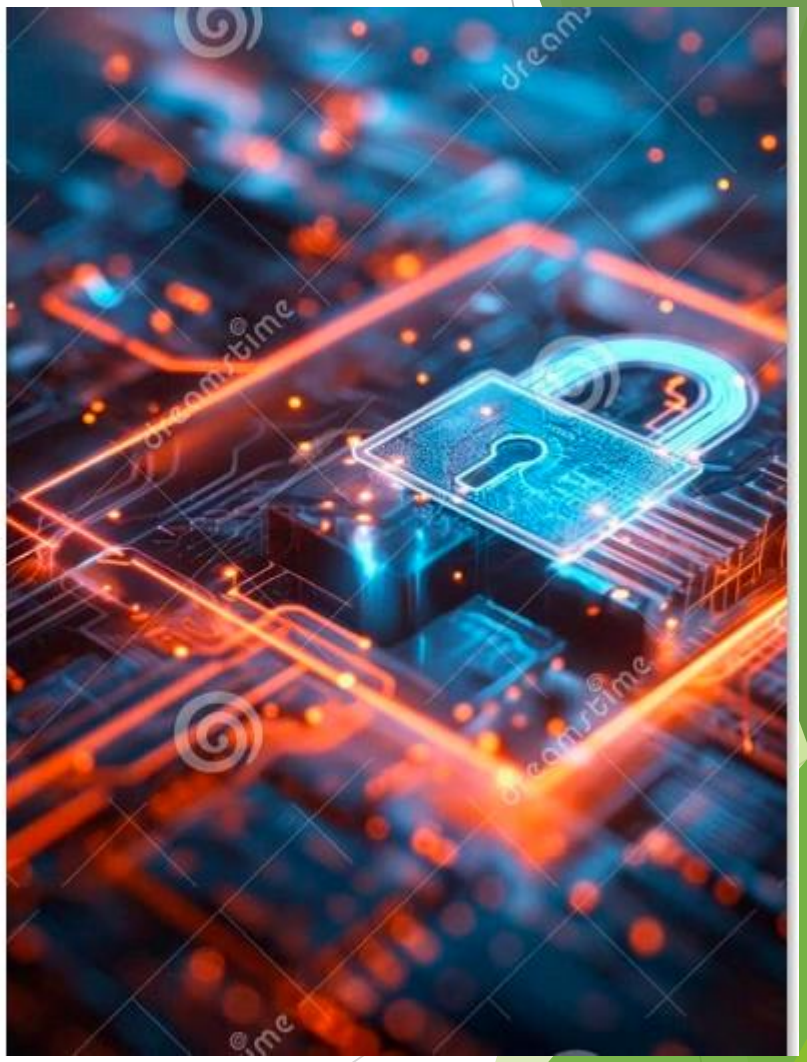
Отандық шифрлау стандарты

Бұл дәріс ГОСТ стандарты бойынша отандық шифрлау әдістерін, оның ішінде қарапайым ауыстыру және кірістіру режимдерін, сондай-ақ шифрланған деректерді дешифрлау принциптерін қамтиды.



Жоспар

01

ГОСТ бойынша отандық шифрлау стандарты

Негізгі алгоритм компоненттері мен құрылымы.

02

Қарапайым ауыстыру режимі

Деректерді шифрлау процесінің егжей-тегжейлі сипаттамасы.

03

Қарапайым кірістіру режиміндегі шифрлау алгоритмі

Бұл режимнің ерекшеліктері мен қолданылуы.

04

Қарапайым ауыстыру режимінде шифрланған деректерді дешифрлау

Шифрды шешу алгоритмі және оның жұмыс істеу принципі.

ГОСТ бойынша отандық шифрлау стандарты

ГОСТ стандарты бойынша отандық шифрлау алгоритмі күрделі құрылымға ие, ол деректерді қорғау үшін бірнеше компоненттерді пайдаланады:

- 256 биттік кілттерді сақтау құрылғысы (КСҚ).
- Төрт 32 биттік диск N1, N2, N3, N4.
- Тұрақтылары бар екі 32 разрядты диск N5, N6 (C1, C2).
- Екі 32 биттік модульді қосқыш (СМ1, СМ3).
- Бір 32 биттік модуль қосқышы (СМ2).
- Модуль 2 сумматор (СМ5).
- Циклдік ығысу R регистрі.





K алмастыру блогы

K алмастыру блогы сегіз алмастыру түйінінен тұрады (K1-K8), әрқайсысының ұзындығы 8 бит. Бұл блок 8x16 өлшемді кесте (матрица) болып табылады.

1

Векторды бөлу

32 разрядты V векторы сегіз ретті төрт разрядты векторға бөлінеді (V1-V8).

2

Ауыстыру

Әрбір Vi векторының төрт биті K кестесіндегі сәйкес kij санымен ауыстырылады.

3

Индекс анықтамасы

K блогының жол нөмірін анықтайтын i индексі сәйкес келеді, ал баған нөмірі αi санына тең.

Кілтті жазу және КСҚ толтыру

Кілтті жазу кезінде W1, W2, ..., W256 биттері КСҚ-ға енгізіледі. Wq {0,1} интервалында жатыр, q = 1 ÷ 256.

- W1 мәні X0 жетегінің бірінші разрядына.
- W32 мәні X0 жетегінің 32-ші разрядына.
- W33 мәні X1 жетегінің бірінші разрядына.
- W256 мәні X7 дискінің 32-ші разрядына енгізіледі.

КСҚ толтыруды және К ауыстыру блогының кестелерін анықтайтын кілттер құпия элементтер болып табылады.



Криптографиялық схемадағы жұмыс режимдері

Қарапайым ауыстыру

Әрбір ашық мәтін блогы шифрланған мәтін блогымен ауыстырылады. Блоктік шифрларда қолданылады.

Гаммалау режимі

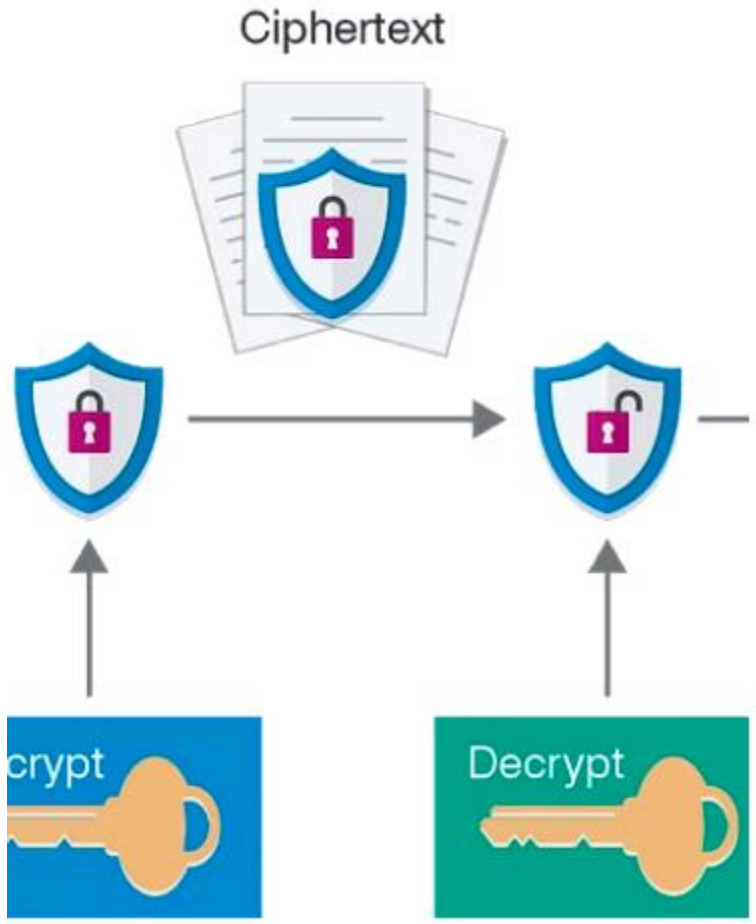
Жалған кездейсоқ реттілік (гамма) генераторы XOR операциясы арқылы ашық мәтінмен біріктіріледі. Ағынды шифрлауға жарамды.

Кері байланыспен гаммалау

Шығыс шифр мәтіні келесі гамманы құру үшін қолданылады, криптографиялық төзімділікті арттырады.

Имитациялық кірістіру

Деректердің тұтастығын және хабарламалардың аутентификациясын қамтамасыз етеді.



Қарапайым ауыстыру режимі

Шифрланатын ашық мәтіндік деректер әрқайсысы 64 биттік TN блоктарына бөлінеді. Әрбір блок N1 және N2 жетектеріне енгізіледі.

Шифрлау алгоритмі 32 циклден тұрады. Әр циклде КСҚ-дан толтырулар оқылып, түрлендіріледі және нәтижелер N1 мен N2 дискілеріне жазылады.

Шифрлау циклінің реті

32 циклде шифрлау кезінде сақтауды толтыруды таңдаудың келесі реті орындалады:

1. **1-8** циклдер
   X0, X1, X2, X3, X4, X5, X6, X7
2. **9-24** циклдер
   X0, X1, X2, X3, X4, X5, X6, X7 (үш рет қайталанады)
3. **25-32** циклдер
   X7, X6, X5, X4, X3, X2, X1, X0 (кері ретпен)



Қарапайым ауыстыру режимінде шифрды шешу

Шифрды шешу алгоритмі шифрлауға ұқсас, бірақ КСҚ-дан толтыруларды оқу реті өзгеше.

Шифрды шешу реті

- X0, X1, X2, X3, X4, X5, X6, X7
- X7, X6, X5, X4, X3, X2, X1, X0 (үш рет қайталанады)

Бұл кері түрлендіру бастапқы ашық мәтінді қайтарады.





Қорытынды және әдебиеттер

ГОСТ стандарты бойынша отандық шифрлау алгоритмі деректерді қорғаудың тиімді әдістерін ұсынады. Оның күрделі құрылымы мен әртүрлі режимдері ақпараттық қауіпсіздіктің жоғары деңгейін қамтамасыз етеді.

Қолданылған әдебиеттер тізімі:

- Гольдвассер С., Беллар М. Достижения в криптологии / Гольдвассер С. – М.: Триумф, 2016. – 513 с.
- Шнайер, Брюс. Криптографическая методы защиты информации, 26-я ежегодная международная конференция по криптологии, Санта-Барбара, Калифорния, США, 20–24 августа 2022 г.
- Фергюсон Н., Шнайер Б., Коно Т. Криптографическая инженерия: принципы проектирования и практическое применение. / Фергюсон Н. – М.: Пресс, 2022. – 416 с.