесі. Қауіпсіздікті бағалау кезінде тек алгоритмді емес, кілттерді басқару мен бүкіл қолдану ортасын бірге қарастыру қажет.

Бақылау сұрақтары

1. Криптографиялық беріктілік дегеніміз не?
2. Теориялық және практикалық беріктіліктің айырмашылығы қандай?
3. n биттік кілт кеңістігінің өлшемі қандай?
4. Үлкен кілт кеңістігі неге жалғыз қауіпсіздік критерийі емес?
5. Толық перебор мен криптоталдаудың айырмашылығы неде?
6. Шабуыл модельдері қарсыласқа белгілі ақпарат бойынша қалай ажыратылады?
7. Қауіпсіздік маржасы нені білдіреді?
8. Алгоритмнің ашық болуы неге қауіпсіздікке қайшы емес?
9. Іске асырудағы қандай факторлар беріктілікті төмендетуі мүмкін?
10. Криптографиялық жүйені неге тұтас жүйе ретінде бағалау керек?

Әдебиеттер тізімі

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016. – 500 б.
2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері: сандар теориясының, топтардың, өрістердің, сақиналардың элементтері. Алматы: АЭжБУ, 2020.
3. Васильева И.Н. Криптографические методы защиты информации. Москва: Юрайт, 2024.
4. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024.
5. Омассон Ж.-Ф. О криптографии всерьез. Практическое введение в современное шифрование. Москва: ДМК Пресс, 2021.