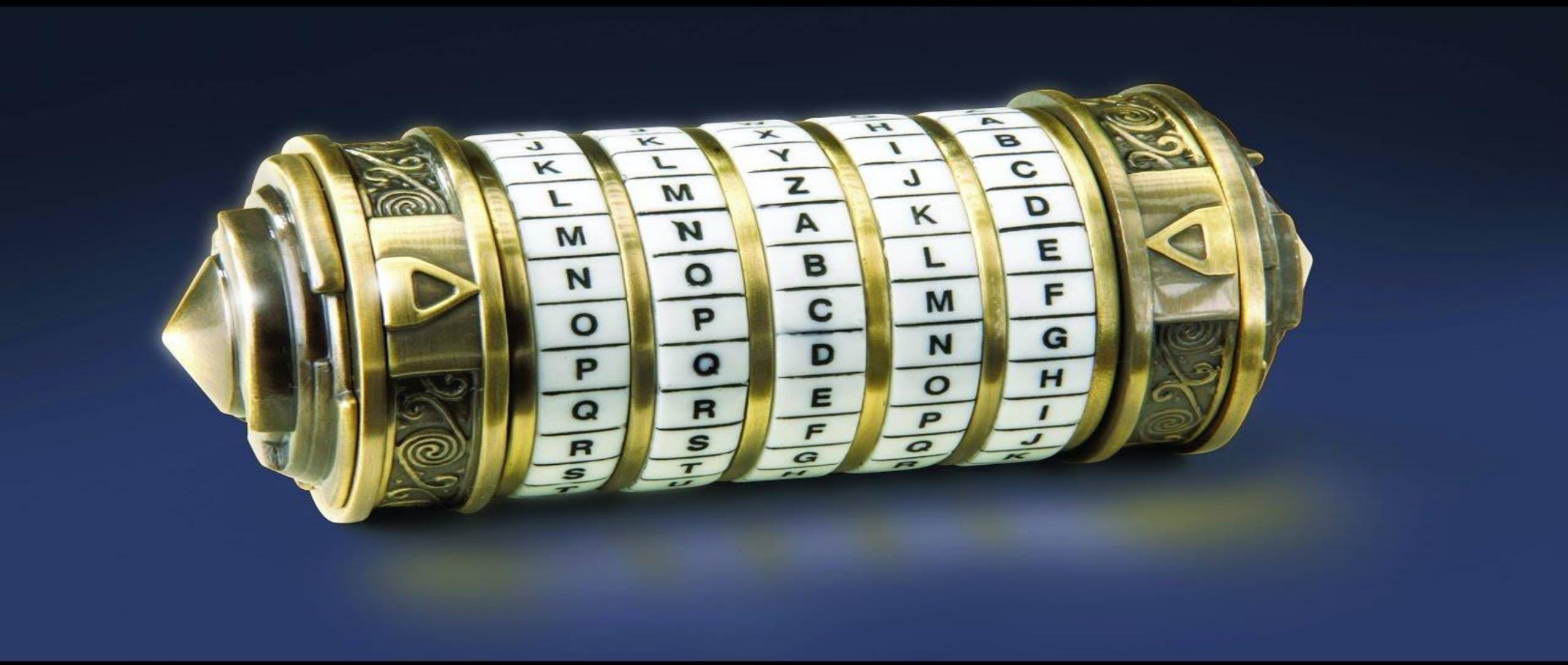
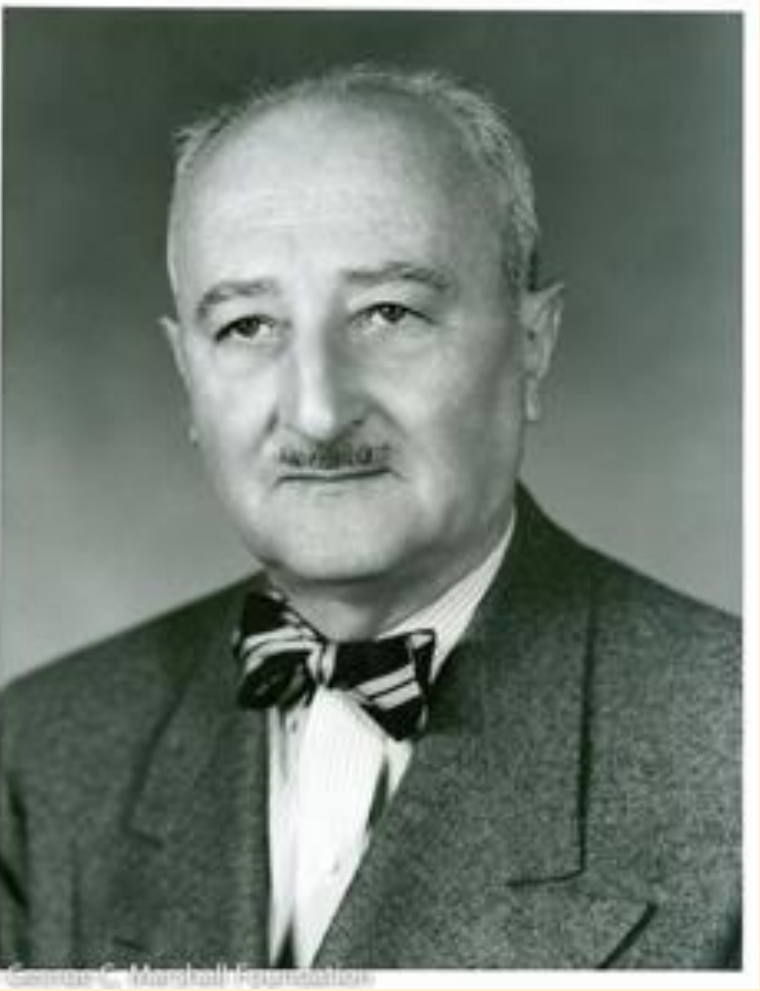
# Прикладная криптография



Часовских В.П.  2019

# Основные понятия



**Уильям Фредерик Фридман**

**Американский криптограф, именуемый «отцом американской криптологии». Ввёл в оборот сами термины «криптоанализ» и «криптология».**

Ввёл в оборот сами термины «криптоанализ» и «криптология». Организатор и первый директор американской службы радиотехнической разведки

Автор трёх учебников по военной криптографии, считающихся основополагающими текстами по этой дисциплине, и ряда научных работ по анализу кодов и шифров; пионер применения статистических методов в криптоанализе. Им разработаны девять шифровальных машин (три из которых запатентованы, 6 остаются засекреченными по сей день.

# Основные понятия

## Отправитель и получатель

Предположим, отправитель хочет послать сообщение получателю. Более того этот отправитель хочет обеспечить секретность своего сообщения: он хочет быть уверен, что перехватчик не сможет его прочесть.

## Сообщения и шифрование

Сообщение называется открытым текстом. Процесс маскировки сообщения, скрывающий его содержание, называется шифрованием. Зашифрованное сообщение называется шифротекстом. Процесс преобразования шифротекста обратно в открытый текст называется расшифровкой.

# Основные понятия

Искусство и наука сокрытия сообщений называется криптографией (cryptography), а специалисты по криптографии называются криптографами (cryptographers).

Криптоаналитиками (cryptoanalysts) называют людей, которые занимаются криптоанализом (cryptoanalysis), искусством и наукой взлома.

В компьютере сообщение представляет собой просто двоичные данные.

# Основные понятия

Кроме обеспечения конфиденциальности, криптография часто применяется для решения следующих задач:

Аутентификация (autentication). Получатель сообщения должен иметь возможность установить его источник, злоумышленник не должен иметь возможности замаскироваться под кого-то другого.

Целостность (integrity). Получатель сообщения может проверить, было ли сообщение изменено в процессе доставки, и злоумышленник не сможет подменить правильное сообщение ложным.

Невозможность отказа от авторства. Отправитель не должен иметь возможности ложно отрицать отправку сообщения.

# Основные понятия

Криптографический алгоритм, который называется шифром - это математическая функция, используемая шифрования и расшифровки. Обычно эти функции связаны друг с другом: одна предназначена для шифрования, другая — для расшифровки.

Если безопасность алгоритма обеспечивается засекречиванием самого алгоритма, то он называется ограниченным. Ограниченные алгоритмы представляют только исторический интерес, поскольку они не соответствуют современным стандартам. Если алгоритм применяется группой пользователей, то при покидания кого-то группы, необходимо менять алгоритм. Современная криптография решает эту проблему с помощью ключа. Ключ применятся при шифровке и расшифровке и заменяется ключ, а не алгоритм.

# Стандарт шифрования данных DES

Стандарт шифрования данных (Data Encryption Standard — DES), который Американский национальный институт стандартов (ANSI) называет алгоритмом шифрования данных (Data Encryption Algorithm — DEA), а Международная организация стандартизации ISO — алгоритмом DEA-1, за двадцать лет стал всемирным стандартом. Он отлично прошел многолетний криптонализ и остается стойким против всех противников, за исключением, возможно, самых могущественных.

# Свойства стандарта шифрования данных DES

- Алгоритм должен обеспечивать высокий уровень защиты.
- Алгоритм должен быть полностью определенным и понятным.
- Стойкость алгоритма должна зависеть от ключа и не должна зависев от секретности самого алгоритма.
- Алгоритм должен быть доступен всем пользователям.
- Алгоритм должен адаптироваться к разным приложениям.
- Алгоритм должен допускать экономичную реализацию в электронных устройствах.
- Алгоритм должен быть эффективным в использовании.
- Алгоритм должен быть тестируемым.
- Алгоритм должен быть разрешен для экспорта.

# ОПИСАНИЕ СТАНДАРТА DES

- Алгоритм DES представляет собой блочный шифр; он шифрует данные 64-битовыми блоками. На вход алгоритма поступает 64-битовый блок открытого текста, а на выходе получается 64-битовый блок шифротекста. DES является симметричным: для шифрования и расшифровки один и тот же алгоритм и ключ (за исключением небольших различий в расписании смены ключа).
- Длина ключа равна 56 битам. (Ключ обычно представляется в виде 64-би тового числа, но каждый восьмой бит используется для проверки четности и игнорируется. Биты четности являются наименьшими значащими битами байтов ключа.) Ключ может быть любым 56-битовым числом, и его можно изменить в любой момент времени. Несколько чисел считаются слабым ключами, но их можно легко избежать. Стойкость полностью определяется ключом.