Дәріс 5. Гаммалау режимі

- Дәріскер: PhD Темирбекова Ж.Е.

Жоспар:

- Гаммалау режимінде шифрлау
- AES шифры
- Кілттерді генерациялау алгоритмі (Key Schedule)
- Кеңейту (жоспарлау) кілті
- Раундтық кілтті таңдау

Гаммалау режимі деген не?

- Гаммалау режимі — ашық мәтінді шифрлау үшін псевдокездейсоқ гамма тізбегін қолданатын тәсіл.
  - Әрбір 64 биттік блок жеке гаммамен XOR арқылы шифрланады.
  - Бұл әдіс ақпарат ағынын қауіпсіз қорғау үшін жиі қолданылады.
  - Гамма ашық мәтінге тәуелсіз жасалады және кілтке негізделеді.

Гамма блоктарының құрылымы

- Шифрлау процесінде әрбір жаңа блок үшін жаңа гамма (Гш(i)) шығарылады.
  - M — шифрланатын деректер блогының саны.
  - Соңғы блок толық 64 бит болмауы мүмкін, артық бөлігі қолданылмайды.
  - Барлық гамма блоктары тек бір кілтке сүйеніп құрылады.

Синхрондау векторы (N1, N2)

- Шифрлауды бастау үшін синхрондау хабарламалары N1 және N2 қолданылады.
  - Олар S массивіне битпен енгізіледі.
  - S массиві гамма генерациясының бастапқы нүктесі болып табылады.
  - Синхрондау векторы өзгерсе, шыққан гамма да толығымен өзгереді.

AES шифры жалпы түсінік

- AES — әлемдегі ең кең қолданылатын симметриялық блоктық шифр.
  - 128, 192 және 256 биттік кілт ұзындықтары қолданылады.
  - 128 биттік блокпен жұмыс істейді.
  - Қауіпсіз, жылдам және аппараттық деңгейде жақсы оңтайландырылған.

State матрицасы қалай құралады?

- Кіріс 16 байт мәлімет 4x4 матрица (State) ретінде орналастырылады.
  - Матрица жолдары емес, баған бойынша толтырылады.
  - State барлық раундтар кезінде өзгеріп отырады.
  - Әрбір баған — 32 биттік сөз ретінде қарастырылады.

AES раундтарындағы негізгі 4 операция

- 1) SubBytes — матрицаның әр байтын S-Box арқылы ауыстыру.
  - 2) ShiftRows — жолдарды циклик түрде жылжыту.
  - 3) MixColumns — бағандарды математикалық түрде араластыру.
  - 4) AddRoundKey — әр байтты раундтық кілтпен XOR жасау.

SubBytes — сызықты емес түрлендіру

- Әр байт S-Box кестесі арқылы жаңа мәнге ауыстырылады.
  - S-Box — криптографиялық тұрақты, алдын ала есептелген кесте.
  - Ол алгоритмнің қорғанысын жоғарылатады және күрделілігін арттырады.
  - Қарсы шабуылдарға қарсы күшті элемент.

ShiftRows — жолдарды жылжыту

- 0-жол өзгермейді.
  - 1-жол 1 байт солға жылжиды.
  - 2-жол 2 байт жылжиды.
  - 3-жол 3 байт жылжиды.
  - Бұл әрекет бағандардың араласуын күшейтеді.

MixColumns — бағандарды араластыру

- Әр баған GF(2^8) өрісіндегі полином ретінде қарастырылады.
  - Баған арнайы матрицаға көбейтіледі.
  - Әр жаңа баған төрт байттың сызықты комбинациясы.
  - Алгоритмнің диффузиясын күрт арттырады.

AddRoundKey — кілтпен байланыстыру

- State матрицасы раундтық кілтпен XOR жасайды.
  - Әр раундтың өз жеке кілті бар.
  - Кілт өзгерсе — шифрлау нәтижесі толығымен өзгереді.
  - Бұл AES-тің ең маңызды қауіпсіздік бөлігі.

Кері шифрлау операциялары

- InvSubBytes — S-Box кері кестесі бойынша байтты қалпына келтіреді.
  - InvShiftRows — жолдарды кері бағытта жылжытады.
  - InvMixColumns — бағандарды бастапқы жағдайына қайтарады.
  - Процесс раундтық кілттерді кері ретпен қолданады.

Key Schedule — кілтті кеңейту

- Бастапқы кілттен көптеген раундтық кілттер өндіріледі.
  - RotWord — сөзді байттар бойынша айналдыру.
  - SubWord — әр байтты S-Box арқылы ауыстыру.
  - Rcon — әр раундқа арналған тұрақты мәндер.

Кеңейтілген кілттің құрылуы

- Алғашқы Nk сөз — бастапқы кілт.
  - Әр келесі сөз алдыңғы сөздерден XOR арқылы жасалады.
  - Әр Nk-ші сөз RotWord, SubWord, Rcon арқылы өзгереді.
  - Нәтижесінде (Nr+1)*4 раундтық кілт алынады.

Раундтық кілттерді қолдану тәртібі

- 1-раундта — алғашқы 4 сөз.
  - 2-раундта — келесі 4 сөз.
  - Соңғы раундқа дейін осылай жалғасады.
  - Кері шифрлау кезінде кілттер кері ретпен қолданылады.

AES және гаммалау режимінің артықшылықтары

- AES өте тұрақты және заманауи стандарт.
  - Гаммалау режимі жоғары жылдамдық береді.
  - XOR операциясы деректерді тез өзгертеді.
  - Екі тәсіл бірігіп — сенімді криптографиялық жүйе береді.