Дәріс 7. Ашық кілтті криптография

Дәріскер: PhD Темирбекова Ж.Е.

Жоспар:

- Ашық кілтті криптография анықтамасы
- Диффи-Хеллман хаттамасы
- RSA криптожүйесі

Ашық кілтті криптография анықтамасы

- • 1976 жылы Диффи-Хеллман ұсынған
- • Біржақты функцияларға негізделген
- • Кері есепті шешу өте қиын
- • Ашық және жабық кілт қолданылады

Біржақты функция

- • x → f(x) оңай есептеледі
- • f(x) → x табу өте қиын
- • Қауіпсіздік осы қиындыққа сүйенеді

Құпия параметрі бар біржақты функция

- • Белгілі k параметрі болса, кері есеп шешіледі
- • Белгісіз k болса, шешу мүмкін емес
- • Ашық кілтті жүйелердің негізі

Ашық кілтті криптография идеясы

- • Әр қолданушыда 2 кілт бар: ашық және жабық
- • Ашық – шифрлау үшін
- • Жабық – дешифрлау үшін
- • Цифрлық қолтаңба, аутентификацияда қолданылады

Асимметриялық шифрлау схемалары

- 1) Ашық кілтпен шифрлау, жабықпен ашу
- 2) Жабықпен қол қою, ашықпен тексеру
- • Екі бағытта да жұмыс істей алады

Аутентификация ұғымы

- • Хабардың шын көзін растау
- • Байланыс сеансын, хабарламаны тексеру
- • Электрондық қолтаңба маңызды рөл атқарады

Диффи–Хеллман хаттамасы

- • Ашық арна арқылы ортақ кілт қалыптастыру
- • Шабуылдаушы кілтті таба алмайды
- • Математикалық негіз: модуль бойынша дәрежелеу

Диффи–Хеллман қадамдары

- 1) p — жай сан, g — база беріледі
- 2) A және B құпия a және b таңдайды
- 3) A: g^a mod p жібереді
- 4) B: g^b mod p жібереді
- 5) Ортақ кілт: g^(ab) mod p

Өзара аутентификация схемасы

- • Әр абонент өз функциясына ие
- • Ашық және жеке функциялар қолданылады
- • Хабарламалардың түпнұсқалығы тексеріледі

RSA криптожүйесінің негізі

- Екі үлкен жай санға негізделген
- n = p*q — модуль
- Ашық кілт: (e, n)
- Жабық кілт: (d, p, q)

Эйлер функциясы және RSA

- • φ(n) = (p−1)(q−1)
- • e және d сандары: e·d ≡ 1 (mod φ(n))
- • Ашық кілт — шифрлау
- • Жабық кілт — дешифрлау

RSA шифрлау

- • Мәтін M
- • Шифр: C = M^e mod n
- • Жабық кілтсіз M табу мүмкін емес

RSA дешифрлау

- • Шифр C
- • M = C^d mod n
- • Бұл тек жабық кілтпен мүмкін

Цифрлық қолтаңба (RSA)

- • Қол қою: S = M^d mod n
- • Тексеру: M = S^e mod n
- • Қол қою тек жабық кілтпен жасалады

RSA беріктігі

- • n санын факторизациялау өте қиын
- • p және q үлкен болуы тиіс
- • Кемінде 100 ондық таңбалы болуы ұсынылады

RSA мысалы

- p=17, q=31
- n=527, φ(n)=480
- e=7 таңдау
- d=343
- Шифрлау/дешифрлау қадамдары

Қорытынды

- Жоғарыда көрсетілгендей, ашық кілтті шифрлау жүйелері салыстырмалы түрде баяу жұмыс істейді. RSA шифрлау жылдамдығын арттыру үшін іс жүзінде шағын е шифрлау көрсеткіші қолданылады.

Қолданылған әдебиеттер тізімі

- 1. Абрамов М., Кренделев П. Криптографические защиты информации. / Абрамов М. – CRYPTO, 2022. – 249 с.
- 2. Blakley GR, Borosh I. Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. Computers & Mathematics with Applications. 2020, pp.169-178
- 3. Бияшев М., Петров П. Криптографическия с открытым ключом. / Бияшев М. – М.Пресс, 2021. – 219 с.