ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ФАРҒОНА ДАВЛАТ УНИВЕРСИТЕТИ

ФарДУ. ИЛМИЙ ХАБАРЛАР-

1995 йилдан нашр этилади
Йилда 4 марта чиқади

3-2015
сентябрь

НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 4 раза в год

МУНДАРИЖА

УДК: 004.056.5

ТАКОМИЛЛАШТИРИЛГАН DES ШИФРЛАШ АЛГОРИТМИНИНГ ФУНКЦИОНАЛ СХЕМАСИ ВА КРИПТОБАРДОШЛИЛИГИ

Ш.А.Умаров, С.Ю.Абдуллаев

Аннотация

Ушбу мақолада ахборот хавфсизлигининг криптоалгоритмлар йўналишидаги DES шифрлаш алгоритмининг Фейстель тармоғида такомиллаштириш, унинг функционал схемаси ва криптобардошлилигини баҳолаш тизими кўрсатиб ўтилган. Шунингдек, такомиллашган MDES–TDES шифрлаш алгоритмининг афзалликлари баён қилинган.

Аннотация

В данной статье рассмотрена разработка шифрующей криптоалгоритма DES в сети Фейстеля в направлении информационной безопасности, оценка функциональной схемы и криптоустойчивость. Показаны также преимущества разработанного шифрующего алгоритма MDES-TDES.

Annotation

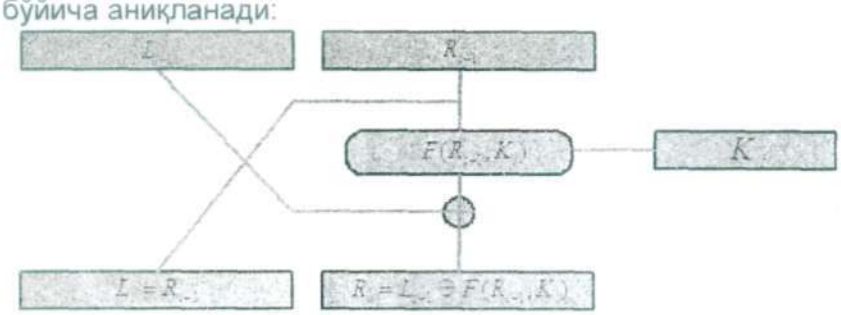
In this article the development of DES code algorithm in the direction of cryptoalgorithms of information security in the Factell network, its functional scheme and making system of cryptopatient are described. The advantages of the developed MDES-TDES code algorithm are also shown.

Таянч сўз ва иборалар: *криптоалгоритм, криптобардош, шифрлаш, дешифрлаш, калит, Фейстель тармоғи, раунд, акслантириш, алгоритм, DES алгоритми, симметрик, итерация.*

Ключевые слова и выражения: *криптоалгоритм, криптостойкость, шифровка, дешифровка, ключ, сеть Фейстеля, раунд, отражение, алгоритм, алгоритм DES, симметрия, итерация.*

Key words and expression: *criptoalgorithm, crypopatient, cipher, decipher, key, Factell network, reflection, algorithm, algorithm DES, iteration.*

Шифрланиши керак бўлган маълумот блокини силжитиш регистрларига киритиб (юклаб), регистрдаги маълумотни шартли равишда чап ва ўнг қисм блок векторларига бўлиб, улар устида ҳар хил калитлар билан бир хил турдаги акслантиришларни босқичма-босқич амалга оширишга асосланган – *Фейстель тармоғи* деб аталувчи шифрлаш жараёни функционал қурилмасига асосланган алгоритмлар кенг тарқалган. Симметрик калитли шифрлаш тизимларини тадқиқ қилиш олимлар жамоасини доктор Хорст Фейстель бошқарганлиги учун қурилмага унинг номи берилган. Фейстель тескариси мавжуд криптобардошли акслантиришларни тадқиқ қилмай, бундай акслантиришлар қатнашмаган криптобардошлилиги юқори бўлган шифрлаш тизимларини топиш масаласини ечимига киришди. У, бу масаланинг ечимини қуйидагича ҳал этди. Шифрланадиган блок иккита L_0, R_0 қисмларга ажратилади. Фейстель тармоғи $i-$раунди итератив блокли шифрлаш қуйидаги схема бўйича аниқланади:



Фейстель тармоғи $i-$ ***раунди.***

Ш.А.Умаров *– ТАТУ Фарғона филиали ахборот технологиялари кафедраси катта ўқитувчиси.*

С.Ю.Абдуллаев *– ТАТУ Фарғона филиали талабаси.*

Бу ерда $X_i = (L_{i-1}, R_{i-1})$ – i -раунд учун L_{i-1} ва R_{i-1} қисмларга ажратилган кирувчи маълумот, $Y_i = (L_i, R_i)$ эса X_i ни i – раунд калити K_i билан F акслантириш натижасида ҳосил бўлган шифр маълумот.

Фейстель тармоғи i – раундининг шифрлаш жараёни математик модели қуйидагича ифодаланади:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ)нинг Миллий Стандартлар Бюроси томонидан 1977 йилда эълон қилинган. DES алгоритмида: дастлабки 56 битли калитдан раунд калитларини ҳосил қилишнинг мураккаб эмаслиги, раунд асосий акслантиришларининг аппарат-техник ва дастурий таъминот кўринишларида қўлланилишини таъминлашнинг қулайлиги ҳамда улар криптографик хоссаларининг самарадорлиги – криптобардошлилигининг юқорилиги бу алгоритмнинг асосий хусусиятларини белгилайди.

Алгоритм акслантиришларини ёритиш учун қуйидаги белгилашлар киритилади:

L_i ва R_i –ҳар бири 32 битли блоклар бўлиб, Фейстель тармоғини чап ва ўнг қисмларини ифодалайди, $i = 0,1,...,16$;

$\oplus$ – битлар блоклари векторлари координаталарини $\mathrm{mod}\,2$ бўйича қўшиш;

K_i – 48 битли раунд калитлари;

F – Фейстель тармоғи асосий акслантиришлари функцияси;

IP – ўрин алмаштириш жадвали.

Навбатдаги T – блокни шифрлаш жараёни бу блок битларини қуйидаги бошланғич *IP* – ўрин алмаштириш жадвали:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

асосида акслантириш билан бошланади. T – блокнинг 58-бити 1-бит ўрнига, 50-бити 2-бит ўрнига ва ҳоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади. Сўнгра, олинган натижа иккита 32 битлик L_0 ва R_0 -қисмларга ажратилиб, 16 раундлик Фейстель тармоғи асосий акслантиришлари функцияси билан ҳар хил 48 битлик калитларда шифрланади. Яъни, раунд натижаси, $T_{i-1} = L_{i-1}R_{i-1}$ $(i-1)$ деб белгиланса, у ҳолда, юқорида таъкидланганидек, i - раунд натижаси қуйидаги тенгликлар:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad i = 1,2,...,16; \end{cases}$$

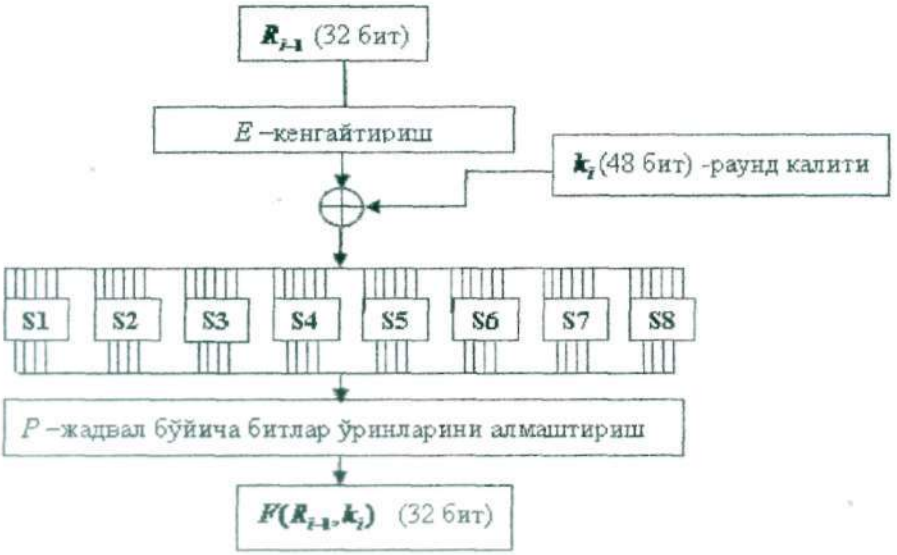
билан топилади. Бу ерда, $F(R_{i-1}, K_i)$ - 32 битли R_{i-1} ва 56 битли дастлабки калитни акслантириш натижасида олинган 48 битли K_i векторларнинг Фейстель тармоғи асосий акслантиришларининг функциясини ифодалайди. Охирги итерация-раунд натижаси $T_{16} = R_{16}L_{16}$ - блок бўлиб, бу блок битлари устида *IP* –жадвал бўйича IP^{-1} –тескари ўрин алмаштириш акслантириши бажарилади: T_{16}-блокнинг 1-бити 58-бит ўрнига, 2-бити 50-бит ўрнига ва ҳоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади.

Дешифрлашда шифрлаш жараёнида бажарилган акслантиришлар тескари тартибда бажарилади, бунда ушбу:

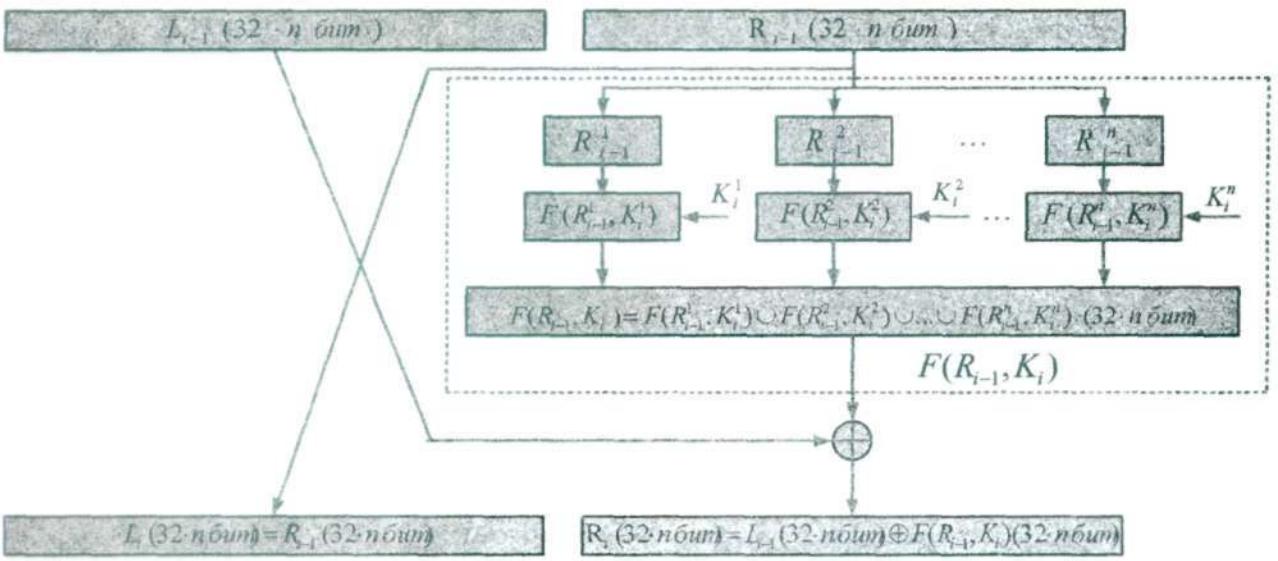
$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), \quad i = 16,15,...,1; \end{cases}$$

муносабатлардан фойдаланилиб, ҳар бири 32 битли бўлган L_{16} ва R_{16} шифр маълумот блокларини кетма-кет акслантириш, L_0 ва R_0 блоклар олиш, 64 битли L_0 R_0 блок устида IP^{-1} - акслантиришни бажариш орқали, T -очиқ маълумот блоки олинади.

DES алгоритми Фейстель тармоғи асосий акслантиришларининг $F(R_{i-1}, K_i)$ - функциясини ҳисоблаш схемаси қўйидагича:



DES шифрлаш алгоритмларини акслантириш асосларини сақлаб қолган ҳолда, K-калит узунликларини ошириш масаласи юқорида олинган илмий асосли натижаларга таяниб қуйидагича ечилади. Фейстель тармоғининг ушбу такомиллаштирилган:



Такомиллашган Фейстель тармоғи i – раунди.

умумий схемасида унинг - DES шифрлаш алгоритмининг базавий акслантиришларидан фойдаланиш кифоя, яъни:

1) шифрланиши керак бўлган очиқ маълумот блоклари узунлиги 64 m *бит*га тенг.
2) калит узунлиги $|K|\cdot n$ *бит*га тенг.
3) $K_i = K_i^1 K_i^2 ... K_i^n - i$-раунд қисм калитлари бирлашмаси.
4) фейстель тармоғи R – ўнг ва L – чап қисмлари узунликлари: $|L| = |R| = 32 \cdot n$ *бит*га тенг.
5) $L_{i-1}(32 \cdot n\ бит) - i$-раунд чап қисми.
6) $R_{i-1}(32 \cdot n\ бит) - i$-раунд ўнг қисми.
7) $L_{i-1}^1(32\ бит)$, $L_{i-1}^2(32\ бит)$,..., $L_{i-1}^n(32\ бит) - i$-раунд чап қисмнинг 32 *битлик;*
8) $R_{i-1}^1(32\ бит)$, $R_{i-1}^2(32\ бит)$,..., $R_{i-1}^n(32\ бит) - i$-раунд ўнг қисмнинг 32 *битлик;*
9) $DES(R_{i-1}^1, K_i^1)$, $DES(R_{i-1}^2, K_i^2)$,..., $DES(R_{i-1}^n, K_i^n) - i$-раунд DES алгоритми базавий акслантиришлари.

Такомиллашган DES, яъни **MDES - TDES** i – раунди математик модели қуйидагича ифодаланади:

$$\begin{cases} L_i(32 \cdot n\ бит) = R_{i-1}(32 \cdot n\ бит) \\ R_i(32 \cdot n\ бит) = L_{i-1}(32 \cdot n\ бит) \oplus DES(R_{i-1}, K_i)(32 \cdot n\ бит) \end{cases}$$

Такомиллаштириш параметри n га боғлиқ бўлган ҳолда бир нечта $DES(R_{i-1}^1, K_i^1)$, $DES(R_{i-1}^2, K_i^2)$,..., $DES(R_{i-1}^n, K_i^n)$ акслантиришларидан фойдаланилади. Бу эса n га боғлиқ ҳолда бир неча Фейстель тармоғига асосланган алгоритмлар функцияларидан ёки бир неча **S**-блоклардан фойдаланиш имконини беради. Шунингдек, n га боғлиқ равишда калит узунликлари ҳам ортиб боради, яъни $n = 1$ да калит узунлиги 256 бит бўлса, $n = 2$ да калит узунлиги 512 ва ҳоказо бўлади. Калит узунлиги ва такомиллаштириш параметри n орасида қуйидагича боғлиқлик ўрнатиш мумкин:

$$l_1 = l \cdot n$$

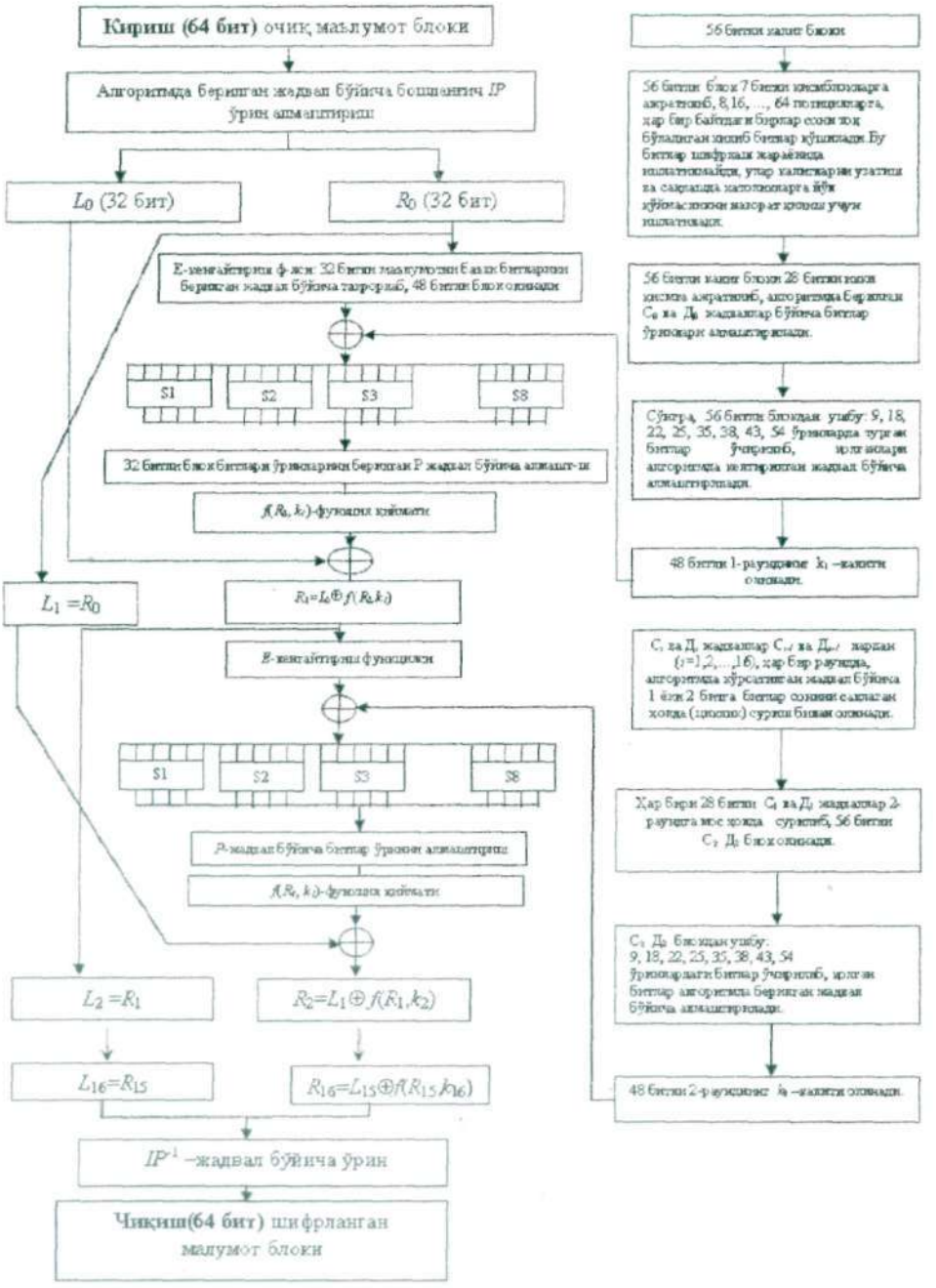
бу ерда l – асосий калити узунлиги, l_1 – такомиллашган калити узунлиги.

Такомиллашган **MDES - TDES** ва **DES** асосий алгоритмларнинг шифрлаш ва дешифрлаш тезлиги тенг, чунки $n = 1$ да алгоритм блок узунлиги 64 га тенг бўлиб, алгоритм тезлиги 20 тактдан иборат бўлса, $n = 2$ да такомиллашган алгоритм блок узунлиги 128 бит бўлиб, тезлиги 40 тактдан иборат бўлади.

Такомиллашган **MDES - TDES** шифрлаш алгоритмининг афзалликлари:

1) такомиллаштириш параметри n га боғлиқ ҳолда шифрлаш алгоритми хоссалари ва бардошлилигини сақлаб қолган ҳолда алгоритм калити узунлигини ошириб бориш имконияти мавжуд. Бу эса, ўз навбатида, ҳисоблаш техникаси қурилмаларининг такомиллашуви натижасида алгоритм калити узунлиги тўлиқ танлаш усулига бардошсиз бўлиб қолишининг олдини олади.

2) алгоритм тезлиги такомиллаштириш параметрига боғлиқ эмас, яъни такомиллашган **MDES - TDES** ва **DES** асосий алгоритм тезликлари тенг. Бу хосса, ўз навбатида, алгоритм тезлигини сақлаб қолган ҳолда такомиллаштириш имкониятини беради.



Адабиётлар:

1. Акбаров Д.Е., Мухтаров Ф. М., Сиддиқов А. Криптотаҳлил масалаларига тизимли ёндашув асослари ва уларни ечиш усуллари. – Фарғона. 2014. –143 б.

2. Умаров Ш., Абдуллаев С. Фейстель тармоқли симметрик блоклаб шифрлаш алгоритмларини такомилаштириш. "ФарДУ. Илмий хабарлар – Научный вестник. ФерГУ", 2014. 2-сон. 10-13 бет.

3. Акбаров Д.Е., Собиров Ш.О. Маълумотларни шифрлашнинг симметрик калитли алгоритмини яратиш // ФарПИ Илмий-техника журнали. 2009. 2-сон. 3-6 бет.

(Тақризчи: Ф.Ю.Полвонов, техника фанлари номзоди, доцент).