

КРИПТОГРАФИЯ

Азы шифрования

и

история развития

Содержание

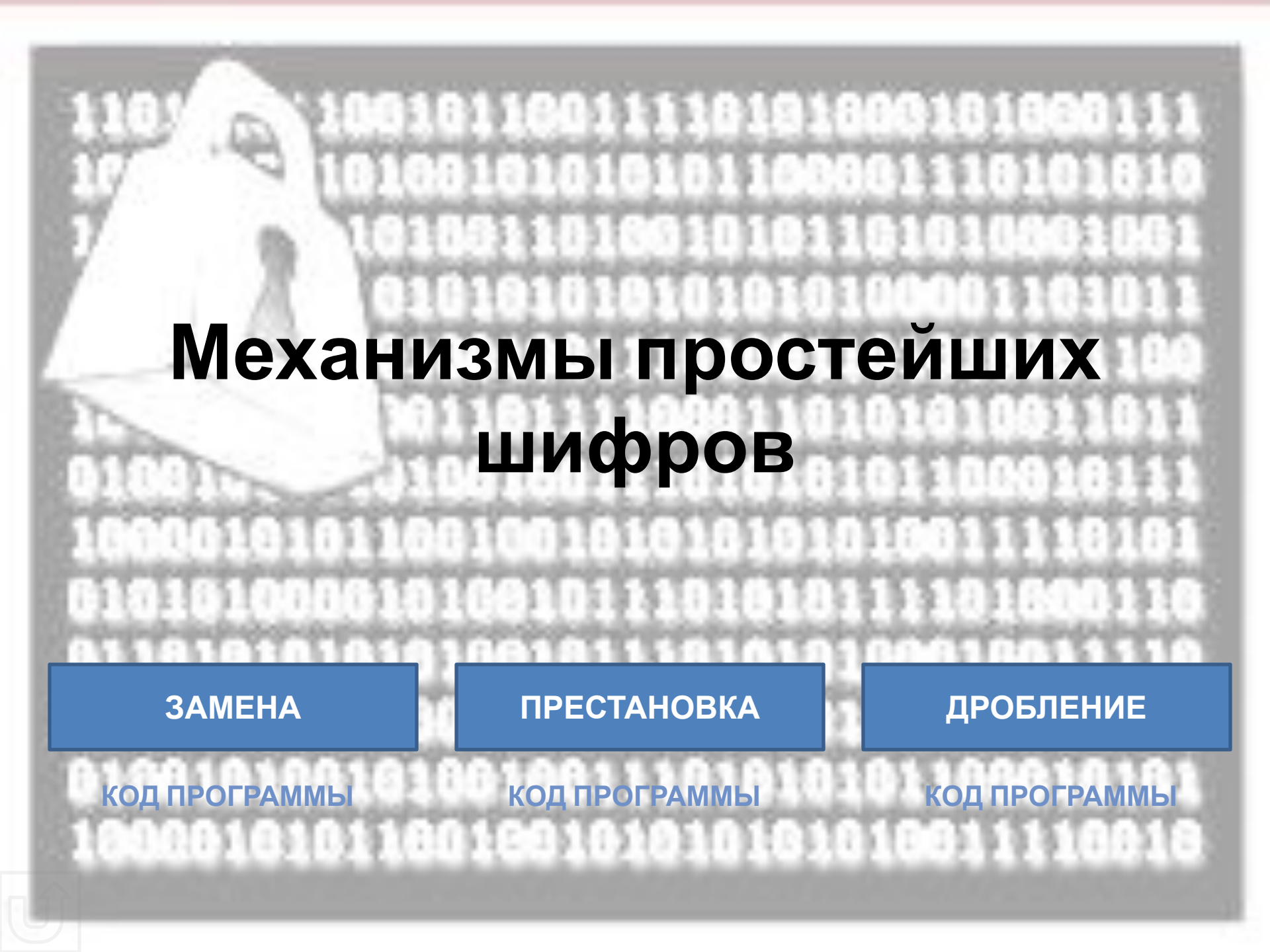
- Ведение
- Механизмы простейших шифров
 - замена
 - перестановка
 - дробление
- Учёные
 - Леон Баттиста Альберти
 - Джироламо Кардано
 - Томас Джефферсон
 - Алан Тьюринг
 - Клод Шеннон
 - Мартин Хеллман
 - Владимир Александрович Котельников
 - Иван Яковлевич Верченко
- Программы на языке Delphi

Введение

КРИПТОГРАФИЯ, или криптология, наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочесть 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.



The image features a white padlock on the left side, set against a dark grey background filled with a pattern of white binary code (0s and 1s). The title 'Механизмы простейших шифров' is centered in a large, bold, black font.

Механизмы простейших шифров

ЗАМЕНА

КОД ПРОГРАММЫ

ПРЕСТАНОВКА

КОД ПРОГРАММЫ

ДРОБЛЕНИЕ

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.



ПЕРЕСТАНОВКА

В шифре Мере перестановки все буквы открытого текста остаются без изменений, но можно набрать и другие «маршруты» перестановки. Например, можно использовать ключ, управляющий процедурой шифрования. Ключевое слово может быть использовано для получения шифровой ципраги и последовательности букв путем нумерации букв ключевого слова (относительно друг друга) в порядке их следования слева направо в стандартном алфавите. Далее, под цифровой последовательностью в перестановке ставятся буквы. При этом в первом и 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.

ДРОБЛЕНИЕ

Третьим составляющим алгоритма является процесс шифрования под каждой буквой открытого текста в бинарном виде. Каждой букве открытого текста сопоставляется ее двоичное представление – более одного символа. В результате, после шифрования, символы перемещаются (переставляются) последовательно, не переводится в определенный порядок. Выведена таблица, обратная в буквенную форму. Эта формула используется для разложения строки исходного сообщения, которая читается уже в строку. При таком шифровании координата строки и координата столбца каждой буквы Феликсу Мари Деластелю указывались сразу единственными, 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 — незаконнорожденный отпрыск Вернувшись в Рим после реставрации папской власти в сентябре 1443; с того времени Альберти жил в Риме до февраля 1454 года в Генуе. главным объектом его научных интересов образование получил в Падуе в школе педагога-стади архитектура и математика. Написал в гуманиста Гаспарино Баррицы, где познакомился с Середины 1440-х *Математические забавы*. В древними языками и математикой, и в Болонском университете, где изучал каноническое право, геометрии и астрономии, а в начале 1450-х греческую литературу и философию. Сочинил ряд свою работу *Десять книг о зодчестве*, где литературных произведений, обобщил античный и современный опыт. По окончании университета в 1428 несколько лет провел во Франции, побывал в Нидерландах и Германии. В 1432 вернулся в Италию и получил должность криптографа. Выступил как архитектор аббревиатора (секретаря) римской курии. После восстания в Риме в конце мая — начале июня 1434 умер в Риме в 1472. вслед за папой Евгением IV бежал во Флоренцию.



Джироламо Кардано



Джироламо Кардано родился в Павии 24 сентября 1501. Сын Фацио Кардано, известного адвоката. В 1526 Джироламо Кардано 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 сокрыто внутри более длинного и

совершенно невинно выглядевшего Кардано был страстным любителем азартных игр. «Побочным продуктом» его любви к игре в кости стала книга, в которой он обнаружил теорию вероятности, формулировку закона больших чисел, некоторые вопросы комбинаторики. Труд Кардано «*Бумаги с прорезями*» (трафарет) слова, появлявшиеся в прорезях, и составляли

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.



Томас Джефферсон



Томас Джефферсон родился 13 апреля 1743 года в семье плантатора в штате Вирджиния. Он учился в колледже Вильгельма и Мэри в Вирджинии, а затем в университете Вирджинии. В 1773 году он был избран депутатом Вирджинской законодательной ассамблеи. Джефферсон выступал активным участником освободительного движения колоний, используя 25 дисков. Каждая группа открытого текста выдвигалась в ряд (в одну строку), а 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. Джефферсон избран вице-президентом США в 1796 году, а затем в 1800 и 1804 гг., - президентом США. Джефферсон скончался на 89-м году жизни 4 июля 1826 г.



Клод Шеннон



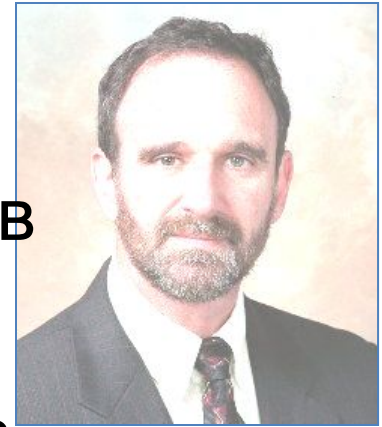
Весной 1940 года он защитил диссертацию и получил звание магистра электротехники и доктора математики. Все эти годы Шеннон работал в различных областях, главным образом - в теории информации, началом которой послужила его статья "Математическая теория связи", окончив местную школу в 1932 году и показав при этом занятия Шеннона проблемами информации и шума имели множество различных приложений. К примеру, в статье

В 1932 он поступил в университет Мичигана. В 1936 он стал бакалавром по электротехнике и математике (род шумов в шумном случае истрабагрантосидевыи). Эта работа привела в дальнейшем к тому, что Шеннон был назначен консультантом Института Исследования США по вопросам криптографии и булеву алгебру на

Ему были присуждены курсы в Мичигано и университете Эйла (майер, 1954), Мобетая дгуопитраня биа (1962), Эдибура. (Образвиттебуридеи 1964), 30 кодор будучи 1970), Наю также ряд ддуви, Лабораториях Беллаже за вем, вернувшись и сад в своей дипломной работе в Массачусетсе.

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.



Иван Яковлевич Верченко



Иван Яковлевич Верченко родился в семье ткачей в селе Бручи
Вятской губернии. В 1907 году окончил гимназию в Костроме.
Окончил механический факультет Московского университета в
1912 году, затем работал в МГУ, в 1914 году переехал в Ленинград
на работу в завод «Механика», где в 1915 году окончил курсы
инженеров-механиков. В 1916 году переехал в Москву, где в
результате работы в Механике был избран членом Московского
университетского комитета. В 1917 году переехал в Петроград,
где в 1918 году был избран членом Петроградского совета.
В 1919 году переехал в Москву, где в 1920 году был избран
доктором наук. В 1921 году переехал в Ленинград, где в
1922 году был избран членом Ленинградского совета. В 1923 году
переехал в Москву, где в 1924 году был избран членом
Самаркандской Академии образования. В 1925 году он
стал руководителем кафедры математики в Московском
университете, где его способности были
замечены академиком А. Н. Колмогоровым, под
руководством которого он в 1926 году разработал
принципы криптографической защиты телеграфной
аппаратуры, а затем кандидатскую диссертацию в области
теории функций. В 1953 году был уволен
Лаврентием Берия.



Программы на языке Delphi

ПРОСТАЯ ЗАМЕНА

КОД ПРОГРАММЫ

ПЕРЕСТАНОВКА

КОД ПРОГРАММЫ

ДРОБЛЕНИЕ

КОД ПРОГРАММЫ



КОНЕЦ

ВЕРНУТЬСЯ

ВЫЙТИ