Лекция 5 ДЕРЕКТЕРДІ КРИПТОГРАФИЯЛЫҚ ТҮРЛЕНДІРУ ГОСТ 28147-89 АЛГОРИТМЫ

Негізгі мәліметтер

Ресейде жабық кілті бар блокты шифрлау алгоритмның стандарты ретінде 1989 жылы ГОСТ 28147-89 қабылданған болатын. Оның пайдалануы деректерді криптографиялық қорғау үшін ұсынылады. Шифр принциптері американдық DES-қа ұқсайды, бірақ оған қарағанда бағдарламалық жүзеге асурыға ыңғайлылау.

Американдық DES-қа қарағанда ГОСТ-ң кілті ұзынырақ - 256 бит. Одан басқа, ресей стандарты шифрлаудын 32 раундын пайдаланады, ал DES-та – тек 16 ғана.

Сонымен, деректерді криптографиялық түрлендіру ГОСТ 28147-89 алгоритмның негізгі параметрлері келесі: блок өлшемі 64 бит, кілт мөлшері - 256 бит, раундтар саны – 32.

Алгоритм классикалық Фейштель желісі болып табылады. Шифрланатын деректер блогы екі бірдей бөлшекке бөлінеді, оң жаққа R және сол жаққа L. Оң жағы раундтын қосалқы кілтімен қосылады және кейбір алгоритм бойынша сол жағын шифрлайды. Келесі раунд алдында сол жағы және оң жағы орындарын айырбастайды. Осындай құрылым блокты шифрлау үшін де дешифрлау үшін де бірдей алгоритмды пайдалануына мүмкіндік береді. Шифрлау алгоритмда келесі операциялар пайдаланылады:

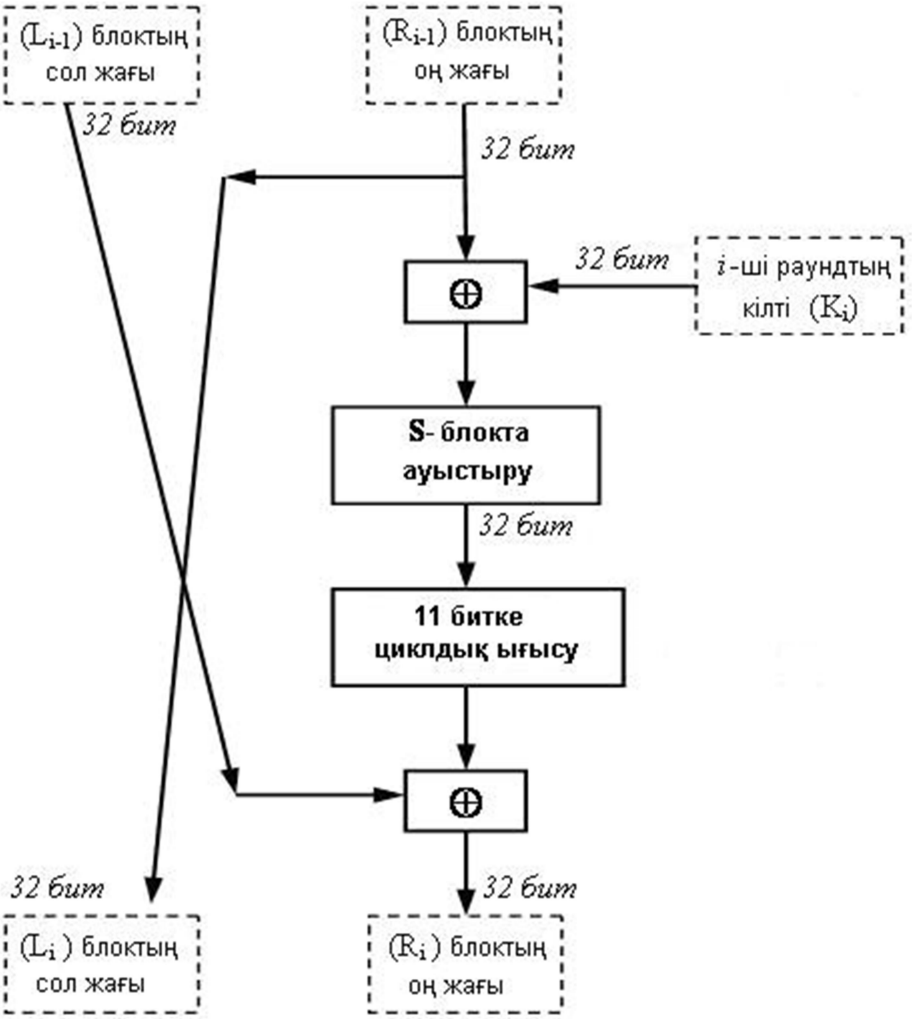
- модулі 2^{32} бойынша сөздерді қосу;
- сөзді көрсетілген бит санына солға қарай циклдық ығысу;
- модулі 2 бойынша бит бойы қосу;
- кесте арқылы ауыстыру.

ГОСТ алгоритмның түрлі қадамдарында деректер түсіндіріледі және әртүрлі пайдаланады. Кейбір жағдайда деректер элементы тәуелсіз биттер массивы ретінде өңделеді, басқа жағдайда – таңбасы жоқ бүтін сан ретінде, үшінші жағдайда – бірнеше қарапайым элементтен тұратын күрделі элемент ретінде өңделеді.

5.2 ГОСТ 28147-89 раундының құрылысы

ГОСТ 28147-89 бір раундының құрылысы 5.1 суретте көрсетілген.

Шифрланатын деректер блогы екі бөлшекке бөлінеді, олар кейін жеке 32-битты таңбасы жоқ бүтін сан ретінде өңделді. Алдымен блоктын оң жақ жартысы және раундтың қосалқы кілті модулі 2^{32} бойынша қосылады. Сосын блок бойы ауыстыру жүргізіледі. Алдынғы қадамда алынған 32-битты мән (оны S деп белгілейік) кодтың сегіз 4-битты блоктан тұратын массив ретінде түсіндіріледі: S=(S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7). Әрі қарай әрбір сегіз блоктын мәні жаңаға ауыстырылады, ол ауыстыру кестеден былай таңдап алынады: S_i блок мәні i-ші ауыстыру түйіндінің (яғни ауыстыру кестенің i-ші жолы) S_i ретті элементпен (нөмірлеу нөлден басталады) ауыстырылады. Басқа сөзбен айтқанда, блок мәні үшін ауыстыру ретінде жол нөмірі ауыстырылатын блок нөміріне тең, және баған нөмірі ауыстырылатын блок мәніне тең элемент таңдап алынады. Ауыстыру кестенің әрбір жолында 0 ден 15 дейін сандар ретсіз, қайталанбай жазылған (себебі төрт битта 0 ден 15 диапазондағы таңбасы жоқ бүтін сан жазулы мүмкін). Мысалы, S-блоктың бірінші жолында мұндай мән болу мүмкін: 5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11. Бұл жағдайда S_0 блогының (32-разрядты S санның төрт кіші биты) мәні нөмірі, ауыстырылатын блок мәніне тең, позицияда тұратын санға ауыстырылады. Егер S_0 = 0, онда 5 ауыстырылады, егер S_0 = 1, онда ол 8 ауыстырылады және т.б.


(Li-1) блоктың сол жағы
(Ri-1) блоктың оң жағы
32 бит
32 бит
32 бит
i-ші раундтың кілті (Ki)
⊕
S- блокта ауыстыру
32 бит
11 битке циклдық ығысу
⊕
32 бит
32 бит
(Li) блоктың сол жағы
(Ri) блоктың оң жағы

Сурет 5.1. ГОСТ 28147-89 бір раундының құрылысы

Ауыстыруды орындағаннан кейін барлық 4-битты блоктар қайтадан бірыңғай 32-битты сөзге бірлеседі, ол сосын 11 битке солға қарай циклдық ығысады. Ақырында, бит бойы «модулі 2 бойынша қосу» операция көмегімен нәтиже сол жақ жартысымен бірлеседі, осыдан жаңа оң жақ жартысы R_i табылады. Жаңа сол жағы L_i өзгертілетін блоктың кіші бөлігіне тең деп алынады: $L_i = R_{i-1}$.

Өзгертілетін блоктың алынған мәні шифрлау алгоритмның бір раундының орындау нәтижесі ретінде қарастырылады.

Шифрлау мен ашып оқу процедурасы

ГОСТ 28147-89 блокты шифр, сондықтан деректердің түрлендіруі базалық циклда блоктармен жүзеге асырылады. Базалық циклда деректер блогы үшін негізгі раунд бірнеше рет орындалады. Әрбір раундта сегіз мүмкін 32-разрядты қосалқы кілттердің біреуі пайдаланады.

Раундтардың қосалқы кілттерін жасау процесін қарап шығайық. ГОСТ-а бұл процедура өте қарапайым, әсіресе DES-пен салыстырғанда. 256-битты кілт K сегіз 32-битты қосалқы кілттерге K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7 бөлінеді. Алгоритмда 32 раунд бар, сондықтан әрбір қосалқы кілт шифрлау кезінде төрт раундта 5.1 кестеде көрсетілген ретімен пайдаланады.

Кесте 5.1. Шифрлау кезінде қосалқы кілттерді пайдалану реті

Раунд	1	2	3	4	5	6	7	8
Қосалқы кілт	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	9	10	11	12	13	14	15	16
Қосалқы кілт	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	17	18	19	20	21	22	23	24
Қосалқы кілт	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	25	26	27	28	29	30	31	32
Қосалқы кілт	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

Ашып оқу процесі шифрлаудағы алгоритмы бойынша жүргізіледі. Бір ғана айырмашылығы қосалқы кілттердің K_i пайдалану ретінде. Ашып оқуда қосалқы кілттер кері ретімен пайдалану керек, 5.2 кестеде көрсетілгендей.

Кесте 5.2. Ашып оқу кезінде қосалқы кілттерді пайдалану реті

Раунд	1	2	3	4	5	6	7	8
Қосалқы кілт	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Раунд	9	10	11	12	13	14	15	16
Қосалқы кілт	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

Раунд	17	18	19	20	21	22	23	24
Қосалқы кілт	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0
Раунд	25	26	27	28	29	30	31	32
Қосалқы кілт	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

5.3 Шифрлаудың негізгі тәртіптері

ГОСТ 28147-89 деректерді шифрлаудың келесі тәртіптері бар: қарапайым ауыстыру, гаммалау, кері байланысы бар гаммалау және бір қосымша тәртіп еліктеу ендірмені жасау.

Осы тәртіптердің қайсысында да деректер шифрланатын массив бөлінген 64 битты блоктармен өңделеді, дәл сондықтан ГОСТ 28147-89 блокты шифрларға жатады. Гаммалау тәртібінде толық емес (өлшемі 8 биттан кем) деректер блокты өңдеуге мүмкіндік бар.

Қарапайым ауыстыру тәртібі. Бұл блокты шифрды пайдалану тәртібі блок бойы қарапайым ауыстыру тәртібіне (ECB) ұқсас. Бұл тәртіпте бастапқы деректердің әрбір блогы бірдей шифрлау кілтті пайдаланып басқа блоктардан тәуелсіз шифрланады. Осы тәртіптің ерекшелігі - бастапқы мәтіннің бірдей блоктары бірдей шифрмәтінге түрлендіріледі. Сондықтан, қарапайым ауыстыру тәртібін ГОСТ 28147-89 тек кілттерді шифрлау үшін ұсынады.

Гаммалау және кері байланысы бар гаммалау тәртібі кез келген өлшемді деректерді шифрлау үшін пайдалануға болады.

Гаммалау тәртібінде бастапқы мәтіннің биттері модулі 2 бойынша гаммамен қосылады, гамма шифрлау ГОСТ 28147-89 алгоритмы көмегімен жасалынады. Яғни берілген тәртіпте шифрлау ГОСТ алгоритмы генератор ретінде 64-разрядты гамма блоктарын пайдаланады. Әрбір жаңа деректер блокты шифрлағанда, бұрыңғы қадамда пайдаланған гамма шифрланады және «жаңа» гамма ретінде пайдаланады. Ең бірінші гамманы алу үшін бастапқы деректер массивы ретінде *синхрожөнелту* деп аталатын 64-түрлі бастапқы деректер блогы пайдаланады (ол екі жақта да бірдей болу керек). Гамманың салу мен алуы бір модулі 2 бойынша қосу операция көмегімен орындалғандықтан, гаммалау тәртібінде шифрлау және дешифрлау алгоритмдер сәйкес келеді.

Нақты шифрлау массивтері үшін гамма элементтері әртүрлі болғандықтан, екі бірдей блоктын шифрлау нәтижесі де әртүрлі болады. Одан басқа, гамма элементтері бірдей 64 битты порциямен жасалынса да, осындай блоктың шифрланатын блок өлшеміне тең бір бөлігін де пайдалануға болады. Дәл осы толық емес деректер блокты шифрлауға мүмкіндік береді.

Кері байланысы бар гаммалау тәртібі гаммалау тәртібіне ұқсайды және тек гамма элементтерін жасау тәсілімен ғана ерекшеленеді. Кері байланысы бар гаммалауда кезекті 64-битты гамма элементі ГОСТ 28147-89 алгоритмдың базалық циклы бойынша бұрыңғы шифрланған деректер блокты түрлендіру нәтижесі ретінде жасалынады. Деректер массивының бірінші блогын шифрлау үшін гамма элементі синхрожөнелту циклы бойынша түрлендіру нәтижесі ретінде жасалынады. Осымен блоктар тіркелуіне жетеді – бұл тәртіпте әрбір шифрмәтін блогы ашық мәтіннің сәйкес және барлық бұрыңғы блоктарына тәуелді. Сондықтан, берілген тәртіпті кейде *блоктар тіркелуі бар гаммалау* деп атайды. Шифр беріктігіне блоктар тіркелуі ешқандай әсер етпейді.

Шифрланған деректер массивінде бұрмалауды табу үшін ГОСТ 28147-89-да криптографиялық түрлендірудің қосымша тәртібі бар – еліктеу ендірмені жасау. **Еліктеу ендірме** – бұл ашық деректерге және құпиялы кілттік ақпаратқа тәуелді бақылау

комбинациясы. Еліктеу ендірменің пайдалану мақсаты ақпарат масивінде барлық кездейсоқ немесе әдейі өзгертулерді табу. Еліктеу ендірмені жасау тәртібінде кіру мәтін блоктар арқылы келесі түрде өңделеді:

$$Y = f((X_{i-1}), K) 1\text{-ден } n\text{-ға дейін барлық } i \text{ үшін,}$$

мұндағы f - ГОСТ 28147-89 бойынша базалық цикл; X_{i-1} – бастапқы мәтіннің 64-разрядты блогы; K – кілт.

Еліктеу ендірме ретінде шығуда алынған Y_n блоктың бөлігі алынады, әдетте оның 32 кіші биты.

Сонымен, қаскүнем шифрлау кілтті білмей, берілген ашық ақпарат массивы үшін еліктеу ендірмені есептей алмайды, және берілген еліктеу ендірме үшін ашық деректерді таңдап алалмайды.

5.4 ГОСТ 28147-89 және DES шифрлау алгоритмдарының айырмашылығы

ГОСТ 28147-89 алгоритмның сенімділіг жеткілікті, себебі шифрлау кілттің ұзындығы үлкен.

Біз білеміз, шифрланған хабардың құпиялығы кілттің құпиялығымен анықталу керек. Яғни криптоталдаушыға шифрлау алгоритмы белгілі болса да, сәйкес кілті қолында болмағанда, хабарды ашып оқуға мүмкіндігі болмау керек. Барлық классикалық блокты шифрлар, сонын қатарында DES пен ГОСТ 28147-89, осы принципке сәйкес және оларды ашу үшін барлық кілттер кеңістігі (яғни барлық мүмкін кілт мәні) бойынша толық іріктеп алуды жүргізу керек. Әрине, осындай шифрлардың беріктігі пайдаланатын кілт өлшемімен анықталады.

ГОСТ 28147-89-да жүзеге асырылатын шифрда 256-битты кілт пайдаланады, және кілттер кеңістігінің көлемі 2^{256}. Егер шифрды бұзуға іріктеп алу мүмкіндігі 10^{12} (бұл жуық тең 2^{40}) кілттер бір секундта бар есептеуіш жүенің барлық қуштері жұмсалса, онда барлық 2^{256} кілттерді толық іріктеп алу үшін қажет болады 2^{216} секунд (бұл уақыт миллиард жылдан астам).

Айтылған айырмашылықтарға келесіні қосуға болады. DES-ң негізгі раундында бастапқы хабардың жүйесіз орын ауыстырулары қолданылады. ГОСТ 28147-89-да 11-битты солға қарай циклдық ығысу пайдаланады. Соңғы операция бағдарламалық жүзеге асыру үшін анағұрлым ыңғайлы. Бірақ, DES орын ауыстыру көшкін эффекті күшейтеді. ГОСТ 28147-89-да бір кіру биттын өзгеруі бір ауыстыру раундта бір 4-битты блокқа әсер етеді, ол сосын келесі раундтың екі 4-битты блогына, келесінің үш блогына әсерлеседі және т.б. ГОСТ 28147-89-да 8 раунд қажет, сосын ғана бір кіру биттын өзгеруі нәтиженің әрбір битіне әсер етеді; DES-та осы үшін тек 5 раунд қажет.

Және де айту керек, DES-қа қарағанда, ГОСТ 28147-89-де ауыстыру операцияны орындау үшін ауыстыру кестесін еркінше өзгертуге болады, яғни ауыстыру кестесі қосымша 512-битты кілт болып табылады.

Негізгі ұғымдар

ГОСТ 28147-89 – симметриялық шифрлаудың блокты алгоритмның ресей стандарты.

Сұрақтар

1. Деректердің криптографиялық түрлендіру ГОСТ 28147-89 алгоритмы қандай мақсат үшін пайдалану мүмкін?
2. Симметриялық шифрлаудың ГОСТ 28147-89 алгоритмнын негізгі параметрлерін айтып беріңіз.
3. Блокты шифрлау ГОСТ 28147-89 алгоритмда қандай операциялар пайдаланады?

4. Шифрлау ГОСТ 28147-89 алгоритмның DES алгоритмнан қандай негізгі айырмашылығы бар?

5. ГОСТ 28147-89 стандартты алгоритмды пайдаланғанда, құпиялы кілттен басқа қандай ақпарат хабарды ашып оқу үшін қажет?

6. Криптографиялық түрлендіру ГОСТ 28147-89 алгоритмы көмегімен қандай тәртіпте деректер шифрлауы орындалу мүмкін?

7. Еліктеу ендірме деген не? Қандай мақсат үшін еліктеу ендірме пайдалану мүмкін?