Дәріс 4. Отандық шифрлау стандарты

Жоспар:

1. ГОСТ бойынша отандық шифрлау стандарты
2. Қарапайым ауыстыру режимі
3. Қарапайым кірістіру режиміндегі шифрлау алгоритмі
4. Қарапайым ауыстыру режимінде шифрланған деректерді дешифрлау

ГОСТ бойынша отандық шифрлау стандарты

ГОСТ бойынша отандық шифрлау стандартының алгоритмі мыналарды пайдаланады:

– 256 биттік кілттерді сақтау құрылғысы (КСҚ), сегіз 32 биттік дискіден тұрады

$$\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3, \mathrm{X}_4, \mathrm{X}_5, \mathrm{X}_6, \mathrm{X}_7;$$

– төрт 32 биттік диск N_1, N_2, N_3, N_4;

– тұрақтылары жазылған N_5, N_6 екі 32 разрядты дискілер C_2 және C_1;

– екі 32 биттік модульді қосқыш 2^{32} $(\mathrm{CM}_1, \mathrm{CM}_3)$;

– 2 разрядтық қосынды модулінің бір 32 бит қосқышы (CM_2) бір 32–биттік модуль қосқышы $(2^{32} - 1)(\ \mathrm{CM}_4)$;

– модуль 2 сумматор (CM_5), қосқыштың сыйымдылығына шектеулер CM_5 сәйкес келмейді;

– циклдік ығысу R регистрі ең маңызды цифрға қарай он бір қадамға ауысады.

K алмастыру блогы сегіз алмастыру түйінінен тұрады,

$$K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8.$$

Әрбір түйіннің ұзындығы $K_i, i = 1, 2, \dots, 8$ бит. Бұл блок 8х16 өлшемді кесте (матрица) болып табылады. Мұндай кестенің элемент өлшемі 4 биттік k_{ij} (төрт разрядты вектор) саны болып табылады. Ауыстыру блогына келген 32 разрядты V векторы сегіз ретті төрт разрядты векторға бөлінеді.

$$V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8.$$

Әрбір $V_i, i = 1, 2, \dots, 8$, векторының төрт биті кейбір α_i санына тең. $V_i, i = 1, 2, \dots, 8$, әрқайсысы К кестесіндегі сәйкес k_{ij}санымен ауыстырылады. V_i–ді k_{ij}–мен ауыстырудың бұл режимінде K блогының жол нөмірін анықтайтын i индексі сәйкес келеді. Индекс V_i k_{ij} элементінің j бағанының саны $\alpha_i., j = \alpha_i$ санына тең, ол V_i векторының 4 битімен анықталады. Нәтижесінде 32 разрядты $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8$ векторы пайда болды. $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8$ разрядты вектормен ауыстырылады

$$k1j1, k2j2, k3j3, k4j4, k5j5, k1j6, k7j7, k8j8,$$

мұндағы $k1j1$ – K ауыстыру кестесінің j_1 саны бар 1-ші жол мен бағанның нөмірі; $k2j2$, – K ауыстыру кестесінің j_2 саны бар 2-ші жол мен бағанның нөмірі;

$k8j8$ – K ауыстыру кестесінің j_8 саны бар 8-ші жол мен бағанның нөмірі;

Жоғарыда j_1, j_2, …, j_8 баған сандары қалай анықталатыны түсіндіріледі (бұл сандар сәйкес V_i төрт разрядтық мәнімен анықталады).

Екілік векторларды қосу және циклдік ауыстыру кезінде ең маңызды разрядтар үлкен сандары бар сақтау құрылғыларының биттері болып саналады.

Кілтті жазғанда

$$W_1, W_2, \dots, W_{256},$$

W_q $\{0,1\}, q = 1 \div 256$ интервалында жатыр. КСҚ W_1 мәні X_0 жетегінің бірінші разрядына, W_{32} мәні X_0, ..., жетегінің екінші разрядына, W_{32} мәні X_0 жетегінің 32-ші разрядына енгізіледі; W_{33} мәні X_1 жетегінің бірінші разрядына, W_{34} мәні X_1, ..., жетегінің екінші разрядына, W_{64} мәні X_1 жетегінің 32-ші разрядына енгізіледі; W_{65} мәні X_2 жетегінің бірінші битіне енгізіледі және т.б. W_{256} мәні X_7 дискінің 32-ші разрядына енгізіледі.

Ақпаратты қайта жазу кезінде бір жетектің (қосқыштың) p разрядының мазмұны басқа жетектің (қосынғыштың) p цифрына қайта жазылады. N_6 және N_5 жетектерінің C_1 және C_2 толтыру тұрақтыларының мәндері 2-қосымшада келтірілген. КСҚ толтыруды және K ауыстыру блогының кестелерін анықтайтын кілттер құпия элементтер болып табылады және белгіленген тәртіппен жеткізіледі. К ауыстыру блогының кестелерін толтыру компьютерлік желіге ортақ ұзақ мерзімді негізгі элемент болып табылады.

Криптографиялық схемада төрт жұмыс режимі қарастырылған:

1) Деректерді қарапайым ауыстыру режимінде шифрлау (шифрын ашу). Бұл режимде әрбір ашық мәтін блогы Негізгі түрлендіруге сәйкес сәйкес шифрланған мәтін блогымен ауыстырылады. Бұл әдіс блоктық шифрларда қолданылады және кілтті дұрыс таңдағанда жоғары тұрақтылықты қамтамасыз етеді.

2) Гаммалау режимінде деректерді шифрлау (транскрипциялау). Бұл режимде 2 модульді қосу (XOR) операциясы арқылы ашық мәтінмен біріктірілген жалған кездейсоқ реттілік (гамма) генераторы қолданылады. Бұл әдіс ағынды шифрлауға жарамды және қорғалған коммуникацияларда кеңінен қолданылады.

3) Кері байланыспен гаммалау режимінде деректерді шифрлау (транскрипциялау). Классикалық гаммадан айырмашылығы, шығыс шифр мәтіні келесі гамманы құру үшін қолданылады. Бұл шифр мәтінінің бірдей ашық мәтін мен кілтпен қайталануына жол бермеу арқылы криптогрфиялық

төзімділікті арттырады.

4) Имитациялық кірістіруді әзірлеу режимі. Бұл режим деректердің тұтастығын және хабарламалардың аутентификациясын қамтамасыз етуге арналған. Кіріс негізінде берілетін ақпараттың өзгермейтіндігін тексеруге мүмкіндік беретін бақылау мәні (Имитациялық кірістіру) есептеледі.

Бұл режимдердің әрқайсысының мақсаты бар және криптографиялық жүйенің қауіпсіздігі мен өнімділігіне қойылатын талаптарға сәйкес қолданылады.

Қарапайым ауыстыру режимі

Шифрланатын ашық мәтіндік деректер әрқайсысы 64 биттік T_N блоктарына бөлінеді, мұндағы N ашық мәтіндегі блоктар саны. Егер j ашық мәтін блогының нөмірін, ал $a(j)$ және $b(j)$осы мәтіннің биттерінің мәнін білдірсе, онда кез келген блоктың кірісі

$$T_j = (a_1(j), a_2(j), \ldots, a_{31}(j), a_{32}(j), b_1(j), b_2(j), \ldots, b_{32}(j))$$

екілік ақпарат N_1 және N_2 жетектеріне $a_1(j)$ мәні N_1 бірінші цифрына, $a_2(j)$ мәні N_1 екінші цифрына енгізілетіндей және т.б. беріледі; $a_{32}(j)$ мәні N_1 32–ші битіне енгізіледі; $b_1(j)$ мәні N_2, бірінші цифрына, $b_2(j)$ мәні N_2 екінші цифрына енгізіледі және т.б.; $b_{32}(j)$ мәні N_2 32–ші битіне енгізіледі. Нәтижесінде блоктар пайда болады

$$a_{32}(s), a_{31}(\text{j}), \ldots, a_2(j), a_1(j)$$

Қарапайым ауыстыру режимінде қарапайым деректердің 64 биттік блогын шифрлау алгоритмі 32 циклден тұрады. Бірінші циклде N_1 қоймасының бастапқы толтырылуы CM_1 қосқышта X_0 қоймасының толтырылуымен 2^{32} модуль бойынша жинақталады, бұл ретте N_0 қоймасының толтырылуы сақталады. Қосындылау нәтижесі K алмастыру блогында түрлендіріледі және алынған вектор R регистрінің кірісіне жіберіледі, онда ол циклді түрде ең маңызды разрядтарға қарай он бір қадамға жылжиды. Ауыстыру нәтижесі CM_3 сумматорында N_2 дискінің 32 разрядты толтыруымен 2–разрядтық модуль бойынша жинақталады. CM_2 алынған нәтиже N_2-ге жазылады, ал N_1-дің ескі толтыруы N_2-ге қайта жазылады. Бірінші цикл аяқталады.

Кейінгі циклдар дәл осылай жүзеге асырылады, екінші циклде X_1 толтыру КСҚ-дан оқылады, үшінші циклде X_2 толтыру КСҚ-дан оқылады және т.б., сегізінші циклде X_7 толтыру КСҚ-дан оқылады. Тоғызыншыдан он алтыншыға дейінгі циклдерде, сондай–ақ он жетіншіден 24-ке дейінгі циклдерде КСҚ-дан толтырулар бірдей ретпен оқылады.

$$\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3, \mathrm{X}_4, \mathrm{X}_5, \mathrm{X}_6, \mathrm{X}_7.$$

25-тен 32-ге дейінгі соңғы сегіз циклде КСҚ толтыруларын оқу тәртібі керісінше өзгереді.

$$\mathbf{X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0}.$$

Осылайша, 32 циклде шифрлау кезінде сақтауды толтыруды таңдаудың келесі реті орындалады:

$$\mathbf{X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7},$$
$$\mathbf{X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7},$$
$$\mathbf{X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7}$$
$$\mathbf{X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0}$$

32 циклде CM_2 сумматорынан алынған нәтиже N_1, дискісіне енгізіледі, ал N_1 дискісінде ескі толтыру сақталады. N_1 және N_2 дискілерінің толтыруларын шифрлаудың 32 циклінен кейін алынған деректер ашық деректер блогына сәйкес шифрланған деректер блогы болып табылады.

Қарапайым ауыстыру режиміндегі шифрлау алгоритмін келесі (2.16), (2.17) формулалар түрінде жазуға болады:

$$a(j) = \big(a(j-1) * X_{(j-1)(mod\ 8)}\big)KR + b(j-1), \quad (2.16)$$
$$b(j) = a(j-1) \quad (2.17)$$

$j = 1 \div 24$ кезінде;

$$a(j) = (a(j-1) * X(32-j))KR + b(j-1),$$
$$b(j) = a(j-1)$$

$j = 25 \div 31$ кезінде;

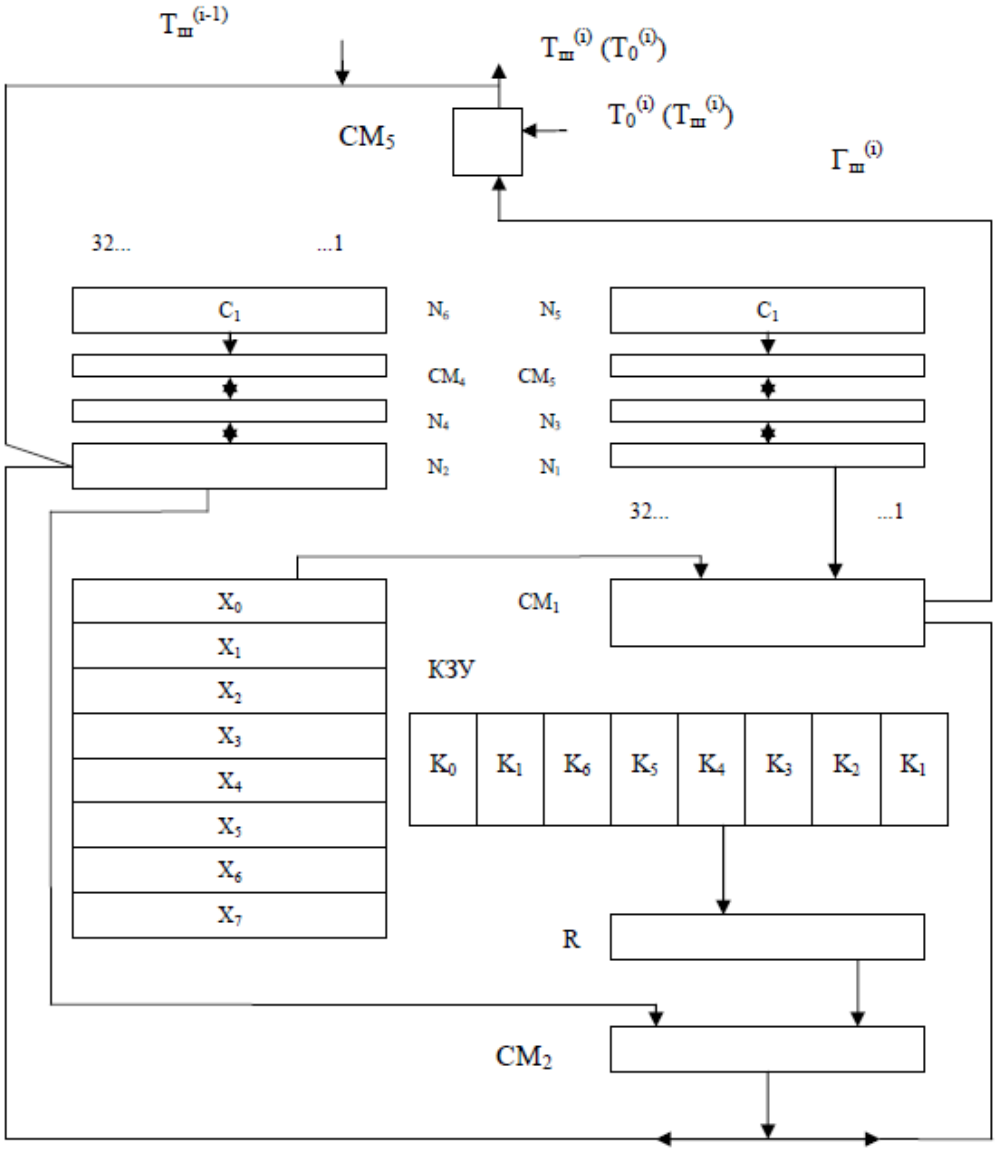
$$a(32) = a(31),$$
$$b(32) = (\ a(31) * X0\ )\ KR + b(31)$$

$j = 32$ кезінде, мұндағы $\mathrm{a}(0) = (\mathrm{a}_{32}(0), \mathrm{a}_{31}(0), \ldots, \mathrm{a}_1, (0))$ – бірінші шифрлау цикліне дейін N_1 бастапқы толтыру;

$b(0) = (b_{32}(0), b_{31}(0), \ldots, b_1(0))$ – бірінші шифрлау цикліне дейін N_2 бастапқы толтыру;

$j = 1 \div 32$ кезінде бізде $\mathrm{a}(j) = (\mathrm{a}_{32}(j), \mathrm{a}_{31}(j), \ldots, \mathrm{a}_1, (j))$ – j–ші шифрлау циклінен кейін N_1 толтыру;

$b(j) = (b_{32}(j), b_{31}(j), \ldots, b_1(j))$ – j–ші шифрлау циклінен кейін N_2 толтыру.



2.6 – сурет. *IDEA* алгоритмнің сұлбасы

+ белгісі 32–разрядты векторлардың модуль 2–нің разрядтық қосындысын білдіреді.

* таңбасы 2^{32} модулінің 32 разрядты векторларының қосындысын білдіреді. Екі бүтін сан a, b $(0 \leq a, b \leq 2^{32} - 1)$ келесі ережеге сәйкес 2^{32} модулінің қосындысын білдіреді:

– $a * b = a + b$, егер $a + b < 2^{32}$,

– $a * b = a + b - 2^{32}$, егер $a + b \geq 2^{32}$,

– R ең маңызды сандарға қарай он бір қадамға циклдік ығысу операциясы яғни,

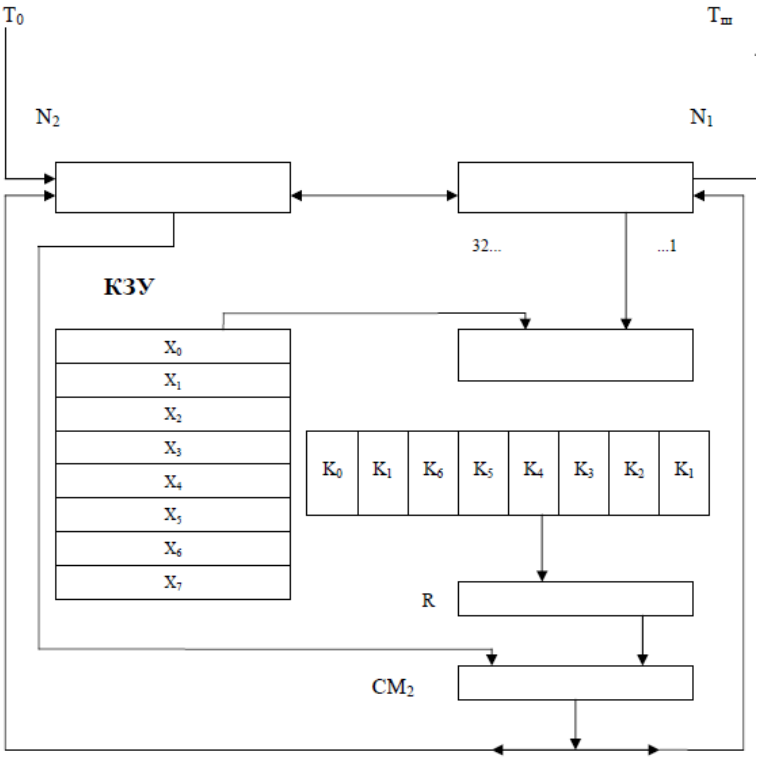
$$R(r32, r31, r30, r29, r28, r27, r26, r25, r24, r23, r22, r21, r20, \dots, r2, r1) = \\ = (r21, r20, \dots, r2, r1, r32, r31, r30, r29, r28, r27, r26, r25, r24, r23, r22).$$

Шифрланған деректердің 64 разрядты блогы $T_{\text{ш}}$ N_1 және N_2 дискілерінен

келесі ретпен шығарылады: N_1 дискінің 1, 2,..., 32 биттерінен, содан кейін 1, 2, ... , 32 биттерінен. дискінің N_1, яғни

$$T_{\text{ш}} = (\text{a}_1(32), \text{a}_2(32), \ldots, \text{a}_{32}(32), b_1(32), b_2(32), \ldots, b_{32}(32)).$$

Қарапайым ауыстыру режиміндегі ашық деректердің қалған блоктары дәл осылай шифрланады. Қарапайым кірістіру режиміндегі шифрлау алгоритмінің криптографиялық сұлбасы 2.7 – суретте көрсетілген.



2.7 – сурет. Қарапайым кірістіру режиміндегі шифрлау алгоритмінің криптографиялық сұлбасы

Қарапайым ауыстыру режимінде шифрланған деректерді дешифрлау

Қарапайым ауыстыру режимінде шифрды шешу алгоритмін жүзеге асыратын криптографиялық схема шифрлау сияқты пішінге ие (10 – суретті қараңыз). КСҚ шифрлау үшін пайдаланылатын бірдей кілттің 256 биттері енгізіледі. Шифры шешілетін шифрланған деректер әрқайсысы 64 биттен тұратын блоктарға бөлінген. Кез келген блокқа кіру

$$\text{T}_{\text{ш}} = (\text{a}_1(32), \text{a}_2(32), \ldots, \text{a}_{32}(32), \text{b}_1(32), \text{b}_2(32), \ldots, \text{b}_{32}(32))$$

N_1 және N_2 дискілері келесідей жүзеге асырылады:

N_1 және N_2 жетектерінде а $a_1(32)$ мәні N_1-нің бірінші разрядына, $a_2(32)$ мәні N_1-тің екінші битіне жазылатындай етіп шығарылады, $a_2(32)$ санының 32 разрядына жазылады;

$b_1(32)$ мәні N_2-нің бірінші цифрына енгізіледі, т.б., b32(32) мәні N_2-нің 32 цифрына жазылады.

Шифрлау X_0, X_1,..., X_7 дискілерін толтыру шифрлау циклдерінде КСҚ-

дан келесі ретпен оқылатын айырмашылығы бар ашық деректерді шифрлау сияқты алгоритм бойынша жүзеге асырылады:

$$\mathbf{X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7,}$$
$$\mathbf{X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0,}$$
$$\mathbf{X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0,}$$
$$X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0,$$

Қарапайым ауыстыру режиміндегі шифрды шешу алгоритмін келесі (2.18) формула түрінде жазуға болады:

$$a(32-j) = (a(32-j+1) * Xj-1)KR + b(32-j+1),$$
$$b(32-j) = a(32-j+1) \qquad (2.18)$$

$j = 1 \div 8$ кезінде;

$$a(32-j) = (a(32-j+1) * X_{(32-j)\,(mod\,8)})KR + b(32-j+1),$$
$$b(32-j) = a(32-j+1)$$

$j = 9 \div 31$ кезінде;

$$a(0) = a(1), b(0) = (a(1) * X_0)KR + b(1)$$

$j = 32$ кезінде.

N_1және N_2 жетектерін толтырудың 32 циклінен кейін алынған ашық деректер блогын құрайды

$$\mathrm{T_0} = (\mathrm{a_0}(32), \mathrm{a_0}(32), \ldots, \mathrm{a_0}(32), \mathrm{b_0}(32), \mathrm{b_0}(32), \ldots, \mathrm{b_0}(32))$$

шифрланған деректер блогына сәйкес келеді.

T_0 блогының $a_1(0)$ мәні N_1 бірінші разрядының мазмұнына, $a_2(0)$ мәні N_1 екінші разрядының мазмұнына сәйкес келеді және т.б., $a_{32}(0)$ мәні 32 N_1 разрядының мазмұнына сәйкес келеді.

Дәл осылай $b_1(0)$ мәні N_2 бірінші разрядының мазмұнына, $b_2(0)$ мәні N_2 екінші разрядының мазмұнына және т.б. мәніне сәйкес келеді. N_2 32 битінің мазмұны $b_{32}(0)$ сәйкес келеді. Шифрланған деректердің қалған блоктары дәл осылай кері шифрланады.

Келесіде 64 разрядты T_0 блогын қарапайым ауыстыру режиміндегі шифрлау алгоритмі *A* деп белгіленеді, яғни

$$A(T_0) = T_{\text{ш}}.$$

Тиісінше, шифрды шешу процесі A^{-1} деп белгіленеді және шифрланған блок үшін $T_{\text{ш}}$ кері түрлендіру орындалады:

$$A^{-1}(T_{\text{ш}}) = T_0.$$

Бұл шифрланған мәтінге A^{-1} алгоритмін қолдану бастапқы ашық мәтінді қайтарады дегенді білдіреді.

Қолданылған әдебиеттер тізімі

1. Гольдвассер С., Беллар М. Достижения в криптологии / Гольдвассер С. – М.: Триумф, 2016. – 513 с.

2. Шнайер, Брюс. Криптографическая методы защиты информации, 26-я ежегодная международная конференция по криптологии, Санта-Барбара, Калифорния, США, 20–24 августа 2022 г.

3. Фергюсон Н., Шнайер Б., Коно Т. Криптографическая инженерия: принципы проектирования и практическое применение. / Фергюсон Н. – М.: Пресс, 2022. – 416 с.