RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI
2025
№2
aprel-iyun
http://dgeconomy.tsue.uz/
ILMIY ELEKTRON JURNAL

ПОВЫШЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ БАНКОВСКИХ СИСТЕМ НА ОСНОВЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТРАНЗАКЦИЙ В ФИНАНСОВЫХ ИНФОРМАЦИОННЫХ СЕТЯХ НА БАЗЕ СОВРЕМЕННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ

Рахимбердиев Кувончбек Бахтиёрович
Ташкентский государственный экономический университет, Старший преподаватель кафедры эконометрики
qquuvvoonn94@gmail.com

Аннотация
В настоящее время в финансовых информационных системах стремительно развиваются процессы обмена информацией. Основной причиной развития этого процесса является применение информационных и современных цифровых технологий к финансовым системам. В результате создание систем электронных платежей, дистанционного банковского обслуживания, систем электронных денег, криптовалют и других финансовых технологий приводит к тому, что объем финансовых транзакций увеличивается с каждым днем. Также представлен процесс моделирования эффективного генератора ключей для алгоритмов симметричного блочного шифрования, таких как AES, DES, Кузнечик.

Ключевые слова
Асимметричные криптосистемы, финансовая криптография, технологии блокчейн, DES, криптографические протоколы, электронная коммерция, электронная торговля, электронные деньги, AES, Кузнечик.

Введение

В настоящее время развитие процессов обмена информацией, использование современных технологий, таких как искусственный интеллект, Интернет вещей и блокчейн, в совершенствовании экономической и социальной сферы приносят человечеству множество удобств.Эти глобальные информационные и трансформационные процессы не обошли и нашу страну. В настоящее время в Республике Узбекистан высокие результаты современной науки и информационных технологий стремительно применяются в социально-экономической, банковско-финансовой, здравоохранении, производстве и во всех других сферах.Также в результате совершенствования систем электронного правительства, процессов цифровизации и трансформации показатели цифровой экономики в Республике Узбекистан значительно увеличиваются, что положительно влияет на показатели валового внутреннего продукта Узбекистана. [1,9]. На современном этапе развития информационных

технологий становится очевидным, что для развития надежных банковских продуктов и услуг необходимо обеспечить адекватный уровень информационной безопасности. Развитие глобального экономического пространства расширяет возможности банковской деятельности.

Как уже говорилось выше, в ее основе лежит структура политики информационной безопасности в Республике Узбекистан. Кроме того, для обеспечения информационной безопасности в банках и финансовых организациях могут использоваться национальные стандарты или современные криптографические алгоритмы. Видно, что алгоритмы национального стандарта Республики Узбекистан O'zDSt 1047:2003, O'zDSt 2927:2015, O'zDSt ISO/IEC 27000:2014 основаны на алгебре параметров и имеют очень высокая криптостойкость.

Однако в большинстве случаев эти алгоритмы используются в электронно-цифровых подписях и шифровании информации. При этом мы можем использовать современные симметричные криптографические алгоритмы с высокой эффективностью шифрования и дешифрования. В настоящее время примерами современных симметричных криптографических алгоритмов являются AES и DES.

Обзор литературы

Вопрос обеспечения информационной безопасности в банковских системах интересует не только банковские и кредитные организации, но и математиков и криптографов. Во всем мире проводятся интенсивные научные исследования по применению современных информационных технологий в банковских системах и обеспечению информационной безопасности. В частности, в научных работах А. Л. Белоусова исследованы вопросы применения современных информационных технологий в банковских системах, а также дан ряд рекомендаций по формированию информационной архитектуры кредитных систем. Сургуладзе В.Ш., Пчелин А.А. и Кулик Т., Ларсен П.Г. научные работы включают защиту информации и разработку политики информационной безопасности, концептуальное обоснование информационной безопасности в кредитных организациях и анализ криптографических алгоритмов, необходимых для решения задач кибербезопасности.

Методология исследования

В данном научном исследовании основным методическим направлением была выбрана оценка эффективности современных симметричных криптосистем, обеспечивающих безопасное выполнение транзакций в банковской и финансовой системе, их совершенствование и экономическое обоснование. В конце исследования было научно обосновано, что криптостойкость и быстродействие алгоритмов DES и AES могут быть повышены за счет использования новых математических функций и усовершенствованных блочных структур. Это послужит усилению цифровой безопасности в банковской и финансовой системах и обеспечению экономической эффективности.

Анализ и результаты

Во-первых, следует проанализировать криптографические методы, используемые для обеспечения информационной безопасности. Дан общий анализ вопросов криптографии и криптоанализа. Алгоритмы шифрования состоят из криптоалгоритмов асимметричного шифрования на основе секретных параметров (симметричный ключ и определяемый протоколом приложения) и асимметричных криптоалгоритмов шифрования на основе открытых параметров.

Алгоритмы симметричного блочного шифрования на основе сети Фейстеля и их усовершенствование. Приложения сети Фейстеля можно найти во многих симметричных блочных шифрах. Примеры этих криптоалгоритмов включают FEAL, LOCI, Khufu, Khafre Blowfish, Lucifer, CAST, а также стандартные алгоритмы, такие как DES, GOST 28147-89 [9,10]. Идея сети Фейстеля выражается следующим образом. Зашифрованный блок разделен на две части. Перестановка итеративного блочного шифра сети Фейстеля определяется по следующей схеме:

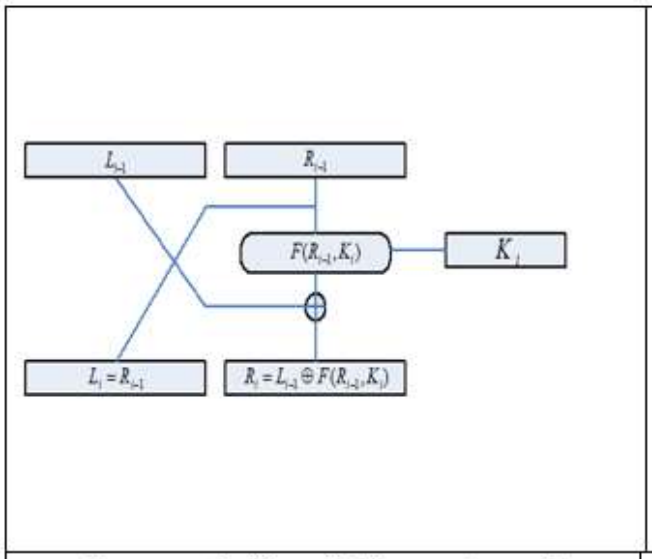

Рисунок 3. Сеть Фейстеля i-round

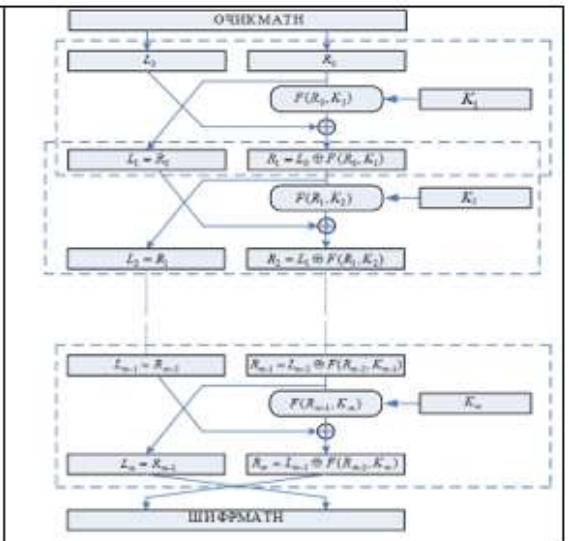

Рисунок 5. Сеть Фейстеля длиной

Здесь $X_i=\left(L_{i-1},R_{i-1}\right)-i$ — это разделенные на L_{i-1}Li и R_{i-1} входящие данные для i-раунда, а $Y_i=\left(L_i,R_i\right)$ — зашифрованный текст, полученный в результате зеркального отображения X_i с помощью ключей $i-$ раунда K_i и F. Математическая модель $i-$ раунда сети Фейстеля выражается следующим образом:

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

Алгоритмы, основанные на сети Фейстеля, состоят из функции, зашифрованной K ключами и состоящей из нескольких итераций. Зашифрованный текст в каждом раунде $i-$ это входящие (открытые) данные для раунда $i+1-$, или зашифрованный текст в раунде i-это зашифрованный текст для раунда $i-1$. K раундовых ключей генерируются из исходного ключа

по правилу, заданному в алгоритме.Основное свойство отражений сети Фейстеля состоит в том, что даже если функция F -раунда необратима, сеть Фейстеля возвращает эти отражения. Действительно, в круглой математической модели $i-$, представленной в выражении (4.1), используя свойство операции сложения в $\oplus$ – двоичная система счисления, можно получить следующее равенство:

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

Эта последняя система равенств представляет собой математическую модель дешифрования алгоритмов шифрования, построенную на основе сети Фейстеля. В общем случае функциональная схема m-раундовой сети Фейстеля выражается следующим образом:

В алгоритмах шифрования на основе сети Фейстеля для шифрования и дешифрования используется один и тот же алгоритм, только использование раундовых ключей обратное, то есть при дешифровании в 1-м раунде используется K_m, во 2-м раунде K_{m-1}. и K_1 в последнем раунде. Даже если функция F односторонняя, расшифровка возвращает эту функцию [6].

Обеспечение безопасности банковских и финансовых операций с использованием алгоритма симметричного шифрования DES. Стандартный алгоритм шифрования DES был опубликован Национальным бюро стандартов США (США) в 1977 году. В 1980 году Национальный институт стандартов и технологий США принял этот алгоритм в качестве стандарта для использования в качестве алгоритма шифрования для защиты не- конфиденциальная, но важная информация в сфере государственного и коммерческого финансирования от посторонних физических и юридических лиц [1]. В алгоритме DES: простота генерации раундовых ключей из исходного 56-битного ключа, простота обеспечения использования отражений раундовых ключей в аппаратно-техническом и программном аспектах, а также эффективность их криптографических свойств - высокая криптостойкость, определить основные характеристики этого алгоритма. Процесс шифрования состоит из перестановки 64-битных блоков открытых данных в соответствии с IP-таблицей, заданной в алгоритме, 16-кратного шифрования с 48-битными круглыми ключами и отражений ключей, генерируемых с использованием циклического сдвига и некоторых отражений с потерей битов, путем замены бит исходного 56-битного ключа по таблицам, приведенным в алгоритме. Заключается в перестановке битов блока результата шифрования согласно заданной таблице IP^{-1}. Для пояснения отражений алгоритма введены следующие аннотации:

L_i и R_i представляют собой 32-битные блоки каждый, представляющие левую и правую части сети Фейстеля, т.е.;

$\oplus$-сложение векторов битовых блоков по координатам;

K_i-48-битные круглые ключи;

F -функция основных отражений сети Фейстеля;

IP - сменный стол.

Следующий процесс шифрования Т-блока представляет собой следующий начальный IP ─ таблицу перестановки битов блока:

Таблица1. Первичный IP─таблица коммутации

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

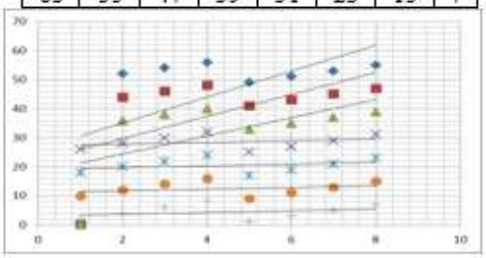

Рисунок 8. Исходный IP ─ таблица перестановок распределения чисел

Таблица 2. Повторение битов 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29 и 32 дважды

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

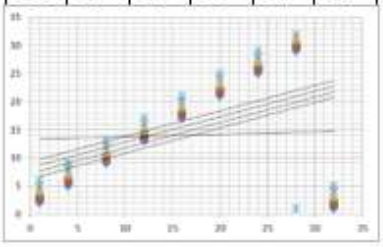

Рисунок 9. Распределение повторяющихся битов

То есть, если результат раунда определен как Т2, то, как отмечалось выше, результатом -раунда являются следующие равенства: начинается с зеркалирования на основе 58-го бита Т-блока вместо 1-го бита, 50-го бита вместо 2-го бита и т. д., а остальные биты переносятся на места, указанные в таблице. Затем полученный результат делится на две 32-битные части L_0 и R_0 и шифруется разными 48-битными ключами с помощью 16-раундовой функции отражения сетевого ключа Фейстеля[18,19]. То есть, если результат раунда определен как $T_{i-1} = L_{i-1}R_{i-1}(i-1)$, то, как отмечалось выше, результатом -раунда являются следующие равенства:

Его можно найти с помощью,

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad i = 1,2,...,16; \end{cases} \tag{4}$$

Здесь $F(R_{i-1}, K_i)$ представляет собой функцию сопоставления ключей Фейтеля для 48-битных векторов K_i , полученных путем сопоставления 32-битного R_{i-1} и 56-битного начального ключа. Результатом последней итерации-раунда является $T_{16} = R_{16}L_{16}$ -блок, по битам этого блока производится IP-1-обратная перестановка согласно IP-таблице: бит 1 блока T_{16} заменяется битом 58, бит 2 заменяется битом 50 и так далее. также переносятся в места, указанные в таблице.

При расшифровке отражения, выполняемые при шифровании, выполняются в обратном порядке, где:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), \quad i = 16,15,...,1; \end{cases} \tag{5}$$

отношений, каждый из которых составляет 32 бита, и путем последовательного зеркалирования блоков зашифрованного текста, получения блоков L_0 и R_0, выполнения IP-1 - зеркалирования на 64-битном блоке $L_0 R_0$, получается Т-открытый блок данных. Алгоритм DES по схеме расчета $F(R_{i-1}, K_i)$ -функции основных отражений сети Фейстеля:

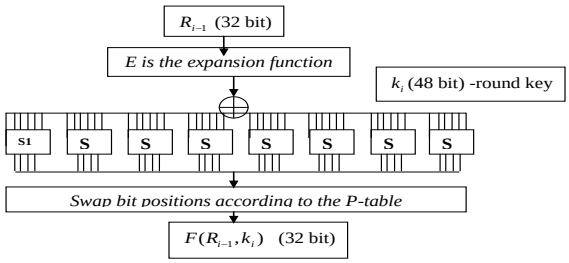

Рис. 10. Схема расчета $F(R_{i-1}, K_i)$ -функции основных отражений сети Фейстеля

$E(R_{i-1})$

$E(R_{i-1})$-функция расширения R_{i-1} - повторяющийся 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29 и 32 бита 32-битного блока дважды и следующая таблица (Таблица 2 и Рисунок 9). Каждый бит 48-битного Е-блока, полученного в результате компоновки по таблице 2, добавляется к соответствующим битам К-48-битного раундового ключа путем $\oplus$ -исключающее ИЛИ (по моду2) операции, а результат выражается в виде восьми шестибитных блоков $B_1,\ldots, B_8$, : $E(R_{i-1}) \oplus k_i = B_1\, B_2 \ldots B_8$.Затем каждый B_j -шестибитный блок ускоряется S -блоком с соответствующей таблицей S_j -блока и заменяется четырехбитным блоком. S_j -блоки состоят из восьми неизменяемых таблиц размером 4x16.

Алгоритм шифрования Des может выполнять шифрование быстрее, чем асимметричные криптосистемы. Таким образом, с помощью этого алгоритма банковские и финансовые транзакции можно отправлять по защищенным и открытым каналам связи. Результаты шифрования банковских и финансовых транзакций в алгоритме шифрования DES представлены в таблице 4.

Таблица 4. Процесс и сроки шифрования финансовых транзакций с использованием алгоритма DES

	KEY	ECB	CBC	CTR	OFB	CFB	Время шифровать финансовые транзакции
Transaction 1 (1,2kb)	34 35 34 35 34 38	KisO7qdHsf 0EG8mVcC W33A==	CX0GUi OWxgi6 gr77koK uKg==	Hd0Ocg nl614GR 6DGOitf XA==	Hd0Ocg 55QKie 2nIbIp+ e9w==	Hd0Ocr sa4DZZ gDPUp neOEw ==	4,97142s
Transaction 2 (1,5 kb)	3435 3435 3438	baWb0n2c3j TTbgiNg2Bf Dw==	gw9fdQ0 dgPsnU8 fa/Et7Y w==	Hd0Ocg Dl41kG Ua/GOSt fXA==	Hd0Ocg d5SK+e zH0bIZ +e9w==	Hd0Ocr Ia6DFS K/PrI+ X1CQ= =	6,21425s
Transaction 3 (1,8 kb)	3435 3435 3438	aLh4Dk1VF n3q03zQ1Bo QWQ==	2BDQ3X yzcpG3Z qmlJEsU mg==	Hd0Ocg Dl41kG Ua/GOSt fXA==	Hd0Ocg Dl41kG Ua/GOS tfXA==	Hd0Ocr Ia6DFS K/PrI+ X1CQ= =	7,45718s

Таблица 5. Стандартное время шифрования и размер данных для алгоритма шифрования DES

Криптографические алгоритмы		Размер ключа (биты)	Поколение Время (миллисекунды)
Symmetric	DES	56	29

Таблица 6. Анализ алгоритмов AES и DES с точки зрения времени шифрования и размера

Криптографические алгоритмы		Размер ключа (биты)	Поколение Время (миллисекунды)
Симметричный	DES	56	29
	AES	128	75

В следующей таблице, исходя из основных характеристик симметричных криптосистем, мы представляем следующий результат (табл. 7).

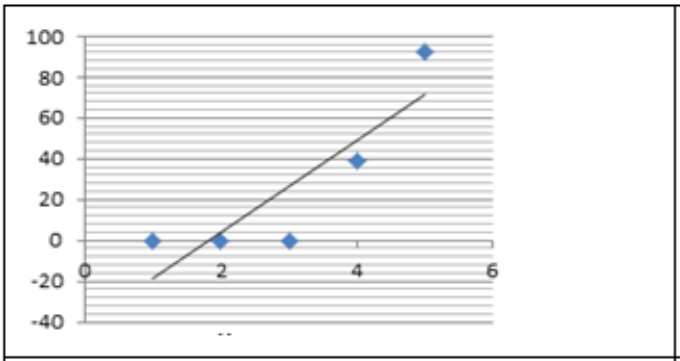

Рисунок 16. Банковские и финансовые операции Время расшифровки (в секундах)

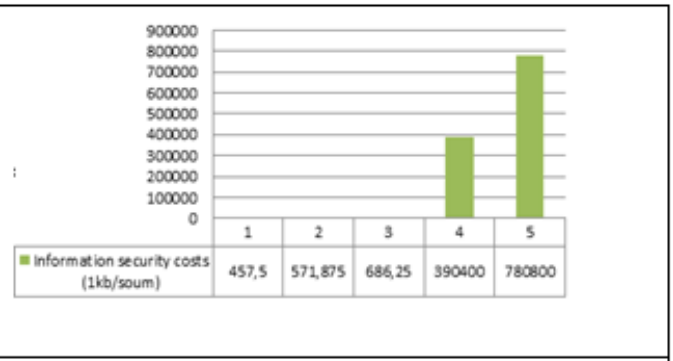

Рисунок 17. Затраты на информационную безопасность (1кб/сум)

В таблице 7 представлены характеристики защиты банковской и финансовой информации с использованием современных алгоритмов симметричного шифрования. Согласно этим показателям время шифрования транзакций размером 1,2, 1,5, 1,8, 1024 и 2048 Кб составляет 0,010125, 0,038906, 0,066937, 46,08 и 106,88 секунды. Кроме того, в процессе расшифровки эти зашифрованные транзакции занимают 0,0165, 0,03046875, 0,047825, 39,36 и 92,8 секунды соответственно. Мы можем заметить, что эти индикаторы менее эффективны, чем криптосистема AES. Однако повысить эффективность алгоритма Деса можно за счет оптимизации и создания быстровычислимых функций для S-блоков.

Заключение

В настоящее время вопросы обеспечения информационной безопасности в банковских и финансовых организациях считаются одними из актуальных. Также, согласно отчетам Центра обеспечения информационной безопасности Республики Узбекистан, количество возможных угроз информации в нашей стране увеличивается. Поэтому актуален вопрос исследования и внедрения эффективных криптосистем. Системы защиты информации банкоматов и

мобильных устройств связи, используемых при банковских и финансовых транзакциях, основаны на симметричных криптосистемах. Поэтому необходимо исследовать и совершенствовать такие криптосистемы, как DES и AES. Согласно полученным в данной статье научным результатам, оптимизация криптосистем DES и AES и использование новых логических функций для блоков C позволяет увеличить скорость шифрования и дешифрования и сократить время. Также стоимость защиты 1 кб информации может составить 457,5 сумов. Кроме того, усовершенствование этих систем может повысить криптостойкость алгоритма и привести к существенному снижению затрат на обеспечение информационной безопасности и повышению экономической эффективности на 10-12%.

Литература

1. Белоусов А. Л. Некоторые аспекты внедрения информационных технологий в финансовую сферу // Инновационное развитие экономики. Будущее России: материалы и доклады V Всероссийской (национальной) научно-практич. конференции. 2018. С. 7-12.
2. Сургуладзе В. Ш. Информационная политика Российской Федерации: доктрина информационной безопасности в системе целеполагающих документов государственного стратегического планирования // Власть. 2017. Т. 25, 2. С. 75-77.
3. Пчелин А. А. О рисках информационной безопасности кредитной организации // Горный информационно-аналитический вестник (научно-технический журнал). 2015. № 2. С. 320-328.
4. Кулик Т., Ларсен П. Г. К формальной верификации стандартов кибербезопасности//Труды Института системного программирования РАН. 2018. Т. 30. № 4. С. 79-94.
5. Г. Джураев и К. Рахимбердиев, Математическое моделирование системы кредитного скоринга на основе задачи Монжа-Канторовича, IEEE Международная конференция по Интернету вещей, электронике и мехатронике 2022, Труды IEMTRONICS 2022.
6. Г. Джураев и К. Рахимбердиев, Моделирование процесса принятия решений кредиторами на основе технологии блокчейн, Международная конференция по информационным наукам и коммуникационным технологиям: приложения, тенденции и возможности, ICISCT 2021, стр. 1-5.