КРИПТОГРАФИЯ

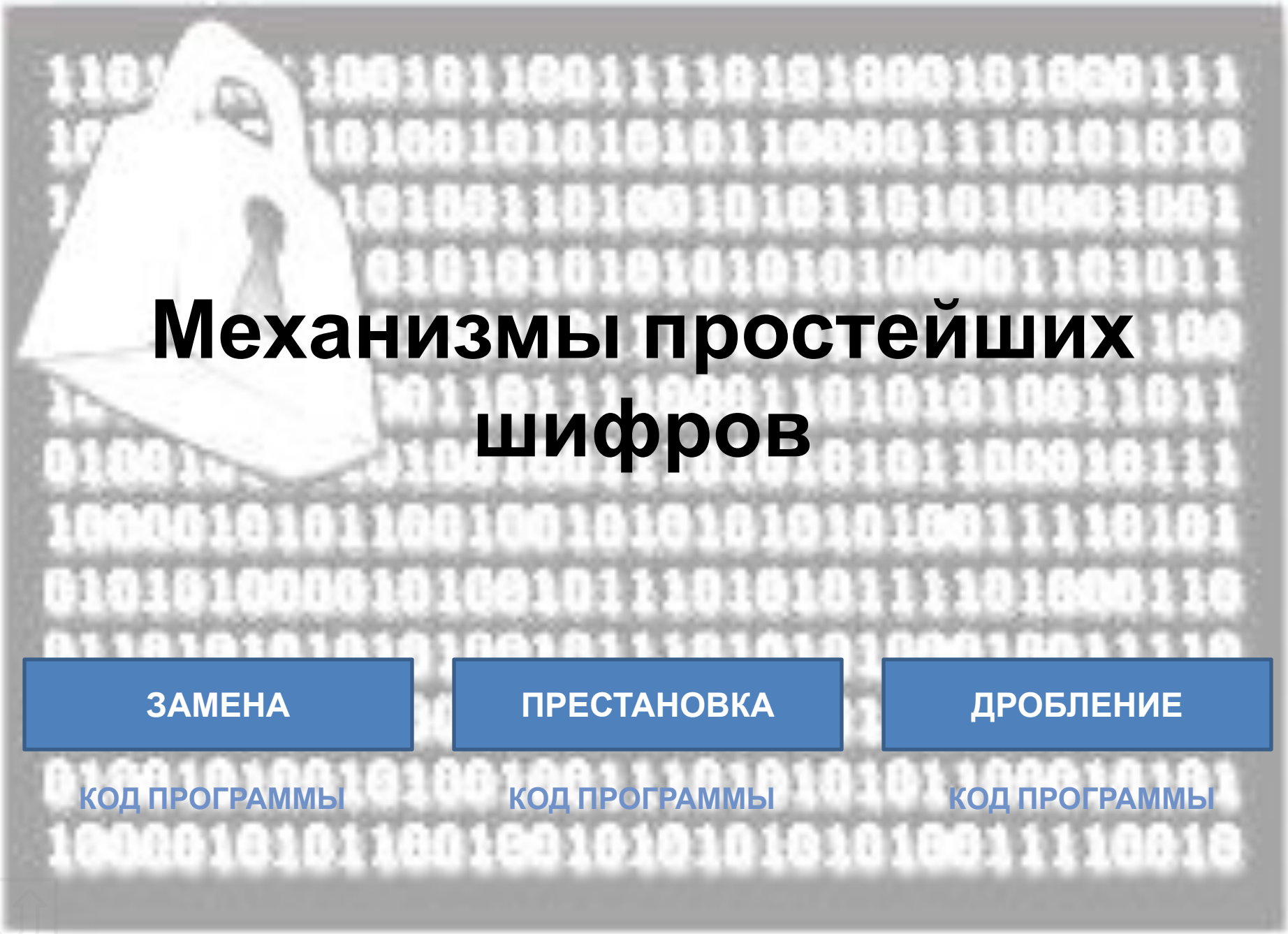
Азы шифрования
и
история развития

Содержание

Введение

КРИПТОГРАФИЯ, или криптология, наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать без специального секретного ключа. Слово «криптограф» происходит от древнегреческих слов kryptos 'секрет' и graphos 'писание'. Исходное сообщение называется в криптографии открытым текстом, или клером. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или криптограммой.

Процедура шифрования обычно включает в себя использование определенного алгоритма и ключа. Алгоритм – это определенный способ засекречивания сообщения, например компьютерная программа или список инструкций. Ключ же конкретизирует процедуру засекречивания.



Механизмы простейших шифров

ЗАМЕНА

ПРЕСТАНОВКА

ДРОБЛЕНИЕ

КОД ПРОГРАММЫ

КОД ПРОГРАММЫ

КОД ПРОГРАММЫ

ЗАМЕНА

Один из способов шифрования – простая замена, при которой каждая буква открытого текста заменяется на какую-то букву алфавита (возможно, на ту же самую). Для этого отправитель сообщения должен знать, на какую букву в шифротексте следует заменить каждую букву открытого текста. Часто это делается путем сведения нужных соответствий букв в виде двух алфавитов. Шифрограмма получается путем замены каждой буквы открытого текста на записанную непосредственно под ней букву шифровального алфавита.

КОД ПРОГРАММЫ

ПЕРЕСТАНОВКА

В шифре перестановки все буквы открытого текста остаются без изменений, но переставляются согласно «заранее оговоренному правилу». Здесь также может использоваться ключ, управляющий процедурой шифрования. Ключевое слово может быть использовано для получения шифровальной числовой последовательности путем нумерации букв ключевого слова (относительно друг друга) в порядке их следования слева направо в стандартном алфавите. Далее под числовой последовательностью в строках, равных по длине ключевому слову, записан открытый текст. В процессе шифрования текст выписывается уже по отдельным столбцам в порядке, определяемом данной числовой последовательностью.

Этот метод перестановки называется перестановкой столбцов, но можно набрать и другие «маршруты» перестановки, например, выписывать шифротекст следуя по диагоналям (слева направо или справа налево, или же следуя левое и правое направления) или по спиралям и т.п. Кроме того, буквы шифротекста могут записываться в виде различных геометрических фигур или любыми другими способами. Один из них состоит в двойном шифровании путем повторной перестановки столбцов. При этом и в первом и во втором блоках перестановки может быть использовано одно и то же ключевое слово, хотя лучше использовать разные ключевые слова. Такой шифр, называющийся двойной перестановкой, получил широкое распространение в XX в.

КОД ПРОГРАММЫ

ДРОБЛЕНИЕ

Третьим основным алгоритмом шифрования является дробление. При этом каждой букве открытого текста сопоставляется более одного символа шифротекста, после чего символы перемешиваются (переставляются) в определенном порядке. Ниже приведена система, демонстрирующая процедуру дробления с использованием знаменитого шифра Bifid, авторство которого приписывается французскому криптографу Феликсу Мари Деластелю.

Сначала составляется шифровальная таблица размером 5x5 (по аналогии с квадратом Полибия), куда построчно вписывается шифровальный алфавит, ключевая фраза, причем ради того, чтобы общее число букв алфавита не превышало 25, буква J опускается (поскольку эта буква, с одной стороны, мало употребительна в английских текстах, а с другой — вполне может быть заменена буквой I без какого либо урона для смысла).

Далее в процессе шифрования под каждой буквой открытого текста в столбик записываются ее табличные координаты – номер строки и номер столбца. Затем получившаяся цифровая последовательность переводится с помощью той же таблицы обратно в буквенную форму, но на этот раз она читается уже в строчку. При таком шифровании координата строки и координата столбца у каждой буквы оказываются разъединенными, что характерно именно для раздробляющего шифра.

КОД ПРОГРАММЫ

УЧЁНЫЕ

- Леон Баттиста Альберти
- Джироламо Кардано
- Томас Джефферсон
- Алан Тьюринг
- Клод Шеннон
- Мартин Хеллман
- Владимир Александрович Котельников
- Иван Яковлевич Верченко

Леон Баттиста Альберти

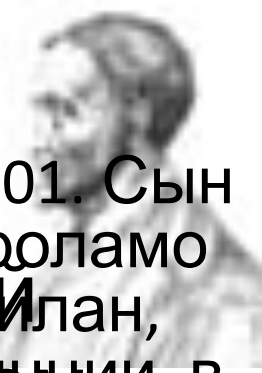
Леон Баттиста Альберти — незаконорожденный отпрыск влиятельного флорентийского куп[illegible]ческого рода Альберти родился 14 февраля 1404 года в Генуе. Образование получил в Падуе в школе педагога-гуманиста Гаспарино Баррицы, где познакомился с древними языками и математикой, и в Болонском университете, где изучал каноническое право, греческую литературу и философию. Сочинил ряд литературных произведений.

По окончании университета в 1428 несколько лет провел во Франции, побывал в Нидерландах и Германии. В 1432 вернулся в Италию и получил должность абревиатора (секретаря) римской курии. После восстания в Риме в конце мая – начале июня 1434 вслед за папой Евгением IV бежал во Флоренцию .

Вернулся в Рим после реставрации папской власти в сентябре 1443; с того времени главным объектом его научных интересов стали архитектура и математика. Написал в середине 1440-х *Математические забавы*, в который затронул ряд проблем физики, геометрии и астрономии, а в начале 1450-х свою работу *Десять книг о зодчестве*, где обобщил античный и современный опыт. Позже составил трактат *О принципах составления кодов* – первый научный труд по криптографии. Выступил как архитектор-практик.

Умер в Риме в 1472.

Джироламо Кардано



Джироламо Кардано родился в Павии 24 сентября 1501. Сын Фацио Кардано, известного адвоката. В 1526 Джероламо окончил Падуанский университет. Вернулся в Милан, читал лекции по математике. Практиковал в провинции, в 1539 был принят в Коллегию врачей.

Книга Кардано *«О тонких материях»* служила популярным учебником по статике и гидростатике вплоть до XVII в.

Кардано был страстным любителем азартных игр. «Побочным продуктом» его любви к игре в кости стала книга *«Книга об азартных играх»*, в которой он заложил основы теории вероятности, формулировку закона больших чисел, некоторые вопросы комбинаторики. Труд Кардано *«Великое искусство»* стал крупным вкладом в развитие современной алгебры.

В 1562 Кардано был назначен профессором в Болонью, где в 1570 его арестовала инквизиция. Остаток жизни провел в Риме, пытаясь добиться прощения.

Умер Кардано в Риме 21 сентября 1576.

Кардано изобрел шифр, называемый решеткой, или трафаретом, в котором секретное послание оказывалось скрыто внутри более длинного и совершенно невинно выглядевшего открытого текста. Секретное сообщение можно было обнаружить, наложив открытый текст лист пергаментной бумаги с прорезями (трафарет). Слова, появлявшиеся в прорезях, и составляли секретное послание.

Томас Джефферсон

Томас Джефферсон родился 13 апреля 1743 года в семье богатого землевладельца. Получив в детстве разностороннее образование, Джефферсон уже в юные годы приобрел широкую известность в своей родной колонии Виргинии. В 26-летнем возрасте он был избран депутатом Виргинской законодательной ассамблеи. Джефферсон выступал активным участником освободительного движения колоний, вылившегося в войну за независимость США 1775-1783 гг. В 1775 г. Он был избран депутатом Континентального конгресса, принявшего впоследствии решение об отделении североамериканских колоний от Англии. В 1776-1779 гг. он член законодательного собрания Виргинии, входил в состав комиссии по пересмотру законов штата. В 1779-1781 гг. он занимал пост губернатора Виргинии. В 1790-1793 гг. — находился на посту государственного секретаря в первом правительстве Джорджа Вашингтона. В 1796 г. он был избран вице-президентом, а затем в 1800 и 1804 гг., - президентом США. Джефферсон скончался на 89-м году жизни 4 июля 1826 г.

В 90-х годах XVIII века Томас Джефферсон изобрел изящное шифровальное устройство – «цилиндр Джефферсона». Это устройство состояло из 25 – 36 вращаемых дисков, закрепленных на общей оси. На каждый диск была нанесена своя (причем перемешанная) алфавитная последовательность. При шифровании текст разбивался на группы, длина которых соответствовала числу используемых дисков. Каждая группа открытого текста устанавливалась на цилиндре в ряд (в одну строку), а в качестве шифротекста выбирался любой из остальных 25 рядов. Дешифровщик совершал ту же процедуру, но в обратном порядке: на цилиндре поочередно устанавливалась в ряд каждая группа шифротекста, после чего просматривались остальные 25 рядов с целью определить, какой из них содержит открытый текст. Этот тип шифра, в свое время являвшийся одной из лучших криптографических систем, называется мультиплексной системой.

Такие устройства применялись до конца Второй Мировой войны.

Алан Тьюринг

[illegible]

Клод Шеннон

Клод Эльвуд Шеннон родился в Петоски, штат Мичиган, 30 апреля 1916 года. Его отец был бизнесменом, а мать — учителем.

Первые 16 лет своей жизни Клод провел в Гэйлорде, окончив местную школу в 1932 году и показав при этом склонность к механике.

В 1932 он поступил в университет Мичигана. В 1936 он стал бакалавром по электротехнике и математике.

В 1936 он получил должность лаборанта на отделении электротехники в Массачусетском Технологическом Институте.

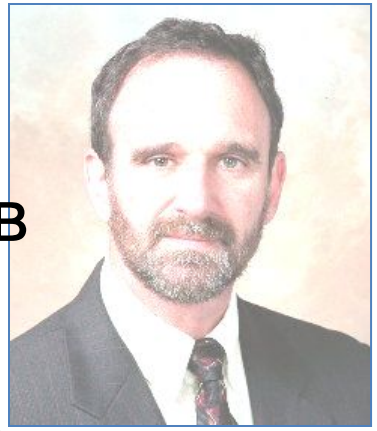
Он изучал символическую логику и булеву алгебру на математических курсах в Мичигане и понимал, что это именно то, что требуется для описания бинарных систем. Он развил эти идеи в 1937 году, будучи в Нью-Йорке в Лабораториях Белла и затем, вернувшись, в своей дипломной работе в Массачусетсе.

Весной 1940 года он защитил диссертации и получил звания магистра электротехники и доктора математики. Все эти годы Шеннон работал в различных областях, главным образом - в теории информации, началом которой послужила его статья "Математическая теория связи". Занятия Шеннона проблемами информации и шума имели множество различных приложений. К примеру, в статье "Теория защищенной связи" он связал криптографию с проблемой передачи информации по зашумленному каналу (роль шума в этом случае играет ключ криптосистемы). Эта работа привела в дальнейшем к тому, что Шеннон был назначен консультантом Правительства США по вопросам криптографии.

Ему были присуждены почетные степени университетов Уэйла (магистр, 1954), Мичигана (1961), Принстона (1962), Эдинбурга (1964), Питтсбурга (1964), Оксфорда (1978), а также ряда других, а кроме того - множество научных наград и медалей.

Клод Шеннон умер 24 февраля 2001 года в возрасте 84 лет.

Мартин Хеллман



Мартин Хеллман — американский криптограф, один из основоположников теории асимметричных криптосистем.

Получил степень бакалавра в Нью-Йоркском университете (1966), степень магистра (1967) и доктора философии (1969) в Стэнфордском университете.

После работы в Уотсоновском исследовательском центре IBM и МИТ, в 1971 г. вернулся в Стэнфорд, где преподавал и занимался исследованиями до 1996 г.

В 1976 г. в соавторстве с Мерклем и Диффи изобрёл первую асимметричную криптосистему.

Автор 5 патентов США. Один из активных сторонников либерализации в сфере криптографии.

Владимир Александрович Котельников

После возвращения в Москву из эвакуации в 1943 году

Умер в Москве в 2005 году.

Иван Яковлевич Верченко

Иван Яковлевич Верченко родился 11 сентября 1907 года в Щорсе в семье работника электрика. Окончив в 1924 году школу, Иван продолжил учебу в ... заводе, получив квалификацию ... работал на динамитном заводе, где в результате неожиданного взрыва лишился ... правой руки. Карьера ... химика ... Самостоятельно подготовившись, в 1929 году он поступил на мехмат МГУ, где его способности были замечены академиком А. Н. Колмогоровым, под руководством которого он впоследствии защитил сначала дипломную работу, а затем и кандидатскую диссертацию в области теории функций.

Война застала его в Ростовском университете. Будучи ... докторской диссертации ... году привлекла к ... Ивану Яковлевичу ... Специалисты ... в результате оказался в знаменитой «Марфинской шарашке». Работая там, он внес существенный вклад в разработку принципов криптографической защиты телефонной аппаратуры, однако в 1953 году был уволен Лаврентием Берия.

В течение длительного времени Верченко читал лекции в МГУ, руководил кафедрой математического анализа в МГПИ имени В. П. Потемкина. За время руководства 4-м факультетом ВКШ И. Я. Верченко был награжден орденом Трудового Красного знамени, избран членом-корреспондентом Российской Академии образования. Под его руководством был составлен новый пятилетний учебный план.

Умер в 1995 году.

Программы на языке Delphi

ПРОСТАЯ ЗАМЕНА

КОД ПРОГРАММЫ

ПЕРЕСТАНОВКА

КОД ПРОГРАММЫ

ДРОБЛЕНИЕ

КОД ПРОГРАММЫ

КОНЕЦ

ВЕРНУТЬСЯ

ВЫЙТИ