ISSN 2181-7200

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ФАРҒОНА ПОЛИТЕХНИКА ИНСТИТУТИ

ИЛМИЙ–ТЕХНИКА ЖУРНАЛИ

2018 (спец. вып. 1)

НАУЧНО–ТЕХНИЧЕСКИЙ ЖУРНАЛ ФерПИ

SCIENTIFIC –TECHNICAL JOURNAL of FerPI

ФАРҒОНА – 2018

ФУНДАМЕНТАЛЬНЫЕ НАУКИ

ФУНДАМЕНТАЛ ФАНЛАР

МЕХАНИКА

ҚУРИЛИШ

ЭНЕРГЕТИКА, ЭЛЕКТРОТЕХНИКА, ЭЛЕКТРОН ҚУРИЛМАЛАР ВА АХБОРОТ ТЕХНОЛОГИЯЛАР

КИМЁВИЙ ТЕХНОЛОГИЯ ВА ЭКОЛОГИЯ

ИЖТИМОИЙ-ИҚТИСОДИЙ ФАНЛАР

ҚИСҚА ХАБАРЛАР

Таҳририят манзили:
150107. Фарғона шаҳри, Фарғона кўчаси, 86 уй.
Телефон: 241-13-54.
Факс: 241-12-06.
Бизнинг сайт: http://www.ferpi.uz
E-mail: jurnalferpi@mail.ru

Ўзбекистон республикаси матбуот ва ахборот агентлиги
Фарғона вилояти матбуот ва ахборот бошқармаси
томонидан 2007 йил 22 февралда № 12-064
рақами билан рўйхатга олинган

Босишга рухсат этилди: 15.10.2018 й.
Бичими: А4. Гарнитура Times New Roman.
Босма табоғи:15,25. Адади 20 нусха. Буюртма № 3.
Баҳоси шартнома асосида.
«Dadaxon Nur Print» МЧЖ босмахонасида чоп этилди.
Фарғона шаҳар Б. Марғилоний кўчаси 62-уй.
Лиц: №22-2891 21.11.2012 йил.

УДК 621.396.99

Технологик жараёнларни масофада жойлашган микропроцессорли модулларда қурилган автоматик бошқариш тизимлари.

Автоматизированная система управления технологическим процессам построенная на удаленных микропроцессорных модулях.

Automated control system for technological processes built on remote microprocessor modules.

Абдурахмонов Султонали Мукарамович – к.ф.м.н., доцент, заведующий кафедры информационно-образовательной технологии Ферганского филиала ТУИТ имени Мухаммада ал-Хоразимий, sulton59_15@inbox.ru;

Аннотация

Мақолада информацияларни аралаш турдаги қабул қилиш ва узатиш тизимлари асосида қурилган технологик жараёнларни бошқариш масаласи кўриб чиқилган. Аналог, дискрет сигналларни киритиб чиқариш микропроцессорли модуллари асосида автоматик бошқариш тизимларини қуриш технологияси келтирилган. Автоматлаштириш учун мисол сифатида нефткимё сохасида кенг қўлланиладиган градир қурилмалари иш жараёни олинган.

Таянч иброалар: автоматлаштириш, масофада , модуль, радио модем, интерфейс, градир қурилмаси, ўзгартиргич.

Аннотация

В работе рассматриваются вопросы автоматизации технологических процессов с смешанной системой приема-передачи информации. Приводится техология построения системы автоматизации с использованием удаленных микропроцессорных модулей ввода-вывода аналоговых и дискретных сигналов. Как пример для автоматизации используется технологический процесс работы градирен в промышленности нефтихимии.

Ключевые слова: автоматизация, удаленные, модуль, радио модем, интерфейс, градирни, преобразователь.

Annotation

The paper deals with the issues of automation of technological processes with a mixed system of reception of information transfer. The technology of constructing an automation system using remote microprocessor input-output modules of analog and discrete signals is given. As an example for automation, the technological process of operation of the cooling in the petrochemical industry.

Keywords: automation, remote, module, radio modem, interface, cooling towers, converter.

В современных производственных циклах, как один из основных части управления технологическим процессам, являются информационные коммуникационные системы передачи и приема информации между блоками АСУ ТП (автоматизированная система управления технологическими процессами) с учетом сложности, цикличности и интенсивности прохождения процессов[1]. Основные узлы управления, прием – передача информации в этих циклах осуществляется по специальным каналам данных, имеющих различных форматов и кодировки. Различные АСУ ТП со сложными структурами разработаны и внедрены во многих отраслях промышленности. Но каждый проект имеет свои специфику по организации системы управления и мониторинга[2]. В каждой из этих систем применяются различные методы управления процессами. В основном, выбор метода зависит от многих параметров технологии и подобранного оборудования для автоматизации процесса. В нефтехимических производствах так же разработаны и внедрены многочисленные проекты АСУ ТП со своей спецификой. Эти проекты направлены на повышение эффективности производства и улучшение качество выпускаемые продукции. В этих системах в основном решены технические задачи, относящие к производству. Но разработанные системы не являются универсальными, они решают определенные технологические задачи. Перед нами стояла задачи разработки универсальные системы управления технологическим процессам применяемые в отрасли нефтехимии.

В данной работе объектом исследования является системы охлаждения технологических оборудования по переработки нефти. Результатом исследования, это готовый универсальный проект АСУ ТП построенный на современных микропроцессорных модулях управления. Кроме того проведен анализ и оценка системы приема-передачи информации в системах реального времени.

Объектом управления АСУ ТП проекта, работа охладителей вторичных водных ресурсов (градирен, Ферганского нефтеперерабатывающего завода, расположенных на значительных расстояниях друг о друга) составляли единые системы с обратной связи. Градирни используют вторичные горячие воды полученные от системы охлаждения блоков установок обработки нефти. Их функцией является прием вторичной воды, охлаждения до требуемой температуры и откачка в систему охлаждения установок.

Работа любой градирни основана на охлаждении некоторого объема воды атмосферным воздухом. Испарительная градирня открытого типа работает по принципу разбрызгивания горячей воды и смешивания ее с более холодным наружным воздухом. При этом часть воды превращается в пар и вместе с нагревшимся наружным воздухом выбрасывается в атмосферу, оставшаяся же вода охлаждается[3]. В этом цикле управления процессом является только запуском и остановом определенного количество воздушных вентиляторов в градирнях. Зависимо температуры вторичных воды увеличивается или уменьшается количество включенных вентиляторов. До внедрения разработанной системы управления запуск и останов осуществлялся в ручном режиме, что не обеспечивал экономия энергии. Поскольку количество включаемых вентиляторов определялись по опыту, не имели прямые связи с измеряемой температурой вторичных воды.

В технологических циклах участвовали много технические оборудования и устройств таких как: электронасосы, регулирующие клапаны, температурные датчики, датчики давления, уровнемеры. Эти оборудования не имели системы связи с современным оборудованиям управления. Поэтому нами приведены замены или модернизации существующих оборудования и устройств, которые обеспечивали объединение в единую систему управления на современных микропроцессорных модулях.

Для мониторинга, контроля и управления системы управления градирнями нами использованы следующие технологические параметры:

- температуры воды;

- давления воды в коллекторах насосов;

- уровня воды в бассейнах;

- расход оборотной воды в системе;

- расход пропиточной воды в систему;

- токовые нагрузки в насосах и вентиляторах;

- стоп/пуск насосов;

- стоп вентиляторов;

- положение задвижек в трубопроводах.

Были подобраны следующие приборы и удаленные микропроцессорные модули для построения автоматизированной системы:

- преобразователь тока Е-842/1 (5а – 5ма);

- 8-ми канальный модуль аналогового ввода МВА8 ;

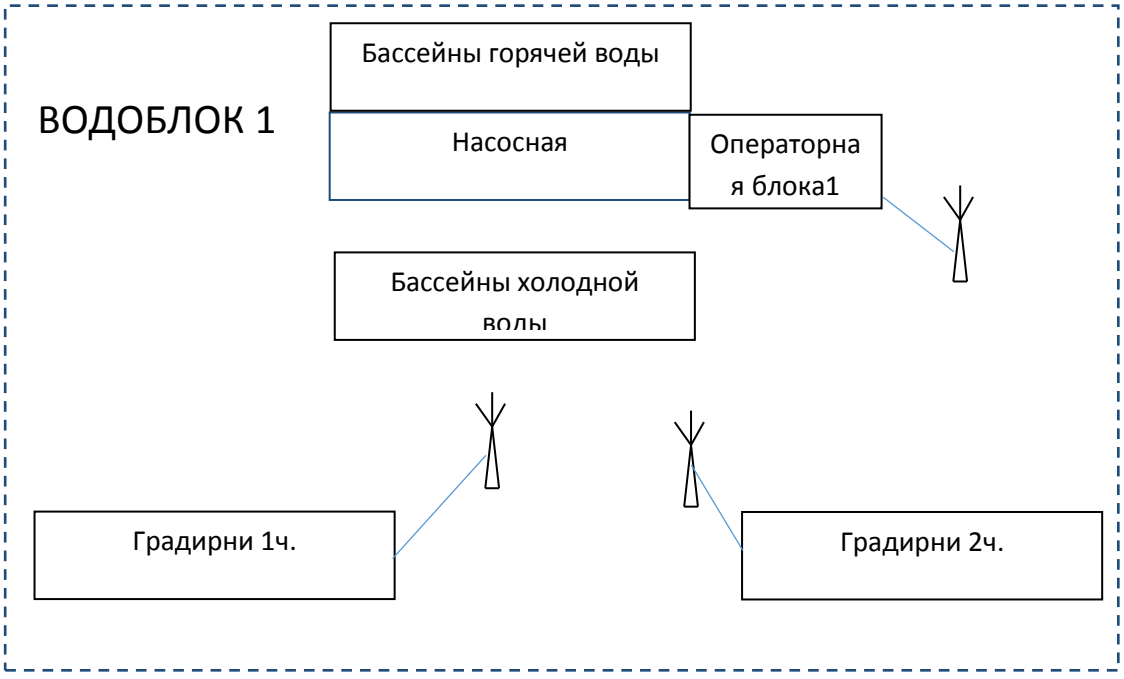
- 8-и канальный модуль дискретного вывода МВУ8 ;

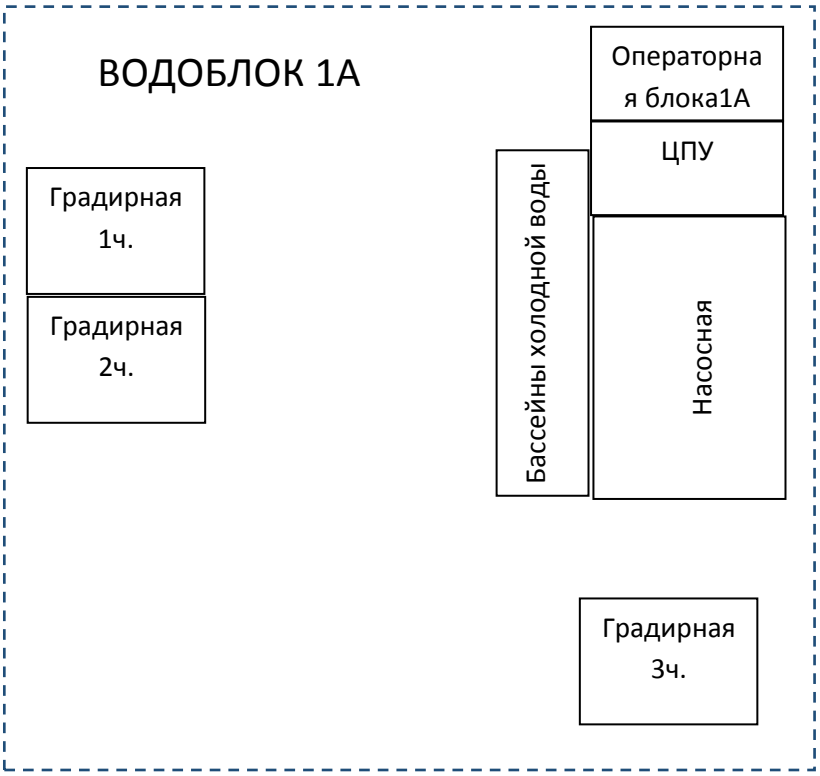
- 4-х канальный промышленный блок питания БП -14-4.24В;

- преобразователь давления КРТ;

- радиомодем Невод 5 .

Схема расположение узлов АСУТП и расположение антенн радиомодемов Невод 5 для передачи информации по радиоканалу имеет следующий вид:





Оборудование системы автоматизации установлены в узлах в специальных шкафах. Информационные кабели (витая пара) приложены по кабельным лоткам с учетом защиты от внешние воздействие.

Поскольку процессы охлаждение и перекачки воды являются инерционным циклам, поэтому разработанная система не требует скоростные модули прием передачи информации.

Исследования показывает, для последующего развития сети передачи данных гораздо проще изменить имеющуюся конфигурацию беспроводной сети, нежели изменять кабельную инфраструктуру системы [1]. В разработанном проекте использована система приема - передачи информации с применением широко известного радиомодема Невод-5 (расширение в радиоканал интерфейса RS-485).

Предлагаемая разработанная система очень дешевая и простая в исполнении и обслуживании. В нём сбор первичной информации по технологическим параметрам проводится на удаленных микропроцессорных модулях. Обработки информации системы реализованы на промышленном компьютере [2].

Система нижнего уровня включает:

- подсистему сбора и преобразование информации;
- передачи информации и прием управляющих сигналов.

Первая из подсистем нижнего уровня осуществляет:

- сбор, преобразование аналоговых и дискретных сигналов с объекта;
- контроль достоверности вводимой аналоговой информации;
- формирование дискретные сигналы (признаки) неисправности каналов;
- блокировки работы насосов по результатам обработки (верхнем уровне) определенных параметров системы;
- управления пуск – стоп двигателей.

Верхняя подсистема осуществляет расчет, проверку на ограничения и реализацию рассчитанных управляющих воздействий на исполнительным механизмам регулирующих устройств.

Система верхнего уровня выполняет, на основе разработанной алгоритме, ниже следующие функции :

- сбора и обработки информации верхнего уровня производит сбор аналоговой и дискретной информации с удаленных микропроцессорных модулей, а также информацию, вводимую машинистом-оператором с клавиатуры, осуществляет фильтрацию и проверку на достоверность входной информации;
- диагностики состояния основного оборудования и ситуационного контроля технологического процесса верхнего уровня предназначена для распознавания с определенной степенью достоверности ситуаций останова основного оборудования и состояния технологического процесса с выдачей рекомендаций по виртуальной структуре контуров регулирования.
- адаптации коэффициентов регуляторов на основании анализа динамики переходных процессов по каналам: "регулируемая переменная - положение регулирующего органа" осуществляет подстройку настроечных коэффициентов регуляторов, а на основании анализа поведения текущих значений аналоговых параметров, осуществляет подстройку коэффициентов фильтрации[3].
- представления информации к реализации комплекс функций диалога машиниста-оператора с персональным компьютером;
- создания мнемосхема технологических процессов в системе реального времени.

Обмен информацией между подсистемами осуществляться через общесистемную информационную базу. Режим функционирования системы - непрерывный.

Реализованная система обладает технические и функциональные избыточность с целью обеспечения возможности ее модернизации и развития.

Система сбор информации организована с первичных датчиков: датчиков давлений КРТ ДИ, токов и датчиков температуры. Измерения значении нагрузки двигателей вводится через токовые преобразователей Е-842. К ним сигналы поступают от токовой трансформаторов установленных на сети питания. Для управления технологический процессом разработана централизованная система управления, в котором управлявшим блоком является индустриальный компьютер ROBO 300.

Радио модем «Невод – 5» работает в диапазоне частот 433 МГц, имеет мощность 10 мВт, и отличаются следующими характеристиками[4]:

- расстояние связи «точка-точка" 10 км;

- поддержка интерфейсов RS-232 и RS-485;

- поддержка сетей со сложной топологией;

- масштабируемости сетей;

- программирование при помощи обычных терминальных программ.

В промышленной автоматизации одним из важнейших требований к радиомодемам является их "прозрачность" для другого оборудования, позволяющая без изменения настроек заменить проводную линию связи между удаленным промышленным контроллером и пунктом сбора данных. Невод-5 позволяет SCADA-системе взаимодействовать с контроллерами фирм Advantech, Fastwel, ICP DAS, Owen по интерфейсу RS-485 на скорости до 38400 бит/с с учетом задержек, возникающих при медленной передачи по эфиру.

Структурная схема системы АСУ ТП имеет следующий вид:

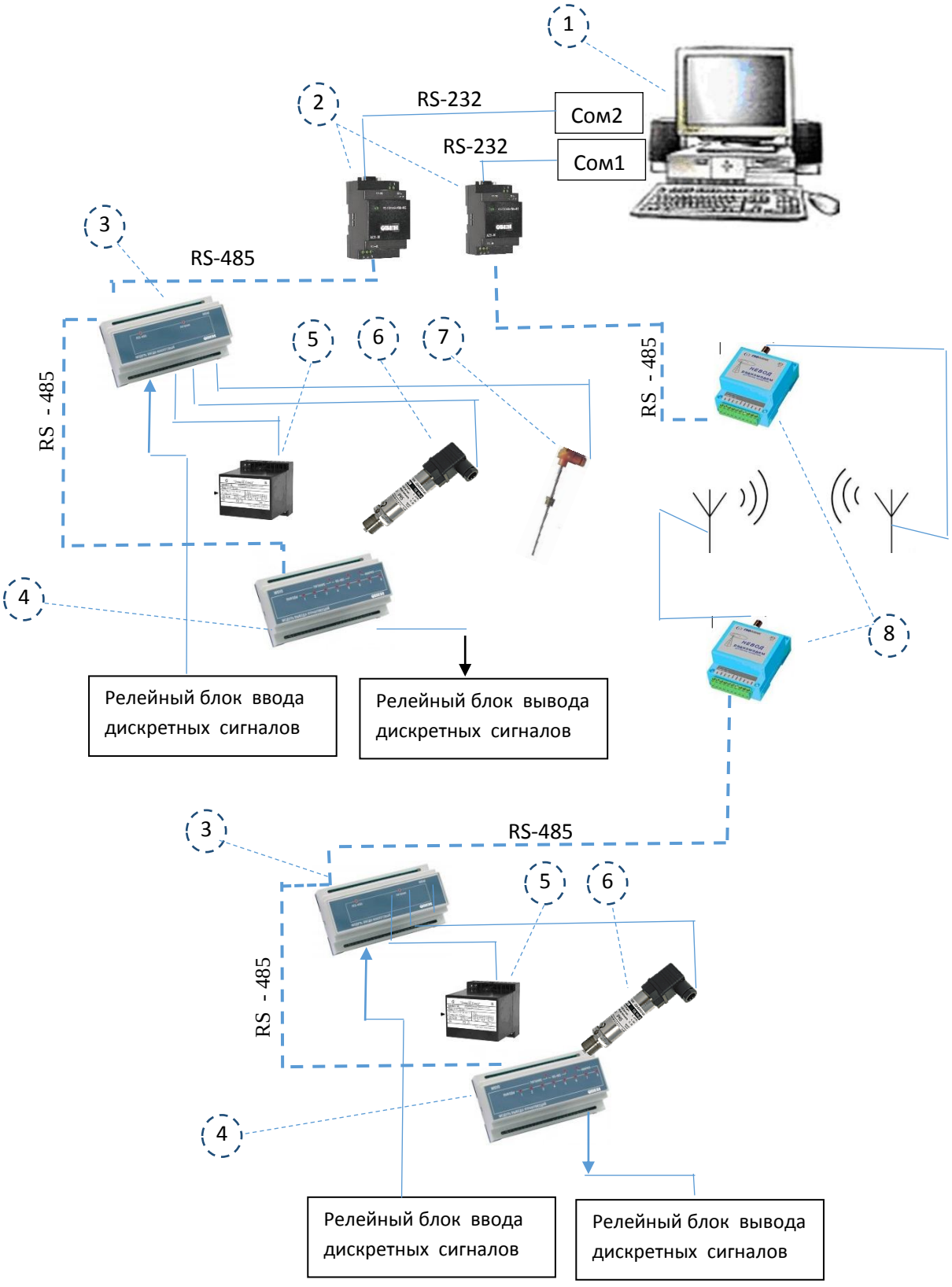


Рис.1 Структурная схема системы. 1-промышленный компьютер ROBO-3, 2. - конвертор RS – 485 на RS – 232, 3- МВА8 микропроцессорный модуль ввода аналоговых

сигналов, 4- МВУ8 микропроцессорный модуль вывода дискретных сигналов, 5- Е-845 преобразователь тока, 6- датчик давления, 7- датчик температуры, 8- радио модем.

Разработанная система автоматизации внедрены к реальному производству. Система используется, и показала свои эффективности с простотой обслуживания. АСУ ТП разработана в инструментальном пакете Trace Mode российской компании Адастра.

При решение поставленных задач разработан проект универсального характера и без особого труда пере настраиваемый к другим приборам АСУ ТП и новых условиях технологических процессов. Алгоритм программного обеспечения определяется требованиями контроля параметров технологического процесса в режиме реального времени. В алгоритме управления процессами предусмотрены реакция на предаварийные ситуации.

Литература.

1. Жуманиязов Р.С., Холкин В.И., Абдурахмонов С.М. Хен В.П. Автоматизированная система управления мельницами сырьевого передела на базе TRACE MODE. Журнал Приборы и системы. Управление, Контроль, Диагностика. №4, 2003 г., стр. 29-31, Россия.

2. Абдурахмонов С.М., Жураев Н.М. Прием-передача информации по интерфейсу RS-485 по беспроводном каналам в системах АСУ ТП. ФерПИ. Научно-технический журнал, 2016, №3, стр.154-157.

3. Пономаренко В. С., Арефьев Ю. И. Градирни промышленных и энергетических предприятий: Справочное пособие / Под общ. ред. В. С. Пономаренко. — М.: Энергоатомиздат, 1998. — 376 с

4.Абдурахмонов С.М., Нишонов И.У., Ахунова Ё.Н.. Модернизация технологического цикла помола цемента на основе микропроцессорной техники. ФерПИ. Научно-технический журнал, 2018, №2, стр.151-155..

МАЪЛУМОТЛАРНИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИДА ФОЙДАЛАНИЛАДИГАН БИР ТОМОНЛАМА ФУНКЦИЯЛАР.

Билолов Иномжон, Худойназаров Умиджон

Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали

Аннотация. Ҳозирда мавжуд симметрик шифрлаш алгоритмлари бир томонлама функцияларга асосланган чекли майдонда дискрет логарифмлаш, факторлаш ва даража параметри каби мураккабликларни келтириб чиқармайди. Мақолада чекли майдонда дискрет логарифмлаш муаммосига тенг кучли бўлган, бир томонлама функцияга асосланган шифрлаш алгоритми орқали симметрик криптотизимларни такомиллаштириш таклиф этилган.

Таянч сўзлар: Криптография, блокли шифрлар, криптобардошлилик, бир томонлама функция, дискрет логарифмлаш, факторлаш, тескарилаш, эллиптик эгри чизиқлар.

ОДНОСТОРОННИЕ ФУНКЦИИ, ИСПОЛЬЗУЕМЫЕ В СИММЕТРИЧНЫХ АЛГОРИТМАХ ШИФРОВАНИЯ ДАННЫХ

Билолов Иномжон, Худойназаров Умиджон

Ферганский филиал Ташкентского университета информационных технологий имени Мухаммад аль-Харезми

Аннотация. Существующие алгоритмы симметричного кодирования не усложняют дискретный логарифм, факторизацию и параметр степени, основанный на однонаправленной функции. В статье предлагается улучшить симметричные криптосистемы с использованием одностороннего алгоритма шифрования на основе функций, который одинаково силен в проблеме дискретного логарифма.

Ключевые слова: Криптография, блочные шифрования, криптостойкост**,** односторонние функции**,** дискретного логарифма**,** факторизации**,** эллиптических кривых.

ONE-WAY FUNCTIONS USED IN SYMMETRIC ENCRYPTION ALGORITHMS

Bilolov Inomjon, Xudoynazarov Umidjon

Fergana branch of the Tashkent University of Information Technologies of Muhammad al-Kharizmi

Annotation. The existing symmetric encoding algorithms do not make the complexity of the discrete logarithm, factorization and degree parameter based on a one-way function**.** The article suggests improving the symmetric cryptosystems by using a one-way function-based encryption algorithm that is equally strong in the problem of discrete logarithm.

Key words: Cryptography, block cypher, one way function, Tolerance, discrete logarithms, factoring, Elliptic Curve.

МАЪЛУМОТЛАРНИ СИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИДА ФОЙДАЛАНИЛАДИГАН БИР ТОМОНЛАМА ФУНКЦИЯЛАР.

Билолов Иномжон, Худойназаров Умджон

Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали

Кириш. Ахборот муҳофазасини таъминлашнинг энг самарали усулларидан бири криптографик алгоритмлардан фойдаланишдир. Чунки симметрик шифрлаш алгоритмлари тезкор, самарали ҳамда очиқ коммуникация тизимларида ишончли ахборот алмашинишни таъминлаш мумкин. Ахборот коммуникация тармоқларида маълумотлар алмашинувининг мухофазасини таъминлаш масалаларини ечишда симметрик шифрлаш алгоритмлари асосида яратилган криптотизим қанчалик ишончли бўлмасин, ундан амалда фойдаланиш жараёнида баъзи ечилиши керак бўлган муҳим хавфсизликни таъминлаш масалалари келиб чиқиши мумкин.[1]

Масаланинг долзарблиги. Ахборот коммуникация тизимларида ахборот хавфсизлигининг асосий масалаларидан бири юқори ҳажмдаги ахборотларни алмашинишда самарали криптотизимлардан фойдаланиш лозимлигини эътиборга олиб, бардошлилиги оширилган симметрик шифрлаш алгоритмларини ишлаб чиқиш долзарб муаммоларни ечишга йўналтирилган ишлардан бири ҳисобланади.

Масаланинг қўйилиши. Маълумотларни криптографик услублар билан мухофазалаш жараёнлари алгоритмик тиллар билан махсус криптобардошли алгоритмларни дастурлаш орқали ёки махсус техник аппаратлар ёрдамида амалга оширилади. Бунда дастурлаш услублари ўзининг қўлланилиши жиҳатидан қулайлиги билан ажралиб туради.

Юқорида қўйилган масалалар ва замонавий шифрлаш алгоритмларига қўйиладиган талабларни ҳисобга олиб, мавжуд симметрик блокли шифрлаш алгоритмларининг криптобардошлилигини таъминловчи хусусиятлари ва уларнинг таҳилини кўриб чиқамиз.

Симметрик блокли шифрлаш алгоритмлари бир нечта босқичлардан иборат бўлиб, ҳар бир раунд аралаштирувчи ва тарқатувчи акслантиришлардан тузилган. Бундай асосда тузилиш тамойили, ҳар бир раунд шифрлаш жараёнини ҳар хил калитлар билан бир хил турдаги акслантиришларни амалга оширишга, ҳамда, дешифрлаш жараёнини раунд акслантиришлари ва калитларини тескари тартибда қўллашнинг самарали имконини беради. Алгоритм асосини ташкил этувчи, раунд шифрлаш жараёнини амалга оширувчи, аралаштириш ва тарқатиш хусусиятларига эга бўлган функциялар асосий акслантиришлар дейилади. Асосий акслантришларнинг аппарат-техник жиҳатидан қулай қўлланиш модели сифатида тескари боғлиқликка эга бўлган силжитиш регистрларини келтириш мумкин. Бунда тарқатувчи акслантириш тескари боғлиқликни таъминловчи функция билан, аралаштирувчи акслантириш эса, регистрдаги маълумотларни силжитиш билан амалга оширилади. Юқоридаги акслантиришлар ҳозирда мавжуд аксарият симметрик блокли шифрлаш алгоритмларининг криптобардошилигини таъминловчи хусусиятларидан бири ҳисобланади.[2]

Ҳозирда кўплаб дастурий иловаларда маълумотларни химоялаш учун турли криптографик алгоритмлардан фойдаланилмоқда. Дастлаб бу алготирмлар самарали натижа берсада лекин, замонавий суперкомпьютерлар ҳамда етарлича мураккаб криптотаҳлил воситалари ва вақт мавжуд бўлганда бу алгоритмларни замонавий ахборот технологияларида қўлланилганда ҳужумларга етарлича бардошсизлик ва ишончсизлик ҳолатларини учратиш мумкин. Симметрик блокли шифрлаш алгоритмлари ёрдамида тузилган криптотизимлар ҳам турли ҳил криптотаҳлил усулларига бардошли бўлишини таъминлаши лозим. Бу эса дастурий иловаларда қўлланилаётган шифрлаш алгоритмларининг маълум мезонларга кўра таҳлил этишни тақозо этади. Бу мезонлар

алгоритмнинг *архитектураси*, *хавфсизлиги*, *хотира хажми*, *шифрлаш усули*, эластиклиги ҳамда *бардошлилиги* каби ҳусусиятларини ўз ичига олади.[3]

Қуйида биз бир нечта амалиётда кўп фойдаланиладиган криптографик алгоритмларнинг юқоридаги мезонлар бўйича таҳлилини кўриб ўтамиз.

Архитектура- архитектура алгоритмнинг тузилиши, бажарилаётган жараёнлар, ўзига хослиги ва алгоритмнинг амалга ошириш усулларини ифодалайди. 1-жадвалда алгоритмларнинг архитектураси тасвирланган.[3]

1-жадвал

Алгоритмлар	**Алгоритм тузилиши**	**Очиқ матн узунлиги**	**Калит узунлиги**	**Блоклар сони**	**Раундлар сони**
DES	Feystel тармоғи	64 бит	56 бит	8	16
Blowfish	Feystel тармоғи	64 бит	128-448 бит	4	16
CAST	Feystel тармоғи	64 бит	40-128 бит	4	12-16
AES	Элементлар устида ўрнига қўйиш, аралаштириш амаллари	128 бит	128,192,256 бит	1	10,12,14

Хавфсизлик- бу криптотизимнинг ҳужумга қаршилик қила олиш қобилиятидир.

DES алгоритмининг хавфсизлиги 56 бит узунликдаги калитни 7,2×1016 эҳтимолий калитларга генерациялаш ва махсус калитларни ишлаб чиқишга боғлиқ. Агар калитлар тез-тез алмаштирилса, модификация ва криптианализларга қарши етарли бардошликка эга бўлади. Дастлаб алгоритм ҳужумларга бардошли ва хавфсиз деб ҳисобланган. DES турли дифференциал ва чизиқли криптотаҳлилларга бардошли ҳисобланган аммо DES ни дешифрлаш учун махсус машина ишлаб чиқилди. Бир нечта компьютерлар фойдаланиб қилинган криптотаҳлилда 17 соат давомида шифрлаш калити қўлга киритилган. Ўз навбатида алгоритм бошқарув органлари ва катта корпорациялар фойдаланиши учун ишончсиз эканлиги исботланди.[4]

Blowfish алгоритмида қўлланилган унинг хавфсизлигига етарлича таъсир кўрсатади. Бу алгоритмда чап ярим блокнинг ўзгариши ўнг ярим блокнинг ўзгаришига олиб келади. Бундан ташқари калитнинг ўзгариши ҳар бир раунддан сўнг чап ва ўнг ярим блокларга ҳам таъсир кўрсатади. Асосий калитнинг ҳар бири автоном бўлган мустақил раунд калитларини ўз ичига олиб, турли ҳужумларни амалга ошириш самарасиз ва жуда мураккабдир.[5]

CAST алгоритмида ҳимояни кучайтириш учун ўзгарувчан узунликдаги калитлар ишлаб чиқилади. **CAST** алгоритми ҳимояси чизиқли ва дифференциал анализларга етарлича қаршилик кўрсата олади.[3]

AES. Rijndael алгоритмининг ҳимояси зиддиятли ҳужум ва квант имкониятидаги компьютер ҳужумларига қаршилик кўрсатишни таъминловчи рухсат этилган калит узунлиги 256 битли ўзгарувчан ҳарактердаги калитларга боғлиқ. Rijndael алгоритмининг раундларига бўладиган асосий ҳужумлар, тартибли, мукаммалашган тартибли ва тескари калитлар жадвали ҳужумларидир. Аммо бу ҳужумларни амалга ошириш амалий жиҳатидан имконсиздир.[4]

Хотира ҳажми ва шифрлаш усули. Ушбу бўлимда шифрлаш алгоритмлари хотира ҳажми, шифрлаш усуллари ва калитлар тақсимланиши асосида таҳлил қилинади. Хотира ҳажми алгоритмда қатнашган функциялар миқдорига боғлиқ. AES, DES, Blowfish, CAST алгоритмларини хотира ҳажми ва шифрлаш суръати бўйича таққослайдиган бўлсак, улар орасида AES, DES, алгоритмлари хотира ҳажми бўйича минимал натижани акс этади, AES ва Blowfish алгоритмлари эса шифрлаш суръати бўйича максимал натижани кўрсатади. Аммо алгоритмларни самаралилигини бундай хулосалари бўйича ўзаро

таққослаш анча эскирган усулдир. Хозирги замонавий ахборот технологиялари ва тизимларнинг ривожланишини ҳисобга оладиган бўлсак, алгоитмларнинг лойиҳалаш учун зарур бўлган бошқа параметрларни ҳам ҳисобга олиш зарур.[6]

Эластиклиги- бу мустақил алгоритмнинг етарлича кичик ўзгаришларга бардошлилигини ифодалайди.

Қуйидаги графикда алгоритмлар уларнинг эластиклиги, калитларнинг ўзгариши ва бошқа хусусиятлари бўйича таҳлил қилинган.[1]

2-жадвал

Алгоритмлар	**Эластиклиги**	**Калитлар ўзгариши**	**Изоҳ**
DES	Йўқ	Йўқ	DES алгортимин турли калит ўзгаришларини қўллаб қувватламайди.
Blowfish	Ҳа	64-448	Калит узунлиги 32 битли кўп сонли раунд калиталарига боғлиқ.
CAST	Ҳа	64,125,256	Калит узунлиги 64 бит бўлганда CACT алгортими турли дифференсиал ва чизиқли ҳужумларда ошкор этилган. 128 ва 256 битли ўзгарувчан калитли эластик тузилиши унинг бардошлилиги ва хавфсизлигини оширади.
AES	Ҳа	128,192,256	AES структураси 64 битли узунликдаги калитни кенгайтириб бир ҳил қисмкалиткарга ажратишдан иборат.

Бардошлилик- алгортмнинг қай тарзда мавжуд компьютер ресурсларидан фойдаланган ҳолда самарали натижа беришини ифодалайди**.** Криптографик алгоритмнинг криптобардошлилиги унинг турли ҳужумлар ва криптотаҳлилларга дош бера олиш қобилиятидир.

DES алгоритмининг заиф калитлари унинг чизиқли криптоанализ ҳужумларига бардошсиз эканлигини кўрсатади. Алгоритм яна “қўпол куч” ҳужумида тўлиқ фош этилган.[4]

Blowfishнинг 4 раундли алгоритми 2-даражали чизиқли криптоанализда очиб ташланган. Алгоритм S блоклар маъкум бўлган ҳолатда калитлар генератсия иштирок этган P массивни дифференсиал криптотаҳлил усулида $2^{8н+1}$ та танлаб олинган очиқ маълумот ва шифрмаълумот ёрдамида калитни топпиш мумкин. $R = 16$ да бу қиймат 2^{129} га тенг. Акслантиришларнинг келтирилган ҳусусиятлари алгоритмнинг самарадорлигини оширишга қаратилган.[5]

AES алгоритми турли криптотаҳлил ва ҳужумларга етарлича қаршилик кўрсата олади. Шифрлаш алгоритмининг кузатилган математик ҳусусиятлари ҳужумга бардошлидек кўринса ҳам, алгоритмнинг жиддий заифлик томонлари йўқ эмас.

CAST алгоритмининг мавжуд версиялари дифференсиал криптотаҳлилга бардошсиздир. Алгоритмда қўлланилган S блокларда кирувчи қийматларни билган ҳолда чиқувчи қийматларни топиш мумкин, лекин, чиқувчи қийматларни билган ҳолда киоувчи қийматларни топиш мумкин эмас. Шундай бўлсада Л.Кнудсен бу алгортимни таҳлил қилиб, чизиқли ва дифференсиал криптотаҳлил усулларига бардошли эмаслигини кўрсатади. Алгоритмни танлаб олинган очиқ матнларга боғлик калитлар билан таҳлил қилиш тўлиқ танлаб олиш усулига нисбатан деярли 4 марта осон эканлигини кўрсатади.[6]

Мисол учун DES шифрлаш алгоритмида хавфсизлик, махфий калитларни генератсийлаш, тезлик ва аутентификатсия ва бир нечта хусусиятларида камчиликлар мавжуд. Блowфиш алгортимининг уч раундли нақли таҳлилида заиф калитлар аниқланган, мавжуд нақллари эса дифференсиал криптотаҳлилда ошкор этилган. Кўрилган алгоритмлар орасида AES алгоритмида жиддий камчиликлар мавжуд эмас. Шунга қарамай ахборот технологияларининг ривожланишини ҳисобга олиб, бир қанча нозик

томонларига эътибор қаратиш керак. Алгоритмнинг бир нечта параметрлари турли криптотаҳлилларга етарлича бардош бера олмаслиги мумкин.[6]

Юқорида турли алгоритмлар турли параметрлари архитектураси, эластиклик, ишончлилик, шифрлаш суръати, хотира ҳажми ҳамда бардошлилиги бўйича таҳлил қилинди. Мавжуд алгоритмларнинг заифликларига эътибор бериш ҳамда дастурий иловалар учун мукаммал ва етарли даражада мураккабликни таъминловчи симметрик шифрлаш алгоритмларини ишлаб чиқишдан иборат. Криптографиядаги аксарият симметрик шифрлаш алгоритмлари масалаларни ечишнинг кўп вақт талаб қилиниши ва ҳисоб китоблар-учун ҳисоблаш қурилмаларида катта ҳажмдаги хотира талаб этилиши билан боғлиқ бўлган мураккаблиларни келтириб чиқармайди. Симметрик шифрлаш алгоритмларини такомиллаштириш ва улар асосида криптотизимлар яратиш усуллари ҳамда алгоритмларини ишлаб чиқиш долзарб масалалар қаторига киради.

Масаланинг ечилиши. Агар симметрик шифрлаш алгоритмларига масалаларни ечишнинг кўп вақт талаб қилиниши ва ҳисоб-китоблар учун ҳисоблаш қурилмаларида катта ҳажмдаги хотира талаб этилиши билан боғлиқ бўлган мураккаблиларни келтириб чиқарувчи бир томонлама функциялар устида керакли математик акслантиришларни амалга ошириб, тадбиқ қилинса, еталича бардошли симметрик криптотизимларни яратиш имконига эга бўлинади.

Бир томонлама функция- бу таъриф бўйича, шундай $y = f(x)$ функцияки, унинг аниқланиш соҳасидан бўлган ихтиёрий x учун $f\ x\ = y$ қиймат осон ҳисобланиб, қийматла соҳасининг барча y қийматларига мос келувчи x қийматларни ҳисоблаб топишни амалий жиҳатдан имконияти йўқ.[2]

Криптологияда носимметрик криптотизимлар етарлича мураккабликларни келтириб чиқарувчи алгоритмлардан ташкил этилади. Ҳозирда носимметрик криптотизимлар ахборот хавфсизлигининг кўплаб муаммоларини ечиб беришга қодир деб тан олинган.[5]

Носимметрик криптотизимларнинг математик асосини катта тартибли чекли тўпламларда берилган чекли майдон, ҳалқа, группа, қисмгруппа кўринишидаги алгебраик структуралар ва махфийликка эга бўлган бир томонлама функциялар ташкил этади ҳамда турли ҳужумларга бардошлилиги эса бир томонлама функцияларнинг тескариланиши ўта мураккаб муаммо бўлишига асосланади. [7]

Замонавий носимметрик криптотизимлар қуйидаги турдаги масалаларни ечишнинг кўп вақт талаб қилиниши ва ҳисоб китоблар-учун ҳисоблаш қурилмаларида катта ҳажмдаги хотира талаб этилиши билан боғлиқ бўлган мураккаблиларга асосланади.[7]:

Қуйидаги жадвалда муаммо тури бўйича носимметрик криптотизимлар таснифи келтирилган.

3-жадвал

Муаммо	**Баёни**
Факторлаш	Бутун факторлаш муаммоси: бутун мусбат n берилган, унинг Туб факторларини топпиш керак, яъни $n = p_1^{e_1} p_2^{e_2} \ldots . p_k^{e_k}$кўринишида ёзиш керак, бу ерда p^i −турли туб онлар ва ҳар бири $e_i \geq 1$.
RSA муаммоси (RSAP)	RSA муаммоси: иккита турли p ва q тоқ сонларнинг кўпайтмаси бўлган бутун мусбат n сони, $EKUB\ e,\ p-1\ \ q-1) = 1$ га тенг бўлган бутун мусбат e сони ва c берилган. Шундай бутун m ни топпиш керакки, унда $m^e \equiv c(mod\ n)$.
Квадратик чегирма муаммоси	Квадратик чегирма муаммоси: тоқ мураккаб бутун n ва $\frac{a}{n} = 1$ Якоби белгисига эга бўлган бутун a сони берилган, a сони n модул бўйича квадратик чегирма эканлиги ёки чегирма амслиги

	аниқлансин.
n модули бўйича квадрат илдиз (SQROOT)	n модули бўйича квадрат илдиз: мураккаб бутун n сони ва n модули бўйича $a \in Q$ квадратик чегирма тўплами берилган, n модули бўйича a дан шундай бутун квадратик илдиз x топилсинки, унда $x^2 = a \ modn$ ўлсин.
Дискрет логарифм муаммоси. (DLP)	Дискрет логарифм муаммоси: туб сон p учун, чекли майдон Z_{p*} да ҳосил қилувчи элемент α ҳамда $\beta = Z_{p*}$ берилган бўлса, шундай $0 \le x \le p-2$ бўлган бутун x сон топилсинки, унда $\alpha^x = \beta \ modp$ бўлсин. Бу ерда x- даража кўрсаткичи.
Умумлашган дискрет логарифм муаммоси. (GDLP)	Умумлашган дискрет логарифм муаммоси : n тартибли чекли циклик группа G, Gнинг ҳосил қилувчиси α ва $\beta \epsilon G$ элемент берилган, шундай $0 \le x \le n-1$ бўлган бутун x сони топилсинки, унда $\alpha^x = \beta$ бўлсин.
Диффи-Хеллман муаммоси (DHP)	Диффи-Хеллман муаммоси: туб сон $p, Zp*$ ҳосил қилувчиси- α ҳамда $\alpha^a(modp)$ ва $\alpha^b(modp)$ элементлари берилган, $\alpha^{ab}(modp)$топилсин.
Умумлашган Диффи-Хеллман муаммоси(GDHP)	Умумлашган Диффи-Хеллман муаммоси: чекли циклик группа G, G ҳосил қилувчиси – α ва группа элементлари α^a ва α^b берилган, α^{ab} топилсин.
Эллиптик эгри чизиқда дискрет логарифм муаммоси. (ECDLP)	Эллиптик эгри чизиқда дискрет логарифм муаммоси : K чекли майдон ва G нуқтада тартиби n бўлган G нуқта, $Q \in E(K)$ нуқтада E эллиптик эгри чизиқ берилган. $Q \in [d]G$ шартни қаноатлантирувчи d, $0 \le d \le n-1$ бутун сонни топиш талаб этилади, агарда у мавжуд бўлса.

Ушбу мақолада чекли майдонда дискрет логарифмлаш муаммосига тенг кучли бўлган бир томонлама функцияга асосланган симметрик шифрлаш алгоритми таклиф этилади.

Шифрлаш алгоритми. Шифрлаш алгоритми қуйидаги шифрлаш параметрлар асосида амалга оширилади:

R диакўпайтириш ва модул учун асос бўлган махфий сон;

диадаражага кўтариш кўрсаткичи $r =$ 3 деб эълон қилинади;

g_1 шифрлаш асоси;

x – диакўпайтириш рамзи R_1ни ҳосил қилувчи тасодифий сон;

Шифрлаш алгоритми қуйидаги қадамларни ўз ичига олади:

Кириш:

R сони, g_1, x ёпиқ калитлар киритилади;

M очиқ матннинг бутун сон шаклидаги кўриниши киритилади.

Чиқиш:

Шифрматн C.

1. $R_1 \leftarrow R * x \ modn_0$ ҳисобланади,
2. $M_1 \leftarrow g_1^{\backslash M_1} modn_0$ ҳисобланади, бунда диакўпайтириш коэффициенти R_1 га тенг,
3. $C \leftarrow g_1^{\backslash M_1} modn_0$ ҳисоланади, бунда диакўпайтириш коэффициенти R_1 га тенг,
4. C шифрматн чиқарилади

Дешифрлаш алгоритми:

Кириш

R сони, ёпиқ калитлар g_1, x киритилади,
шифрматн C нинг сон қиймати киритилади.
Чиқиш : очиқ матн M.

1. 1. $s(1)_1 = \mathrm{R} - C * g_1{}^{\backslash -1} mod R$ ҳисобланади,
   2. $g_1{}^{\backslash s(1)_1} = g_1{}^{\backslash s(1)_1} \mathrm{mod}\ \mathrm{R}^2$ ҳисобланади,
   3. $s(1)_2 = \quad C \circledR g_1{}^{\backslash s\ 1\ 1} \quad * g_1{}^{\backslash -1} - s\ 1\ _1 \quad mod R^2$ ҳисобланади,
   4. $s(1)_3 = R^2 - s(1)_2$ ҳисобланади,
   5. $g_1{}^{\backslash s(1)_3} = g_1{}^{\backslash s(1)_3} mod R^2$ ҳисобланади,
   6. $M_1 = \quad C \circledR g_1{}^{\backslash s\ 1\ 3} \quad * g_1{}^{\backslash -1} - s\ 1\ _3 \quad mod R^3$ ҳисобланади.

2. 1. $s_1 = \mathrm{R} - M1 * g_1{}^{\backslash -1} mod R$ ҳисобланади,
   2. $g_1{}^{\backslash s_1} = g_1{}^{\backslash s_1} \mathrm{mod}\ \mathrm{R}^2$ ҳисобланади,
   3. $s_2 = \quad M_1 \circledR g_1{}^{\backslash s_1} \quad * g_1{}^{\backslash -1} - s_1 \quad mod R^2$ ҳисобланади,
   4. $s_3 = R^2 - s_2$ ҳисобланади,
   5. $g_1{}^{\backslash s_3} = g_1{}^{\backslash s_3} mod R^2$ ҳисобланади,
   6. $\mathrm{M} = \quad M_1 \circledR g_1{}^{\backslash s_3} \quad * g_1{}^{\backslash -1} - s_3 \quad mod R^3$ ҳисобланади.

3. M очиқ матн чиқарилади.

Алгоритмни шакллантиришда асосан модул функцияси, R параметрли тескарилаш функцияси, тўрт аргументли диадаражага кўтариш кўтариш функцияси ва параметрли кўпайтириш амаллари дастурни шифрлаш ва дешифрлаш жараёнлари учун асосий функциялар бўлиб хизмат қилади.

Алгоритм реализациясини амалга ошириш масаласини амалий тарзда ҳал этиш ва уни текшириш учун икки хил усулдан фойдаланамиз.

Биринчи усул тажриба сифатида MS Excel office дастурида амалга оширилган шифрлаш алгоритмларининг қадамлари кетма-кетлиги бўйича реализациясини амалга ошириш. Бу усул ҳисоблаш қадамларининг натижалари ва алгоритмнинг тўғри бажарилишини текшириш учун қулай ҳисобланади.

Шифрлаш жараёни

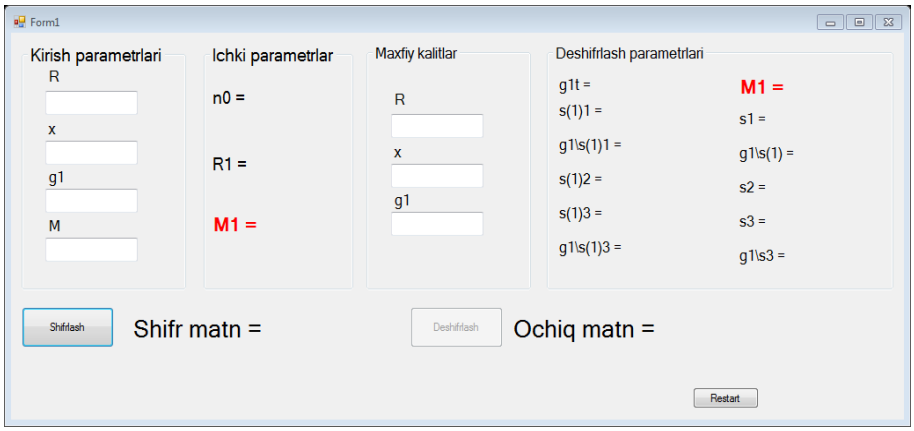
Дешифрлаш жараёни

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	R	r	l	x	Rr	g1	M	n0	R'	M1	C	g1t	s(1)1	g1\s(1)1	s(1)2	s(1)3	g1\s(1)3	M1	s1	g1\s1	s2	s3	g1\s3	M	
2	13	3	1	3	2197	4	2000	2197	39	1591	1957	10	8	97	70	1451	1475	1591	2	632	141	1380	1919	2000	
3	17	3	1	3	4913	7	1194	4913	51	3122	1505	22	6	246	232	2369	4649	3122	13	227	38	2563	3916	1194	
4	19	3	2	1	6859	4	2789	6859	19	4449	4990	5	16	83	117	244	2800	4449	4	35	262	99	3664	2789	
5	11	3	1	1	1331	4	1194	1331	11	1245	558	3	9	80	35	86	388	1245	5	86	105	16	130	1194	
6	13	3	1	2	2197	4	13	2197	26	1742	546	10	0	1	62	614	1338	1495	0	1	88	588	558	338	

1-расм Алгоритмнинг Excel дастуридаги шаклланиши.

Аксарият симметрик шифрлаш алгоритмларида очиқ матнни шифрматнга ўгириш акслантиришлари ва шифрматнни очиқ матнга ўгириш акслантиришлари қадамлари сони бир хил бўлади. Бир томонлама функцияга асосланган симметрик шифрлаш алгортмида эса дешифрлаш учун фойдаланилган функсионал алмаштиришлар шифрлаш учун фойдаланилган функционал алмаштиришларидан бир неча марта кўп. Бу эса махфий калитлар маълум бўлмаганда очиқ матнни топиш етарлича мураккабликни келтириб чиқаради. Агар алгоритмнинг умумий кўринишида шифрлаш асоси ва диадаражага кўтариш кўрсаткичлари сони етарли даражада оширилса шифрлаш ва дешифрлаш қадамлари орасидаги фарқлари сони анча ортади.

Иккинчи усул эса алгоритмнинг дастурий маҳсулот сифатида реализациясини амалга ошириш. Бунда алгоритмнинг хосса ва имкониятлари аниқроқ тарзда намоён бўлади. Бир томонлама функцияга асосланган симметрик шифрлаш алгоритми шифрлаш ва дешифрлаш функцияларининг амалга ошиш жараёнларини текшириш мақсадида, алгоритмнинг $l=1$ ва $r=3$ га тенг бўлган хусусий ҳоли учун дастур тузилди.



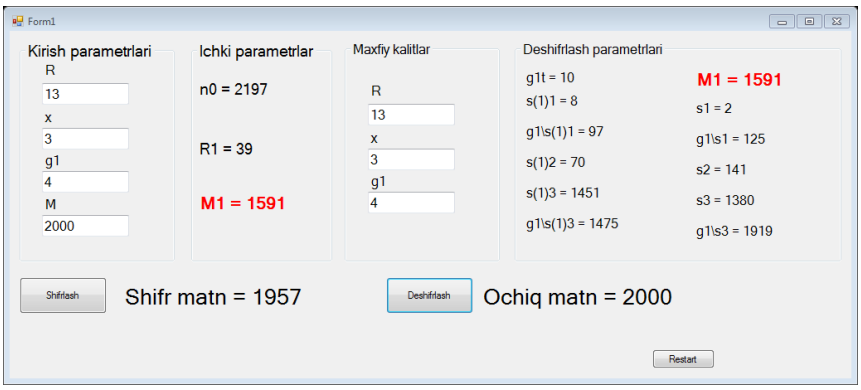
2-расм. Шифрлаш алгоритми дастури ойнаси.

Дастур ойнаси *шифрлаш* ва *дешифрлаш* жараёнларини акс эттирувчи бўлимдан ташкил топган. Кириш параметрлари қисмида алгоритмдаги махфий параметрлар ва очиқ матннинг сон қийматидаги кўриниши киритилади.

Дастурнинг шифрлаш бўлимига тегишли ички параметрлар қисми эса шифрлаш жараёнида ўзлаштириладиган ички қийматларни акс этиради.

Дешифрлаш бўлимида эса шифрматнни аслига ўгириш жараёнидаги функционал алмаштиришларнинг натижалари акс этади.

Дастурни текшириш учун 2-расмда берилган электрон жадвалдаги кириш параметрлари қийматларини дастурга киритиб дастур ва алгоритмдаги функционал алмаштиришдаги қийматларни ўзаро солиштирамиз. Жадвалнинг 1-сатрида $R = 13, x = 3, g = 4$ ва очиқ матн $M = 2000$ деб олинган.



3-расм Шифрлаш алгоритми дастури ишлаш жараёни

Жадвал ва дастур қийматларини қиёсласак ўзаро бир хил қийматларни акс эттирганини кўриш мумкин. Бу эса дастур функцияларининг тўғри ишлаётганлигини билдиради.

Яна алгоритмнинг жадвалга мос бир нечта кириш қийматларини киритиб дастурни синаб кўрамиз.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	R	r	l	x	Rr	g1	M	n0	R'	M1	C	g1t	s(1)1	g1\s(1)1	s(1)2	s(1)3	g1\s(1)3	M1	s1	g1\s1	s2	s3	g1\s3	M
2	23	3	1	1	12167	4	1194	12167	23	11170	1325	6	8	285	61	468	2125	11170	2	376	136	393	10933	1194
3	17	3	1	3	4913	7	1194	4913	17	2952	4633	5	6	110	62	227	4836	2952	13	40	38	251	2284	1194
4	19	3	2	1	6859	4	2789	6859	19	4449	4990	5	16	83	117	244	2800	4449	4	35	262	99	3664	2789
5	11	3	1	1	1331	4	1194	1331	11	1245	558	3	9	80	35	86	388	1245	5	86	105	16	130	1194
6	11	3	1	1	1331	4	1194	1331	11	1245	558	3	9	80	35	86	388	1245	5	86	105	16	130	1194
7																								
8	19	3	1	1	6859	7	2789	6859	19	4646	1134	11												

4-расм Қийматлар берилганда жадвалдаги акслантиршлар.

4-расмда берилган жадвалидаги криш қийматларини дастурга киритиб уларни ўзаро қиёслаймиз. Жадвалнинг биринчи сатридаги дастурга мос кириш қийматлари R=23, x=1, g1=4 ва очиқ матн M=1194 га тенг.

Агар дастур ишлаш жараёнида дешифрлаш бўлимидаги калитлардан бирортаси ўзгарса, мос равишда дешифрлашнинг акслантиришлари қийматлари ҳам ўзгаради.

Чунки шифрлаш ва дешифрлаш махфий параметрлари бир-бирига боғлиқ бўлганлиги учун уларнинг ихтиёрий бирининг ўзгариш шифрлаш параметрларининг деярли барчасини ўзгаришига ва очиқ матнни ўзгаришига сабаб бўлади.

Олинган натижалар таҳлили ва хулоса. Одатда бир томонлама функциялар носимметрик криптотизимларда кенг фойдаланилади. Таклиф этилган шифрлаш алгоритмида эса, бир томонлама функциянинг симметрик криптотизимларга тадбиқи келтирилган. Мазкур симметрик шифрлаш алгоритми бошқа симметрик алгоритмлардан фарқли равишда бир томонлама функцияга асосланади. Бу эса алгоритмнинг етарлича мураккаблилигини ва криптобардошлилигини таъминлайди.

Хулоса қилиб шуни айтишимиз мумкинки, таклиф этилган бир томонлама функцияга асосланган симметрик шифрлаш алгортмидаги дешифрлаш жараёнидаги қадамлар сони шифрлаш жараёнидаги қадамлар сонидан бир неча марта кўп эканлигини кўриш мумкин. Айтиб ўтилган хусусиятлар махфий калитлар маълум бўлмаганда очиқ матнни топишда етарлича мураккабликни келтириб чиқаради.

Адабиётлар

[1] Худойназаров Умиджон. Бардошлилиги оширилган симметрик шифрлаш алгоритмини ишлаб чиқиш. Магистр академик даражасини олиш учун ёзилган диссертатсия.Тошкент-2016.

[2] Акбаров Д.Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши”. Тошкент 2009.

[3] Г. Мутҳукумар, Др. Э. Георге Дҳарма Пракаш Раж. А Сомпаративе Аналйсис он Сймметрис Кей энсрйптион Алгоритҳмс. Интернатионал Жоурнал оф Адвансед Ресеарч ин Сомпутер энгинееринг & Течнологй Волуме 3, Иссуе 2, Фебруарй 2014.

[4] W. Сталлингс, Срйптограпҳй анд Нетwорк Сесуритй Принсиплес анд Прастисес Фоуртҳ эдитион, Пеарсон эдусатион, Прентисе Ҳалл, 2010

[5] Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002. – 816 с

[6]Худойназаров У.У. “ Замонавий шифрлаш алгоритмларининг қиёсий таҳлили”. Республиканский семинар: “ «Актуальные проблемы использования электронной цифровой подписи». Сборник тезисов и докладов. Ташкент, 20 мая 2016 г

[7] Акбаров Д., Хасанов П., Хасанов Х., Ахмедова О. Криптографиянинг математик асослари. Ўқув қўлланма.– Тошкент, 2010 – 210 б.

Муаллифлар тўғрисида

1. Билолов Иномжон Ўктамович - Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали доценти.

   Тел: +998933732410

   e-mail: bilolov1959@mail.ru

2. Худойназаров Умиджон Умаржон ўғли - Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали ассистенти.
Тел: +998905855891
e-mail: Umidjonxudoynazarov@gmail.com