15-ДӘРІС. ШИФРЛАРДЫҢ БЕРІКТІЛІГІ

- Теориялық және есептеуіш беріктілік
- Кілт кеңістігі, шабуыл модельдері және іске асыру қауіпсіздігі

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің оқу нәтижелері

- Шифр беріктілігінің құрамдастарын түсіндіру
- Теориялық және практикалық қауіпсіздікті ажырату
- Кілт кеңістігін есептеу
- Шабуыл модельдері мен қауіпсіздік маржасын сипаттау

Шифр беріктілігі деген не?

Шифрдың беріктілігі — құпия кілтті немесе мәліметті қалпына келтірудің қиындығы.

Ол алгоритмге, кілтке, қолдану режиміне және іске асыруға байланысты.

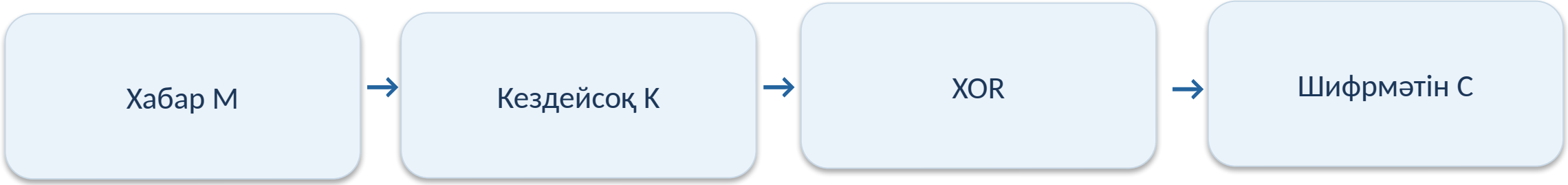
Теориялық беріктілік

Есептеу қуатына тәуелсіз қауіпсіздік қарастырылады.

Бір реттік блокнот — қажетті шарттар орындалса, классикалық мысал.

Бір реттік блокнот идеясы

$$C = M \oplus K;\ \ M = C \oplus K$$



Хабармен бірдей ұзындықтағы кездейсоқ кілт бір-ақ рет қолданылады.

Кілт құпия және тәуелсіз болуы тиіс; оны тарату қиын.

Практикалық беріктілік

Шабуылға қажет операция, уақыт, жады және шығын шектен жоғары болуы керек.

Қазіргі жүйелер көбіне есептеуіш қиындыққа сүйенеді.

Кілт кеңістігі

$$|K| = 2^n$$

n биттік кілттің барлық мүмкін мәндері: 2^n.

Орташа толық іздеу көлемі шамамен 2^{n-1} сынақ.

Кілт кеңістігі: шағын мысал

$$2^8 = 256;\ \ 2^{16} = 65\,536$$

8 бит → $2^8 = 256$ кілт.

16 бит → $2^{16} = 65\,536$ кілт.

128 бит → 2^{128} ықтимал кілт.

Кілт ұзындығы неге жеткіліксіз?

Үлкен кілт кеңістігі алгоритмнің құрылымдық кемшілігін жоққа шығармайды.

Әлсіз генерация немесе қате режим жүйені осал етуі мүмкін.

Шабуыл модельдері

Модель	Қарсыласқа белгілі ақпарат
Тек шифрмәтін	Шифрмәтіндер
Белгілі ашық мәтін	M және C жұптары
Таңдалған ашық мәтін	Таңдалған M үшін C
Таңдалған шифрмәтін	Таңдалған C бойынша нәтиже

Тек шифрмәтін моделі

Қарсыласқа бір немесе бірнеше шифрмәтін белгілі.

Қосымша ашық мәтін немесе шифрлау қызметі берілмейді.

Белгілі ашық мәтін моделі

Қарсылас бірнеше ашық мәтін мен сәйкес шифрмәтін жұбын біледі.

Бұл ақпарат шифрдың құрылымын зерттеуге пайдаланылуы мүмкін.

Таңдалған ашық мәтін моделі

Қарсылас белгілі ережелер шегінде кіріс хабарларды таңдап, шифрлау нәтижесін бақылай алады.

Бұл модель алгоритмнің беріктілігін бағалауда қолданылады.

Таңдалған шифрмәтін моделі

Қарсылас белгілі ережелер шегінде таңдалған шифрмәтіндерге қатысты нәтижелерді алады.

Қорғау механизмі осындай сценарийге де төзімді болуы қажет.

Толық іздеу мен криптоталдау

Толық іздеу — мүмкін кілттерді тексеру.

Криптоталдау — математикалық немесе статистикалық құрылым арқылы тиімдірек әдіс іздеу.

Күрделілікті салыстыру

8 биттік кілт: ең көбі 256 сынақ.

16 биттік кілт: ең көбі 65 536 сынақ.

Кілт ұзындығы 1 битке өссе, толық кеңістік 2 есе ұлғаяды.

Қауіпсіздік маржасы

Толық алгоритм мен белгілі шабуылға ұшыраған жеңілдетілген нұсқа арасындағы қор.

Мысалы, аз раундты нұсқада табылған әлсіздік толық нұсқаны міндетті бұзбайды.

Алгоритмнің ашықтығы

Қауіпсіздік тек алгоритмді жасыруға сүйенбеуі керек.

Ашық зерттеу әлсіздіктерді анықтауға мүмкіндік береді.

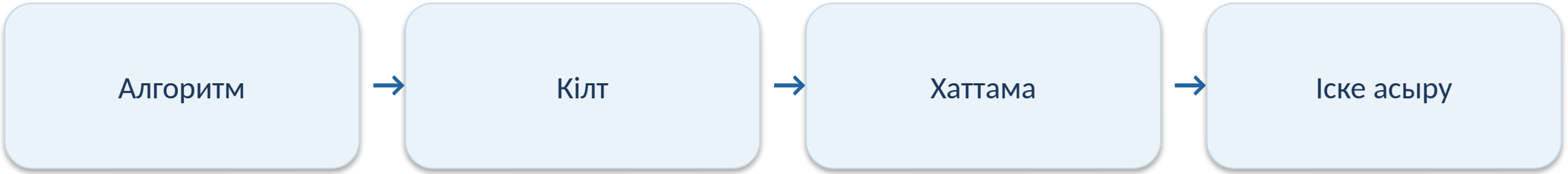
Негізгі құпия — кілт.

Іске асыру қауіпсіздігі

Кілтті ашық сақтау, кездейсоқтық сапасының төмендігі және параметрлерді қате қолдану қауіпті.

Жанама арналар да жүйенің беріктілігін төмендетуі мүмкін.

Қауіпсіздік тізбегі



Берік алгоритм әлсіз кілтті немесе қате хаттаманы өтей алмайды.

Жалпы қауіпсіздік ең әлсіз компонентпен шектелуі мүмкін.

Шифрды бағалау алгоритмі

1. Қауіп моделін анықтау.

2. Кілт кеңістігі мен параметрлерді тексеру.

3. Белгілі талдау нәтижелерін қарау.

4. Режим мен кілт басқаруды бағалау.

5. Іске асыру тәуекелдерін бағалау.

Жағдайлық тапсырма

Жүйеде берік шифр бар, бірақ кілт конфигурациялық файлда ашық сақталған.

Мәселе алгоритмде ме, әлде іске асыруда ма?

Жауап: іске асыру және кілт басқару әлсіздігі.

Теориялық және практикалық беріктілік

Критерий	Теориялық	Практикалық
Негізі	Ақпараттық шектеу	Есептеу қиындығы
Ресурс	Тәуелсіз	Маңызды
Мысал	Бір реттік блокнот	Қазіргі шифрлар

Қорытынды

Беріктілік бір ғана кілт ұзындығына тәуелді емес.

Шабуыл модельдері мен белгілі криптоталдау нәтижелері ескеріледі.

Алгоритм, кілт, хаттама және іске асыру бірге бағаланады.

Бақылау сұрақтары

Криптографиялық беріктілік деген не?

Теориялық және практикалық беріктілік қалай ажыратылады?

n биттік кілт кеңістігі қанша?

Үлкен кілт кеңістігі неге жеткіліксіз?

Толық іздеу мен криптоталдаудың айырмасы қандай?

Шабуыл модельдері қалай бөлінеді?

Қауіпсіздік маржасы деген не?

Әдебиеттер

Ахметов Б.С. және т.б. Қолданбалы криптология. Алматы, 2016.

Ахметов Б.С. және т.б. Криптография негіздері. Алматы, 2020.

Васильева И.Н. Криптографические методы защиты информации. 2024.

Лось А.Б. және т.б. Криптографические методы защиты информации. 2024.

Омассон Ж.-Ф. О криптографии всерьез. 2021.