Дәріс 9. Хэш функция

- Дәріскер: PhD Темирбекова Ж.Е.

Хэш функция анықтамасы

- Хэш функция – ерікті ұзындықтағы хабарламаны бекітілген ұзындықтағы мәнге түрлендіретін функция.

Криптографиялық хэш функция талаптары

- 1) Біржақтылық
- 2) Коллизияға төзімділік
- 3) Біркелкі таралу
- 4) Қарлы әсер (avalanche effect).

Хэш функция қолдану салалары

- 1) Деректер тұтастығын бақылау
- 2) Аутентификация
- 3) Электрондық қолтаңба.

Хэш функцияның жалпы сұлбасы

- Хабарлама блоктарға бөлінеді, әр блок қысу функциясынан өтеді.

MD5 алгоритміне кіріспе

- MD5 – 1991 жылы Ривест ұсынған хэш функция. 128 биттік мән шығарады.

MD5 – тұрақтылар T[i]

- Алгоритм 64 тұрақты мәнді (T[i]) қолданады, әр раундта біреуі пайдаланылады.

MD5 – бастапқы айнымалылар A,B,C,D

- A,B,C,D – 32 биттік регистрлер. Бастапқы мәндер алдын ала беріледі.

MD5 – негізгі функциялар F,G,H,I

- F,G,H,I – 32 биттік сызықтық емес функциялар, әр раундта қолданылады.

MD5 алгоритмінің қадамдары

- 1) Толықтау
- 2) Ұзындық қосу
- 3) 512 бит блоктарға бөлу
- 4) 64 раунд өңдеу.

SHA–1 алгоритміне кіріспе

- SHA–1 – 160 биттік хэш шығаратын алгоритм. 512 бит блоктармен жұмыс істейді.

SHA-1 блоктарды өңдеу

- Әр 512 биттік блок 80 Wt сөздеріне кеңейтіледі.

SHA–1 тұрақтылар мен айнымалылар

- Тұрақтылар Kt және айнымалылар A,B,C,D,E қолданылады.

SHA–1 раунд функциялары

- Төрт раунд: AND, XOR, majority функцияларымен орындалады.

Қорытынды

- MD5 және SHA–1 – хэштеу алгоритмдері, бірақ қазіргі таңда SHA–1 әлсіз деп саналады.

Ұсынылатын 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