Криптография

Криптография как наука

Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — это наука о:

- методах обеспечения конфиденциальности (невозможности прочтения информации посторонним);
- целостности данных(невозможности незаметного изменения информации);
- аутентификации (проверки подлинности авторства или иных свойств объекта);
- невозможности отказа от авторства.

Историческая периодизация

Историческая периодизация

В истории развития криптографии можно выделить 4 этапа:

- Наивная криптография.
- Формальная криптография.
- Научная криптография.
- Компьютерная криптография.

Историческая периодизация. Наивная криптография

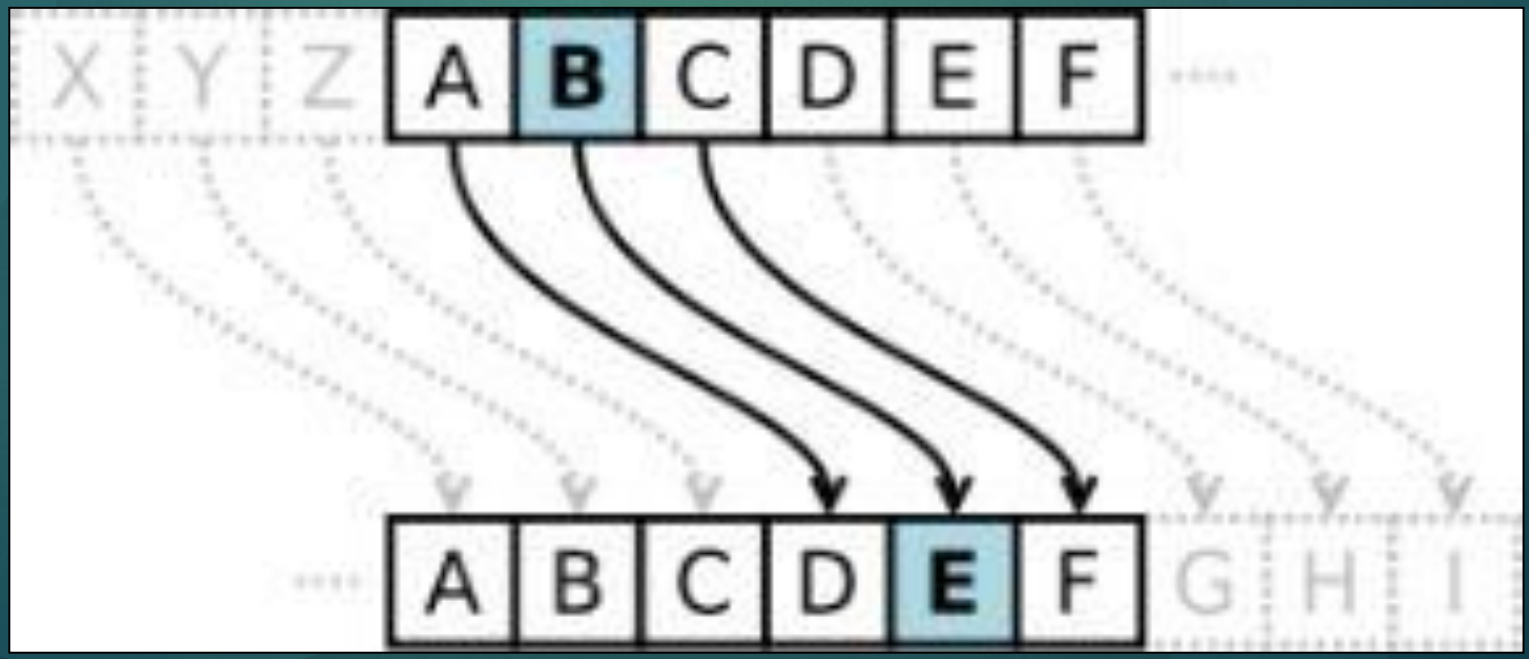
- Для наивной криптографии (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания передаваемых сообщений.
- Шифровальные системы сводились к использованию перестановки или замены букв на различные символы (другие буквы, знаки, рисунки, числа и т.п.).

Наивная криптография. Скитала

- Достоверно известно, что скитала использовалась в войне Спарты против Афин в конце V века до н. э.
- Скитала представляла собой длинный стержень, на который наматывалась лента из пергамента. На ленту наносился текст, так, что после разматывания текст становился нечитаемым. Для его восстановления требовалась скитала такого же диаметра.

Наивная криптография. Шифр Цезаря

- Цезарь использовал в переписке моноалфавитный шифр, вошедший в историю как Шифр Цезаря.
- В шифре Цезаря каждая буква алфавита циклически сдвигается на определённое число позиций. Величину сдвига можно рассматривать как ключ шифрования.
- Сам Цезарь использовал сдвиг на три позиции.



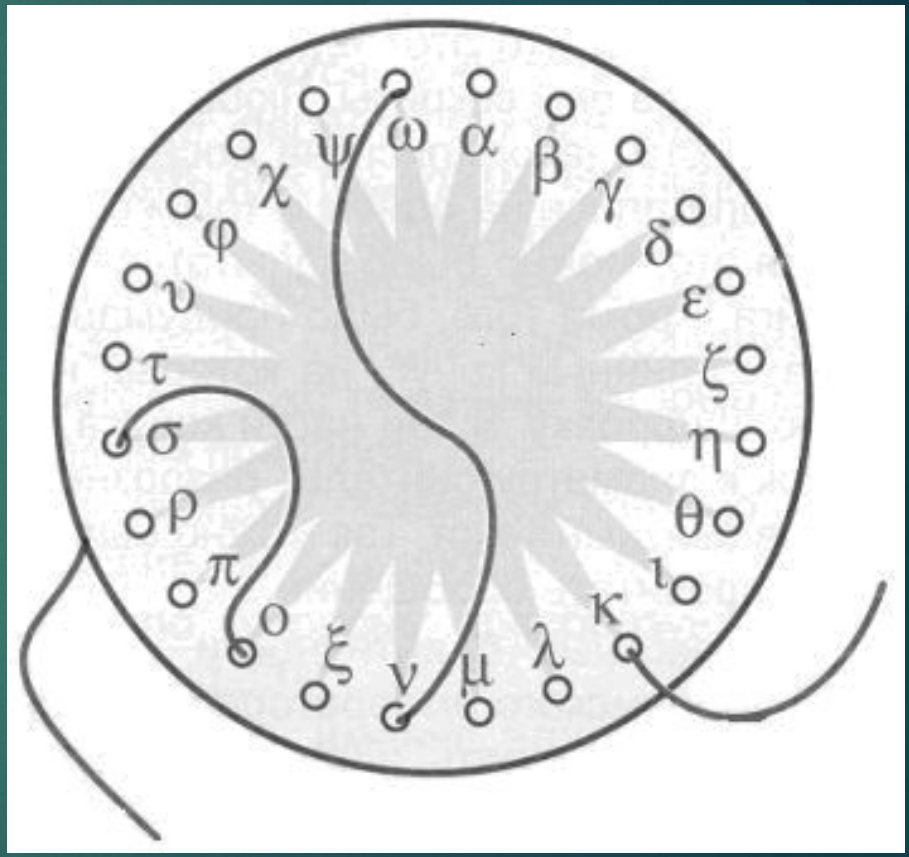
Наивная криптография. Квадрат Полибия

- Во II веке до н. э. в Древней Греции был изобретён квадрат Полибия.
- В нём буквы алфавита записывались в квадрат 5 на 5, после чего с помощью оптического телеграфа передавались номер строки и столбца, соответствующие символу исходного текста (на каждую букву приходилось два сигнала: число факелов обозначало разряд буквы по горизонтали и вертикали)

	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Y
5	Φ	X	Ψ	Ω	

Наивная криптография. Диск Энея

- Диск Энея — диск диаметром 10-15 см с отверстиями по числу букв.
- Для записи сообщения нитка протягивалась через отверстия в диске, соответствующие буквам.
- При чтении получатель вытягивал нитку, и получал сообщение в обратном порядке.
- Если недоброжелатель перехватит диск, Эней предусмотрел способ быстрого уничтожения сообщения — для этого достаточно выдернуть нить, закреплённую на катушке в центре диска.



Наивная криптография. Линейка Энея

- Использовалась линейка с отверстиями по числу букв алфавита, катушкой и прорезью.
- Для шифрования нить протягивалась через прорезь и отверстие, после чего на нити завязывался очередной узел.
- Для дешифрования необходимо было иметь саму нить и линейку с аналогичным расположением отверстий.
- Таким образом, даже зная алгоритм шифрования, но не имея ключа (линейки), прочитать сообщение было невозможно.

Историческая периодизация. Формальная криптография

- Этап формальной криптографии (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации.

- К концу XIV в. между итальянскими городами-государствами в переписке уже применялись **«номенклаторы»** лат. nomen — «имя» и calator — «раб», «слуга»). Они состояли из кодовых обозначений для слогов, слов и имен, а также алфавитов шифрозамен.

Формальная криптография. Л. Б. Альберти

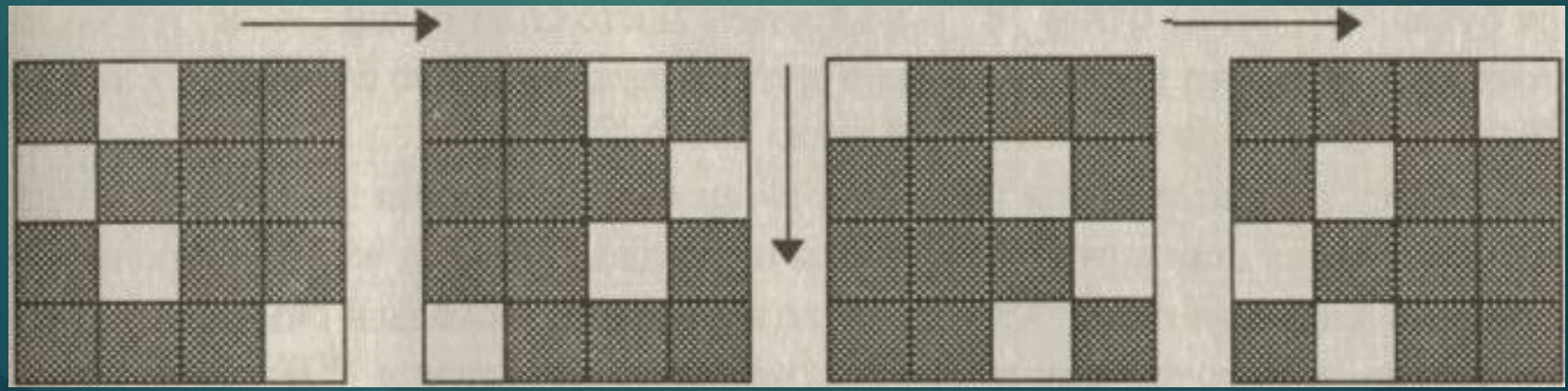
- Отцом криптографии называют Леона Баттисту Альберти.
- Его «Трактат о шифре» 1466 г. считается первой научной работой по криптографии.
- Он предложил вместо единственного секретного алфавита, как в моноалфавитных шифрах, использовать два или более, переключаясь между ними по какому-либо правилу.
- Однако флорентийский учёный так и не смог оформить своё открытие, что было сделано Блезом Вижинером.

Формальная криптография. Иоганн Трисемус

- Другой печатной работой, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, является труд «Полиграфия» (1518 г.) немецкого аббата Иоганна Трисемуса (Тритемия).
- Он же первым заметил, что шифровать можно и по две буквы за раз - биграммами (хотя первый **биграммный шифр** Playfair был предложен лишь в XIX веке).

Формальная криптография. Решетка Кардано

- В 1550 г. итальянский математик Джероламо Кардано предложил новую технику шифрования - решётку Кардано.
- Этот способ сочетал в себе как искусство скрытого письма, так и криптографию.
- Затруднение составляло даже понять, что сообщение содержит зашифрованный текст, а расшифровать его, не имея ключа (решётки) в то время было практически невозможно.
- Решётку Кардано считают первым **транспозиционным шифром**, или, как ещё называют, геометрическим шифром.



Формальная криптография. Роторные криптосистемы.

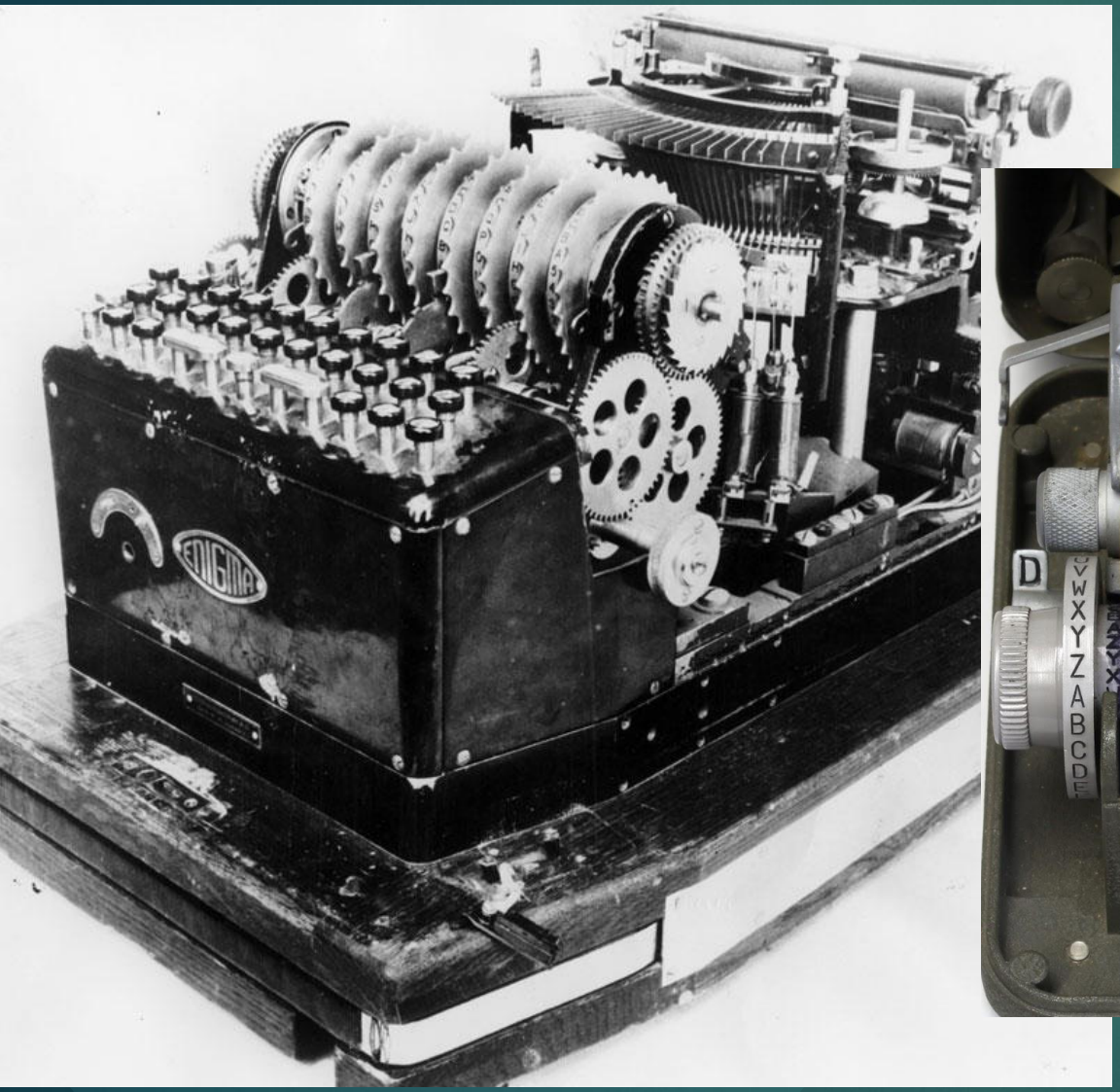
- Одной из первых подобных систем стала изобретенная в 1790 году Томасом Джефферсоном, будущим президентом США механическая машина.
- Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «прошитую» в нем подстановку.

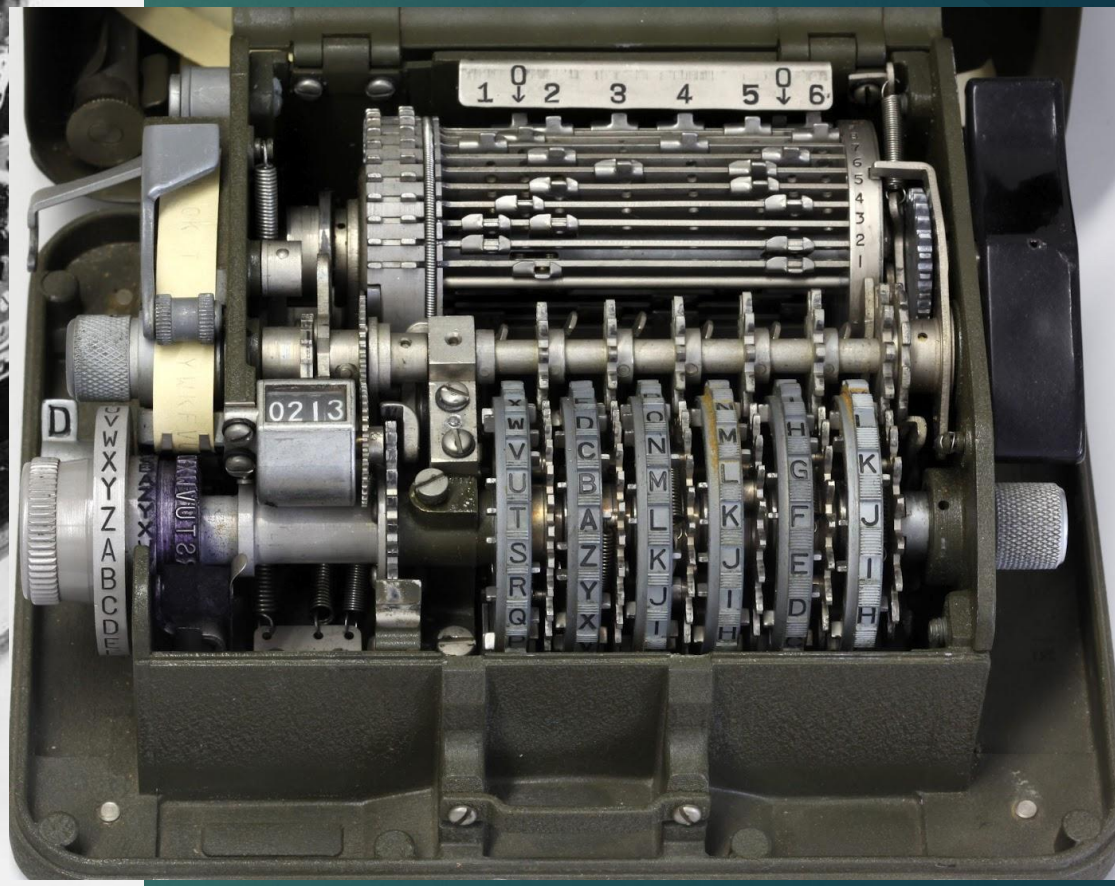
Историческая периодизация. Научная криптография

- **Научная криптография (1930 – 60-е гг.)** – появление криптосистем со строгим математическим обоснованием криптостойкости.
- К началу 1930-х годов окончательно сформировались разделы математики, являющиеся основой для будущей науки: общая алгебра, теория чисел, теория вероятностей и математическая статистика.

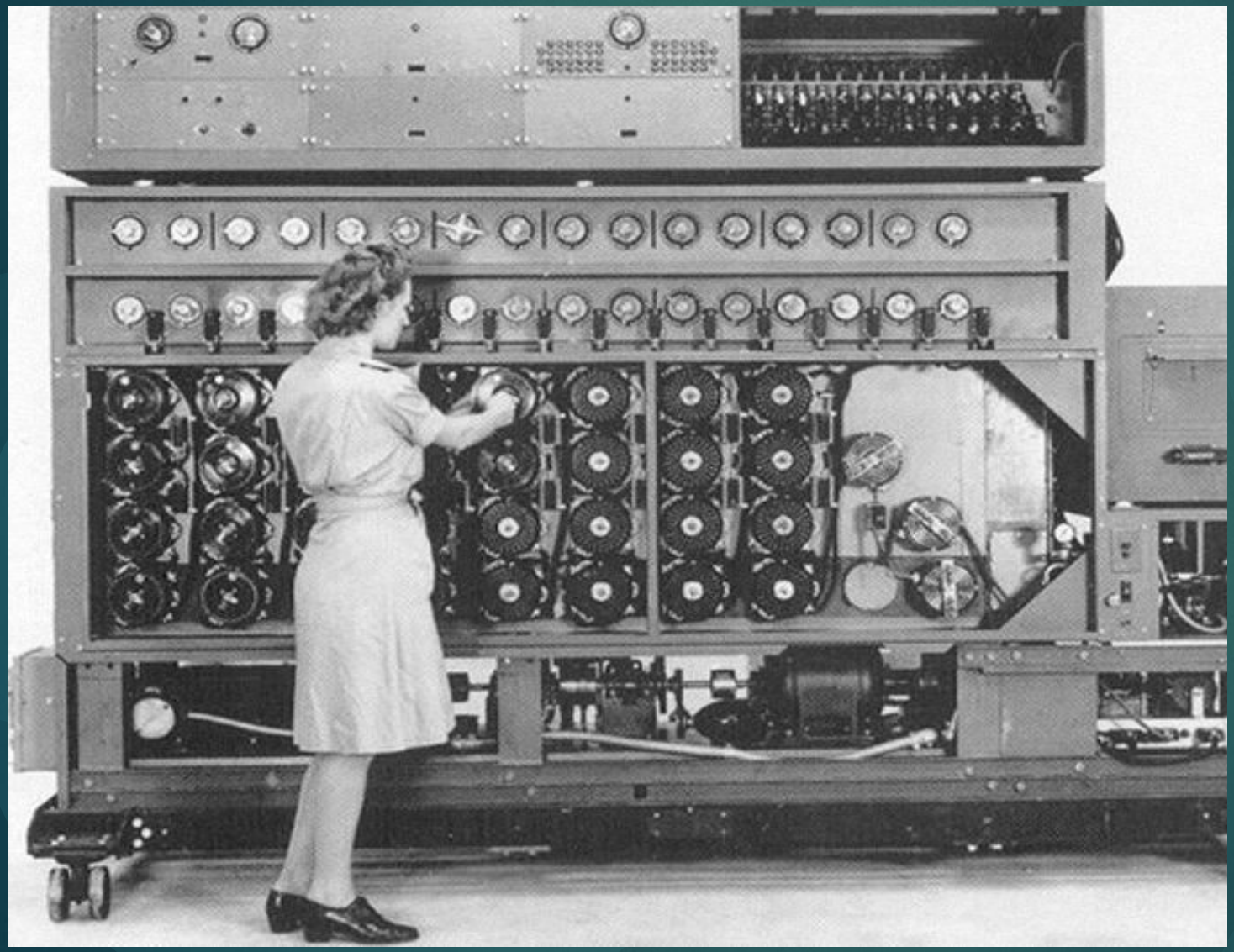
Научная криптография. Шифрующие устройства.

- Перед началом Второй мировой войны ведущие мировые державы имели электромеханические шифрующие устройства.
- Эти устройства делились на два типа - шифровальные машины и машины на цевочных дисках.
- К первому типу относят **«Энигму»**, использовавшуюся войсками Германии и её союзников, второго типа - американская **М-209**.
- В СССР производились оба типа машин.


ENIGMA


0213

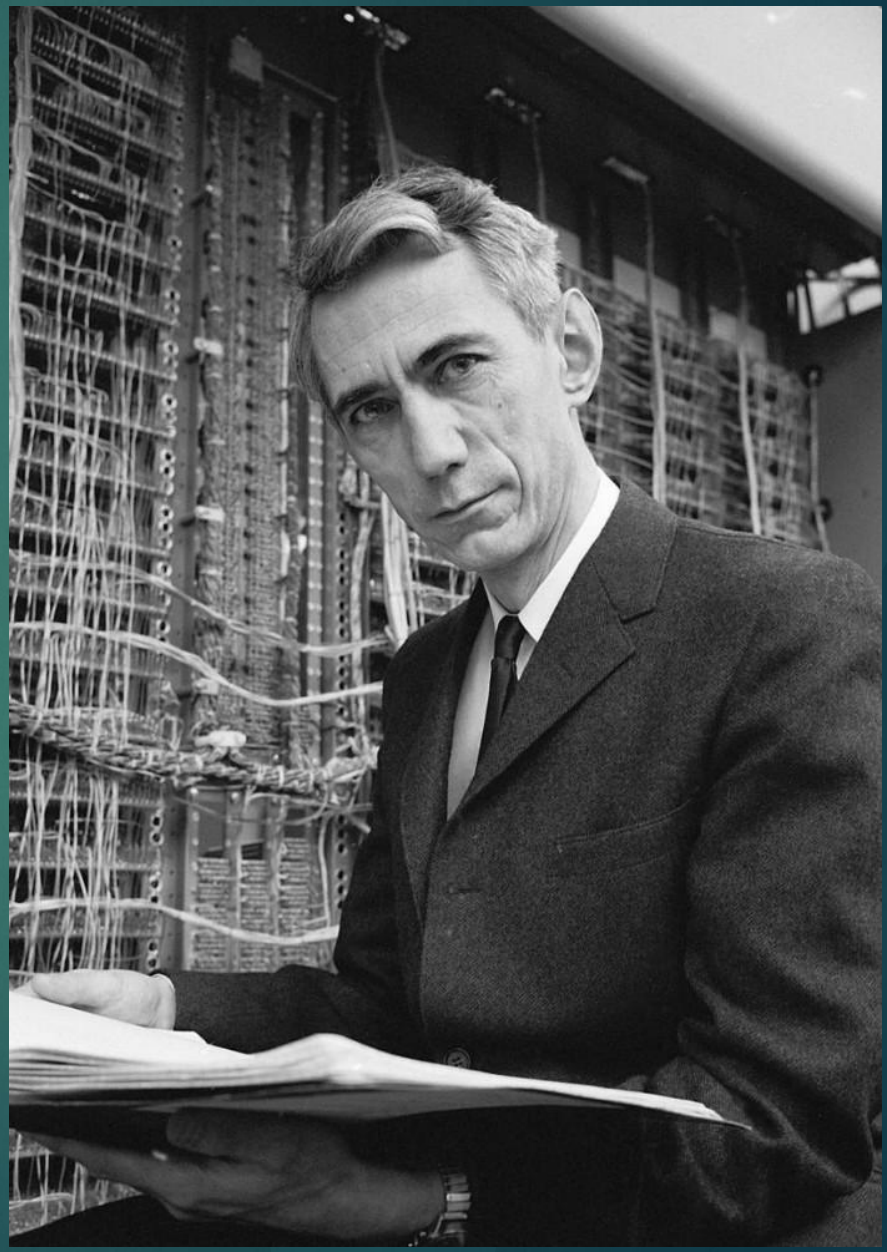
Turing Bombe — электронно-механическая машина для расшифровки кода «Энигмы».



- состояла из 108 вращающихся электромагнитных барабанов:
- 10 футов (3,0 м) длиной;
- 7 футов (2,1 м) высотой;
- 2 фута (0,61 м) шириной;
- весила 2,5 тонны.

Научная криптография. Клод Шеннон.

- Своеобразным водоразделом стала работа Клода Шеннона "Теория связи в секретных системах" (1949), которая подвела научную базу под криптографию и криптоанализ.
- Этап развития криптографии и криптоанализа до 1949 г. стали называть донаучной криптологией.
- Шеннон ввел понятия "**рассеивание"** и "**перемешивание**", обосновал возможность создания сколь угодно стойких криптосистем.



Историческая периодизация. Компьютерная криптография

- Компьютерная криптография (с 1970-х гг.) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры.
- Первым классом криптосистем, практическое применение которых стало возможно с появлением мощных и компактных вычислительных средств, стали блочные шифры.

Компьютерная криптография. DES.

- В 70-е гг. был разработан американский **стандарт шифрования DES** (принят в 1978 г.). Один из его авторов, Хорст Фейстель (сотрудник IBM), описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе отечественный стандарт шифрования ГОСТ 28147–89.
- С появлением DES обогатился и криптоанализ, для атак на американский алгоритм был создано несколько новых видов криптоанализа (линейный, дифференциальный и т. д.), практическая реализация которых опять же была возможна только с появлением мощных вычислительных систем.

Компьютерная криптография. Ассиметричные криптосистемы.

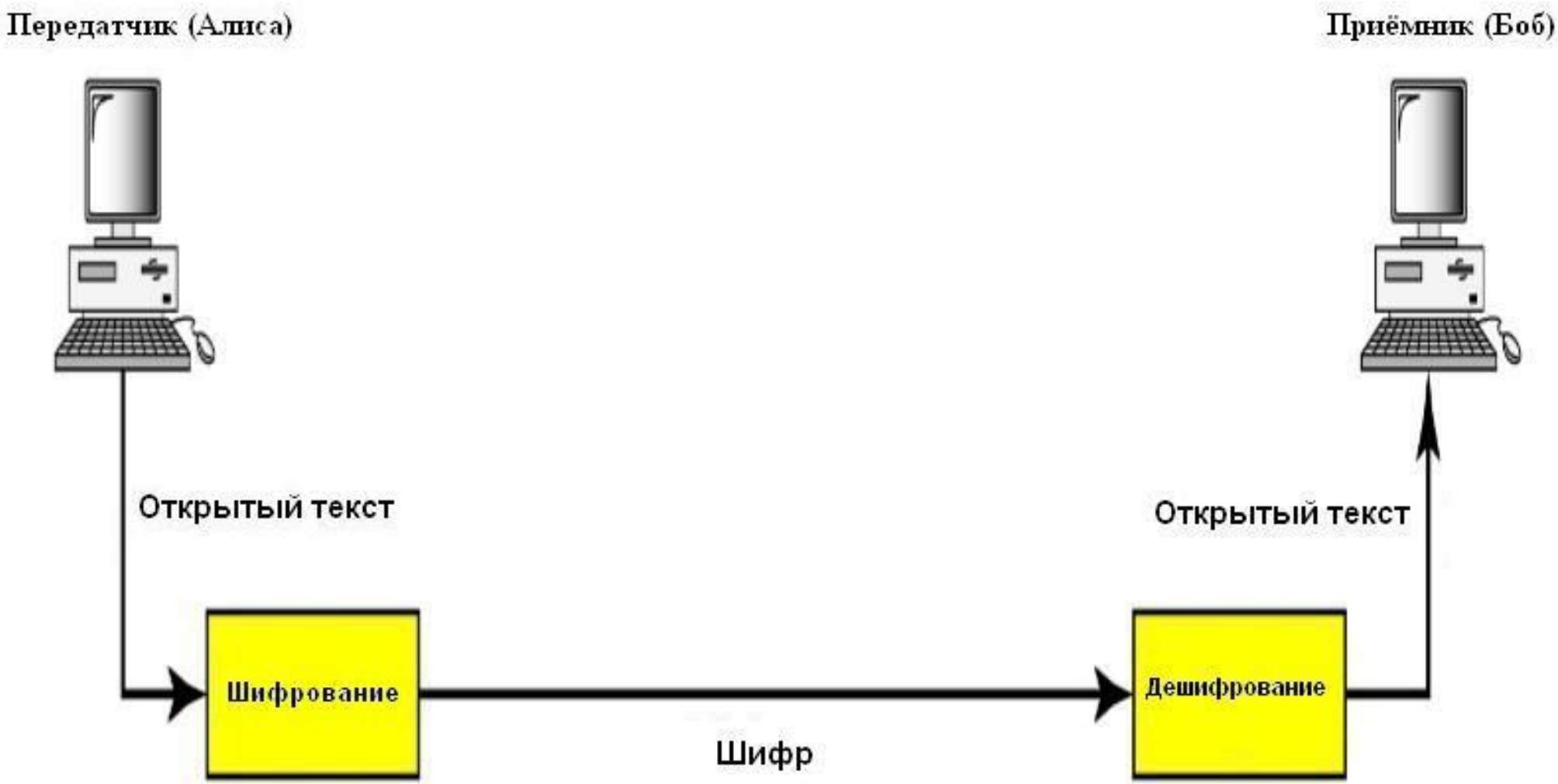
- В середине 70-х гг. XX в. появились асимметричные криптосистем, которые не требовали передачи секретного ключа между сторонами.
- Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 г. "Новые направления в современной криптографии".
- В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом.
- Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме факторизации больших простых чисел.

Компьютерная криптография. Ассиметричные криптосистемы.

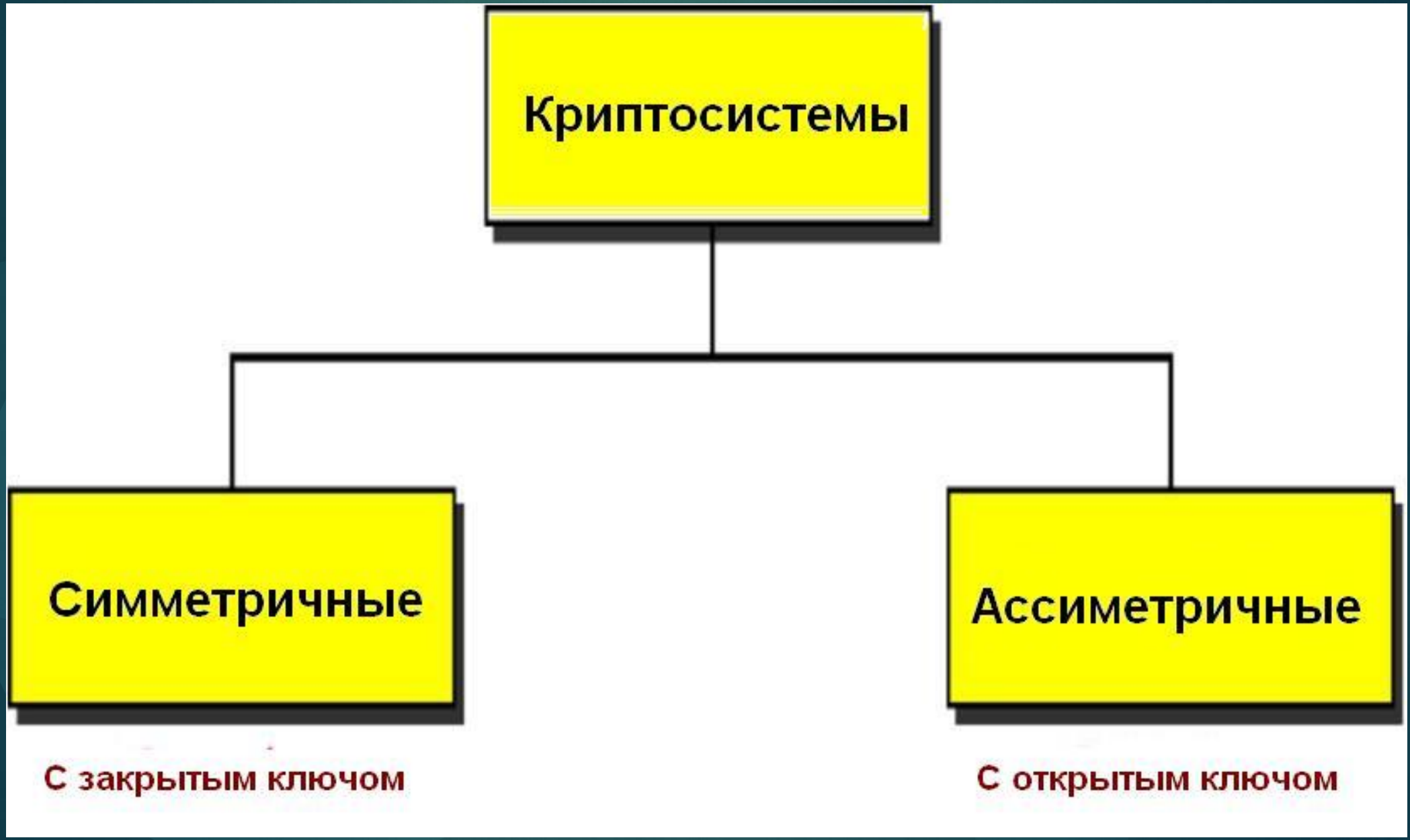
- Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности системы электронной цифровой подписи (ЭЦП) и электронных денег.
- В 1980–90-е гг. появились совершенно новые направления криптографии:
- вероятностное шифрование,
- квантовая криптография и другие.
- В этот же период были разработаны нефейстелевские шифры (SAFER, RC6 и др.), а в 2000 г. после открытого международного конкурса был принят новый национальный стандарт шифрования США – DES.

Категории криптографии

Основная схема криптографии



Категории криптографии

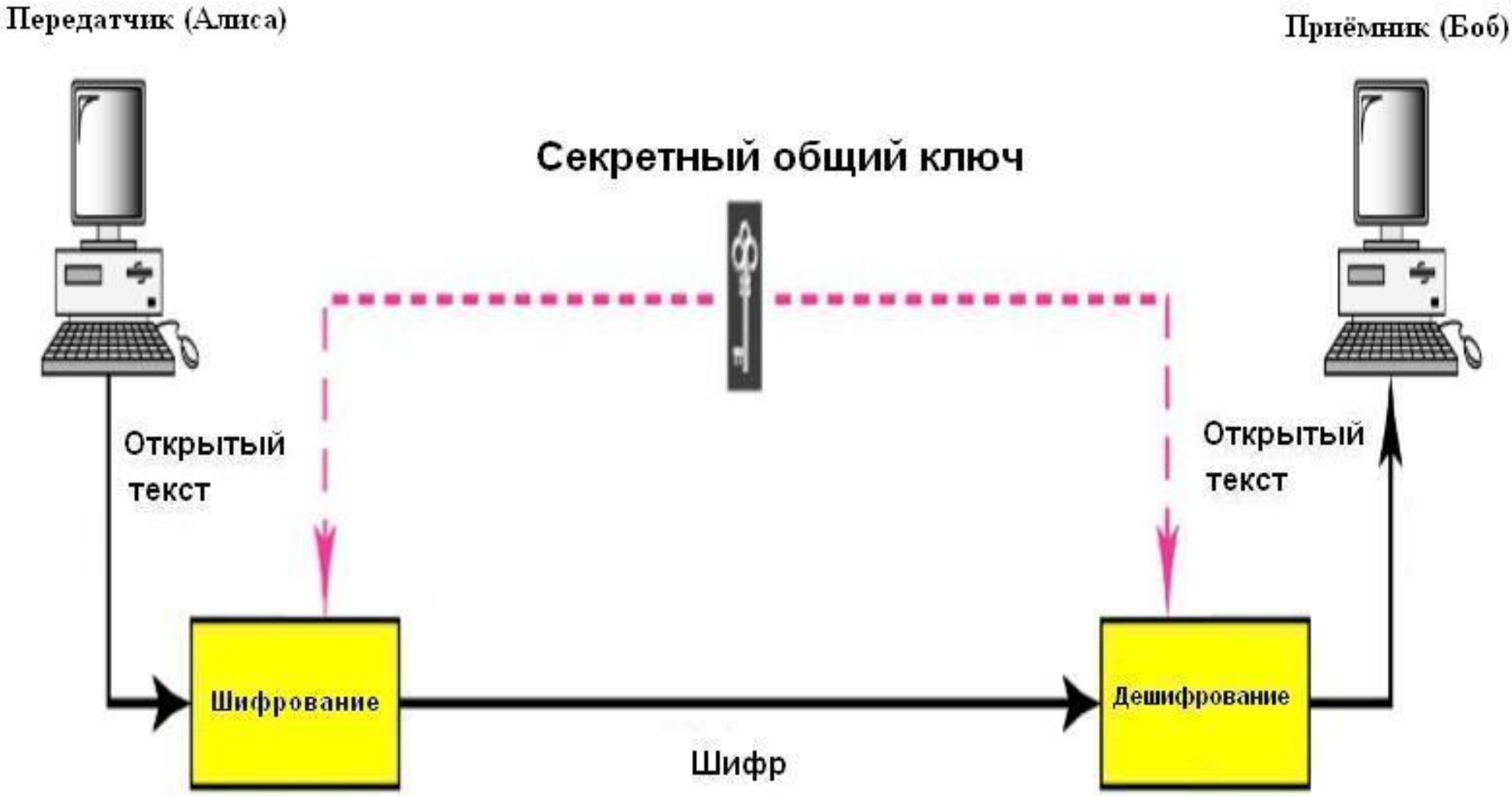


Ключи, используемые в криптографии

Симметричные криптосистемы

Асимметричные криптосистемы

Симметричные криптосистемы



Симметричные криптосистемы. Особенности

- Для шифрования и дешифрования используется ***общий ключ.***
- И передатчик, и получатель должны знать общий ключ.
- Общий ключ должен быть передан по второму секретному каналу связи.
- Создание и передача длинного секретного ключа.
- Непрактичны для большого числа передатчиков и получателей.

Известные симметричные криптосистемы

- Известные симметричные криптосистемы с : DES, AES.
- DES: разработан фирмой IBM для правительства США. Национальный стандарт шифрования США в 1977-2000 годах.
- AES: создан Дейманом и Рейманом в Бельгии. Национальный стандарт шифрования США с 2000 года.

Симметричные криптосистемы. Примеры

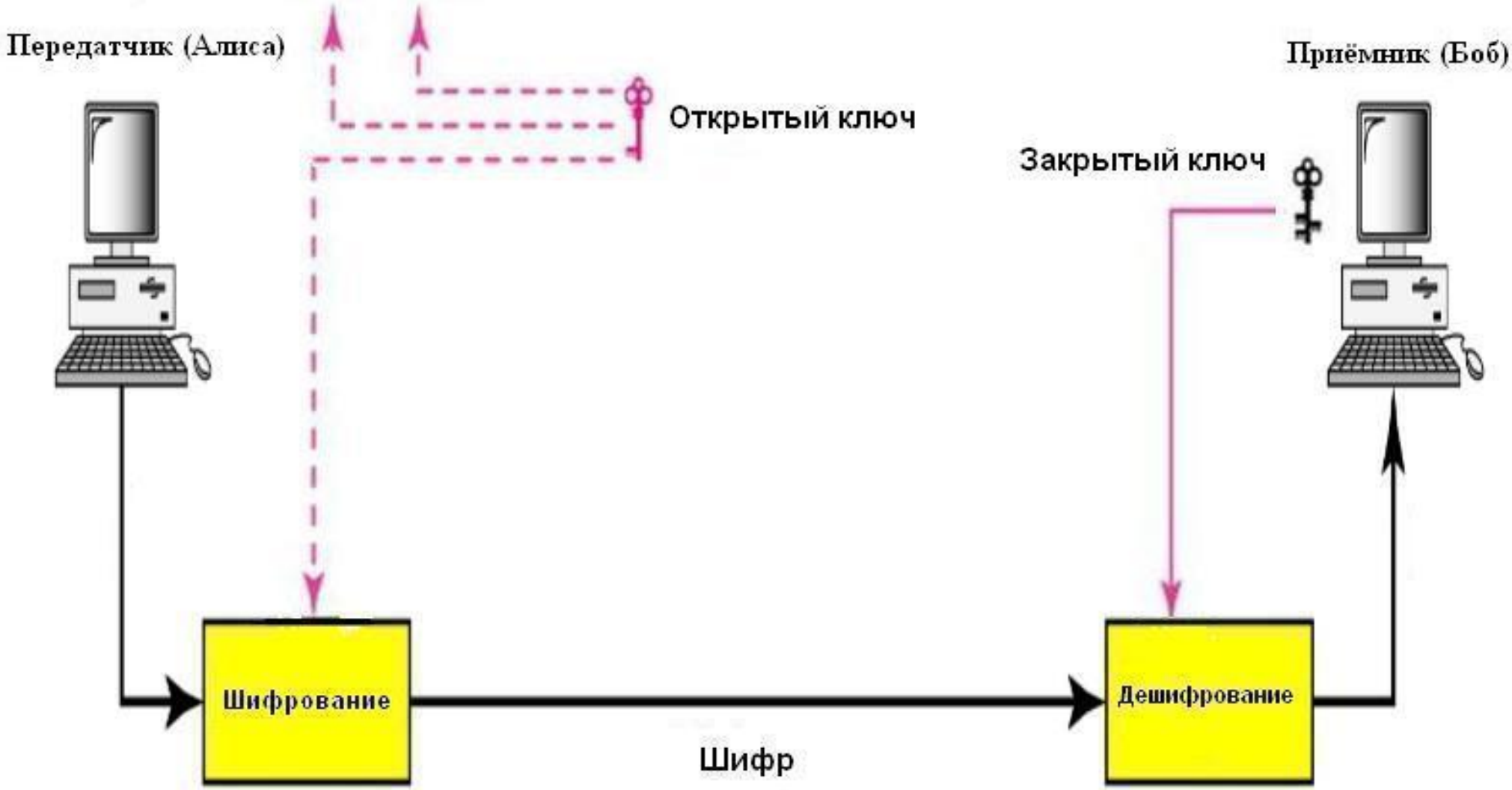
- **Шифр Цезаря:** построен по алгоритму: читать четвертую букву вместо первой, т.е. ключ равен 3.
- В шифре Цезаря ключ равен 3 (величине сдвига букв алфавита).

Пример:

- Открытый текст: **meet me at central park**
- Шифр: phhw ph dw fhqwudo sdun

Недостаток криптосистемы: легко можно раскрыть шифр

Асимметричные криптосистемы

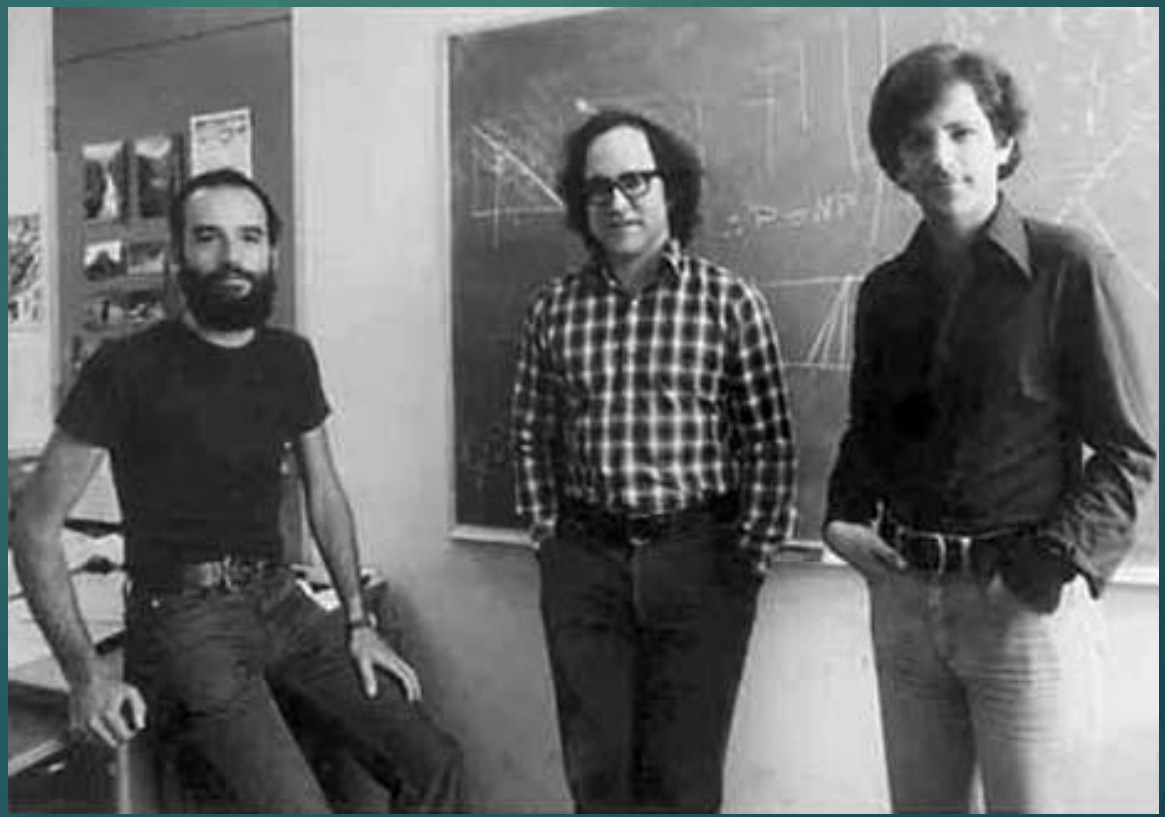


Асимметричные криптосистемы. Особенности

- Для шифрования и дешифрования используются *различные ключи.*
- Для шифрования сообщений используется *открытый ключ,* являющийся общедоступным.
- Для дешифрования сообщений используется *закрытый ключ,* являющийся секретным.
- Знание открытого ключа не даёт возможность определить закрытый ключ.

Известные асимметричные криптосистемы

- Известные криптосистемы с открытым ключом: ***RSA, ElGamal, McEliece.***
- ***Криптосистема RSA*** (создатели: Р. Ривест, А. Шамир и Л. Адлеман(1977 г.)) – одна из надёжных криптосистем.



Методы криптографического преобразования информации

Методы криптографического преобразования информации

Шифрование -проведение обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Стеганография - маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих.

Кодирование - замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков.

Сжатие - метод криптографического преобразования информации, целью которого является сокращение объема информации.

Требования к методам криптографического преобразования информации

- Зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- Структурные элементы алгоритма шифрования должны быть неизменными;
- Шифртекст не должен существенно превосходить по объему исходную информацию;
- Ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- Не должно быть простых и легко устанавливаемых зависимостей между ключами;
- Время шифрования не должно быть большим.

Терминология

- **Криптоанализ** — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.
- Криптография и криптоанализ составляют **криптологию**, как единую науку о создании и взломе шифров.
- **Криптографическая стойкость** — способность криптографического алгоритма противостоять криптоанализу.
- **Криптографическая атака** — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Заключение

- Применение криптографии в решении вопросов аутентификации, целостности данных, передачи конфиденциальной информации по каналам связи и т.п. стало неотъемлемым атрибутом информационных систем.

- В современном мире криптография находит множество различных применений - она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi, для защиты билетов от подделок на транспорте, в банковских операциях, в системах электронных платежей и т.д.

Спасибо за внимание!!!