Криптографические методы защиты информации

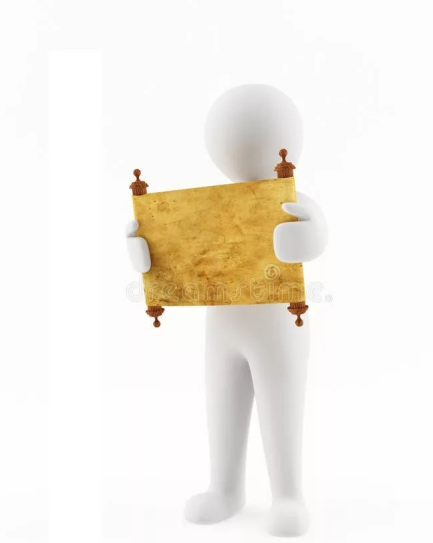
Выполнил обучающийся
группы ТПСл-118 (Ч)
специальности ТПС
Тюленев Максим

- Актуальность:
- В наш век все увеличивающегося потока обмена информацией, к которой относится все больше и больше информации - устойчивое и надёжное шифрование является не просто необходимым, а жизненно важным условием безопасности.

- Проблема:
- На данный момент, современные алгоритмы шифрования удовлетворяют требованиям пользователей и справляются со своей функцией защиты, но с развитием техники в недалеком будущем станут доступны компьютеры с новой архитектурой, которая позволит реализовать более мощные алгоритмы дешифрования.
- Продукт проекта:
- Презентация о криптографических методах защиты информации
- Задачи:
- 1.Рассмотреть понятия криптография и шифрование.
- 2.Рассмотреть популярные системы шифрования.

Определение понятий криптография и шифрование

- Криптография — это наука, изучающая способы сокрытия данных и обеспечения их конфиденциальности.

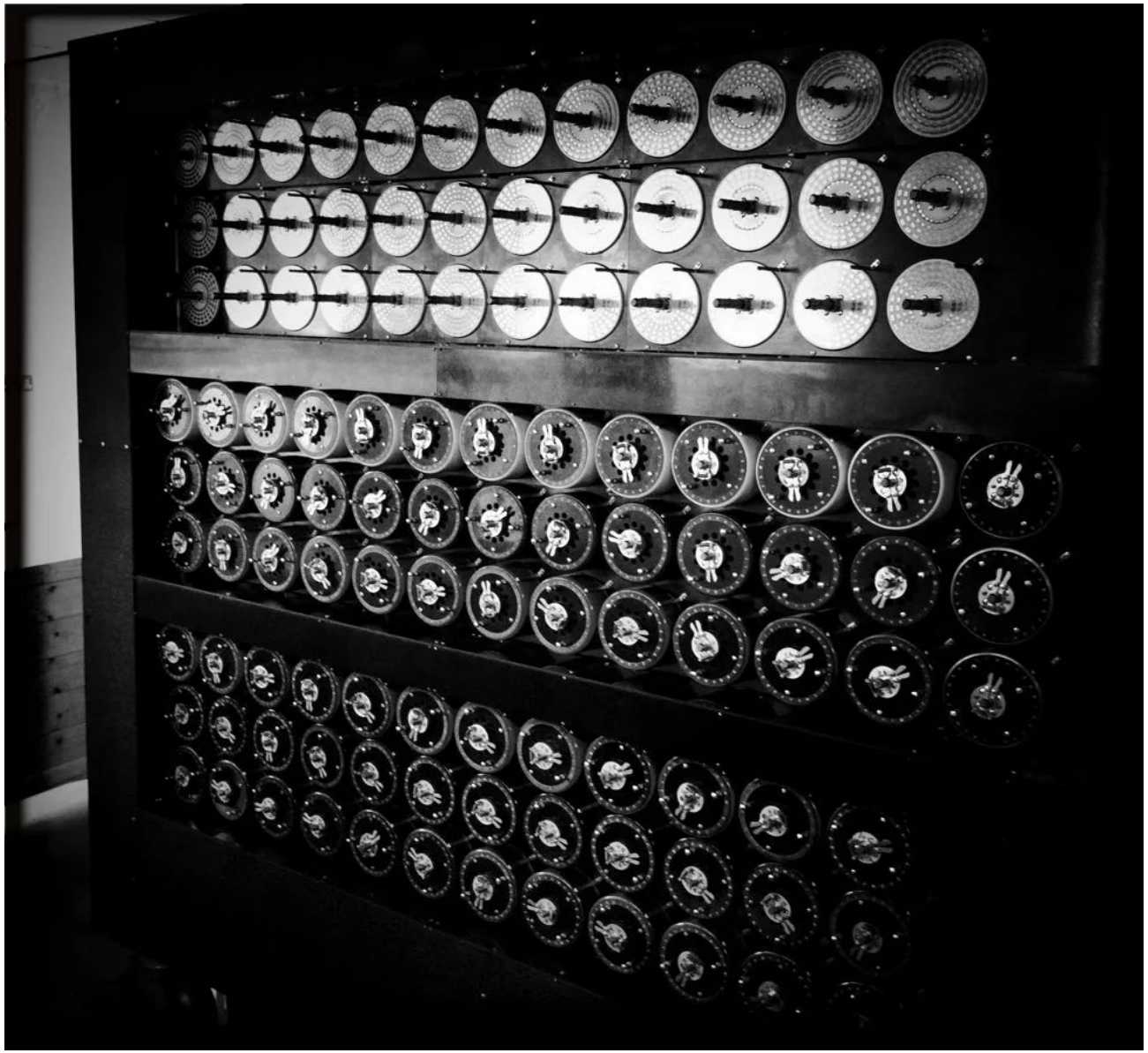


Примеры моноалфавитного шифра

- Шифр простой замены не всегда подразумевает замену буквы на какую-то другую букву.
- Допускается использовать замену буквы на цифру.
- К примеру представим некий шифр-алфавит: **А - 33; Б - 17; В - 8; Г - 16; Д - 2; Е - 15; Ё - 14; Ж - 13; З - 12; И - 98; Й - 10; К - 97; Л - 96; М - 24; Н - 0; О - 11; П - 5; Р - 25; С - 7; Т - 3; У - 64; Ф - 26; Х - 66; Ц - 69; Ч - 4; Ш - 6; Щ - 36; Ь - 21; Ъ - 22; Ы - 23; Э - 37; Ю - 39; Я - 18.**
- В данном шифре применяются цифры, заменяющие буквы. Никакой логики в этих цифрах нет.
- Такой простой шифр можно расшифровать, только имея таблицу шифров.

Шифровальная машина “Энигма”

Британская машина дешифрирования немецких шифров времено Второй мировой войны “Turing Bombe”



Четыре низкоуровневых примитива

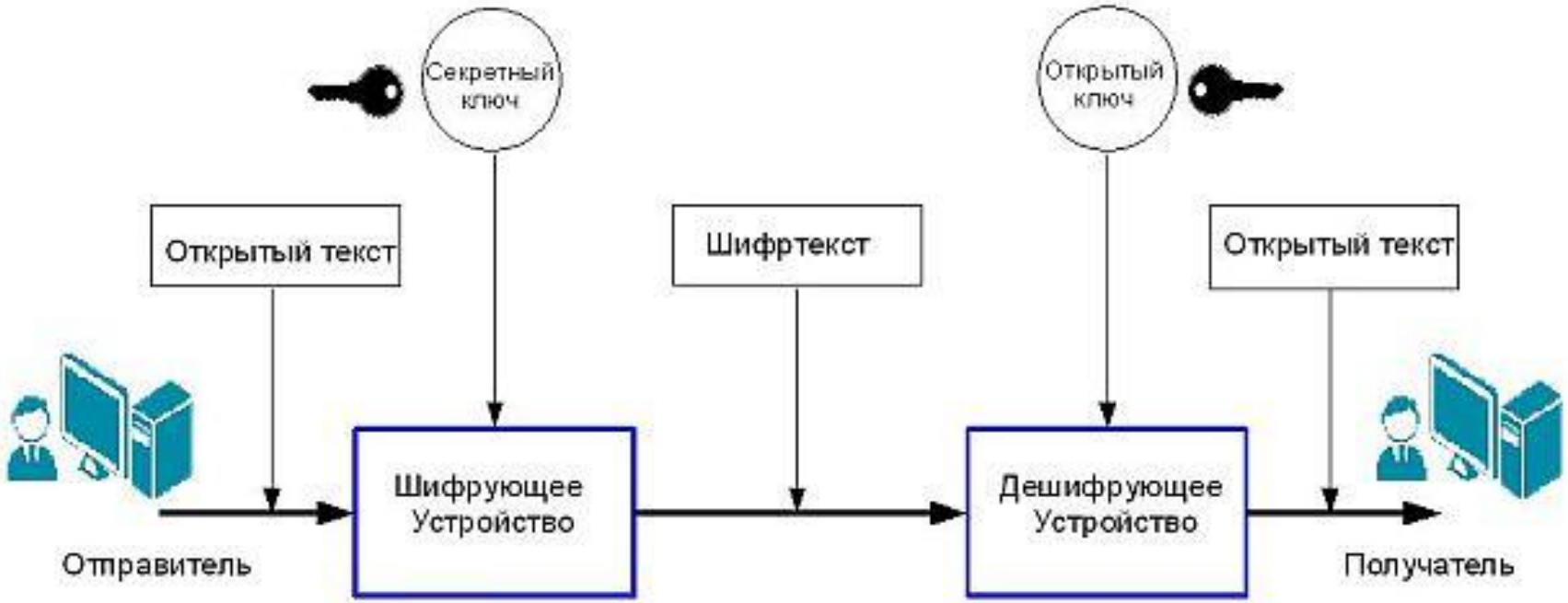
- Симметричное шифрование.
- Асимметричное шифрование.
- Хэширование.
- Электронная подпись.

Симметричное шифрование

- $K_1 = K_2$ (один ключ математически легко вычисляется из другого)

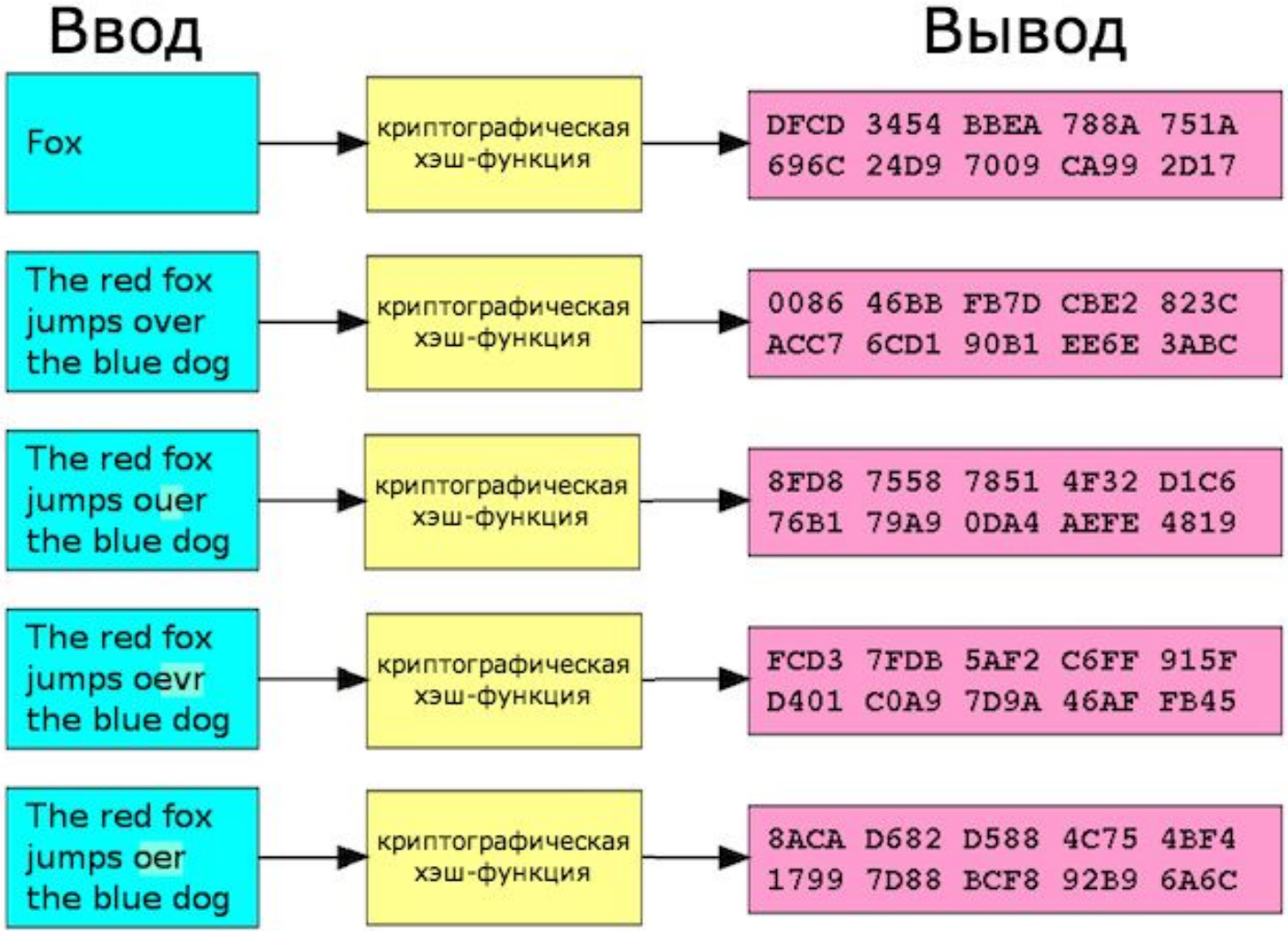
- Блочные шифры: AES (Advanced Encryption Standart), ГОСТ 28147-89 (Советский и российский стандарт шифрования, ставший стандартом всего СНГ), DES (Data Encryption Standart).
- Поточные шифры: SEAL (Software Efficient Algorithm), WAKE (World Auto Key Encryption algorithm)

Асимметричная система

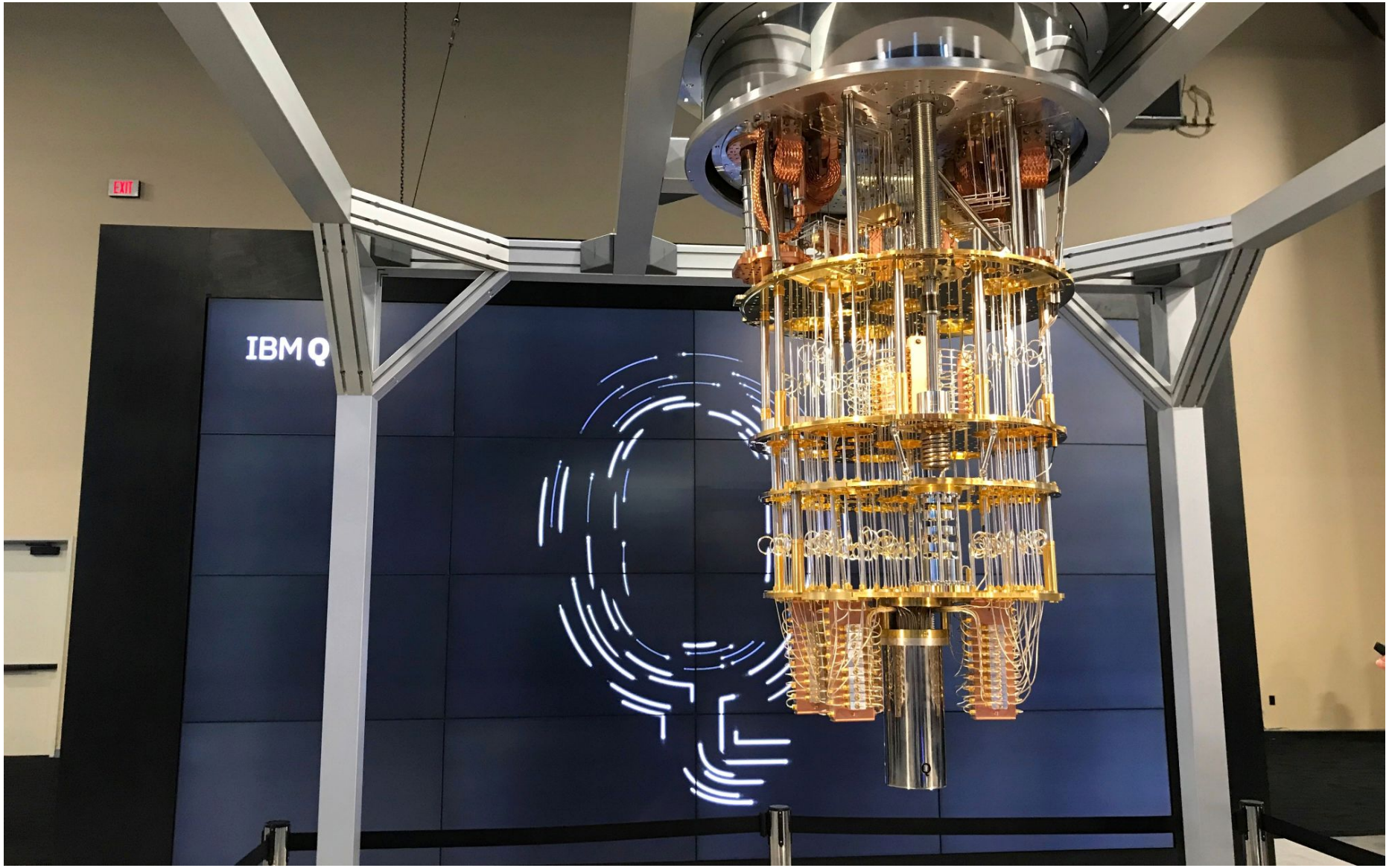


Самые популярные виды такого шифра: RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), ГОСТ Р 34.10-2012.

Метод хэширования



Квантовый компьютер компании IBM



Заключение

- Технологии в области шифрования с каждым днем развиваются, появляются новые шифры и технологии. Параллельно с появлением нового, криптоаналитики помогают совершенствовать уже ранее созданные алгоритмы, благлдаря чему, некоторые используются и в наше время, что показывает их нынешнюю актуальность. Новые же алгоритмы, помимо сложных комбинаций из простейших шифрующих методотов, должны отличаться необычным подходом их реализации.