

# Аутентификация сообщений

# Проблемы, решаемые криптографией

- конфиденциальность
- целостность
- аутентификация
- невозможность отказа от авторства

# Подделка содержимого

Сообщение

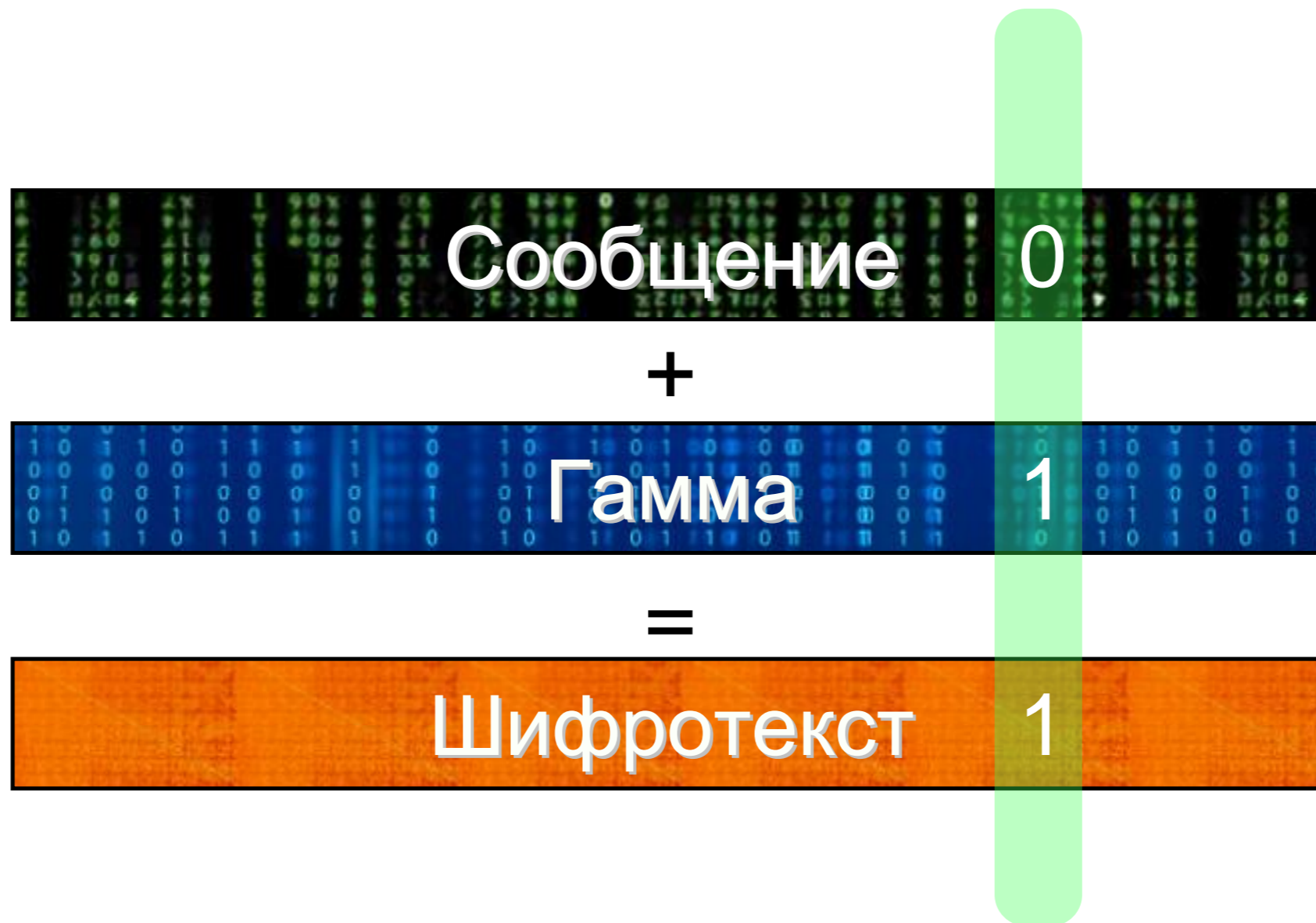
+

Гамма

=

Шифротекст

# One-bit variation



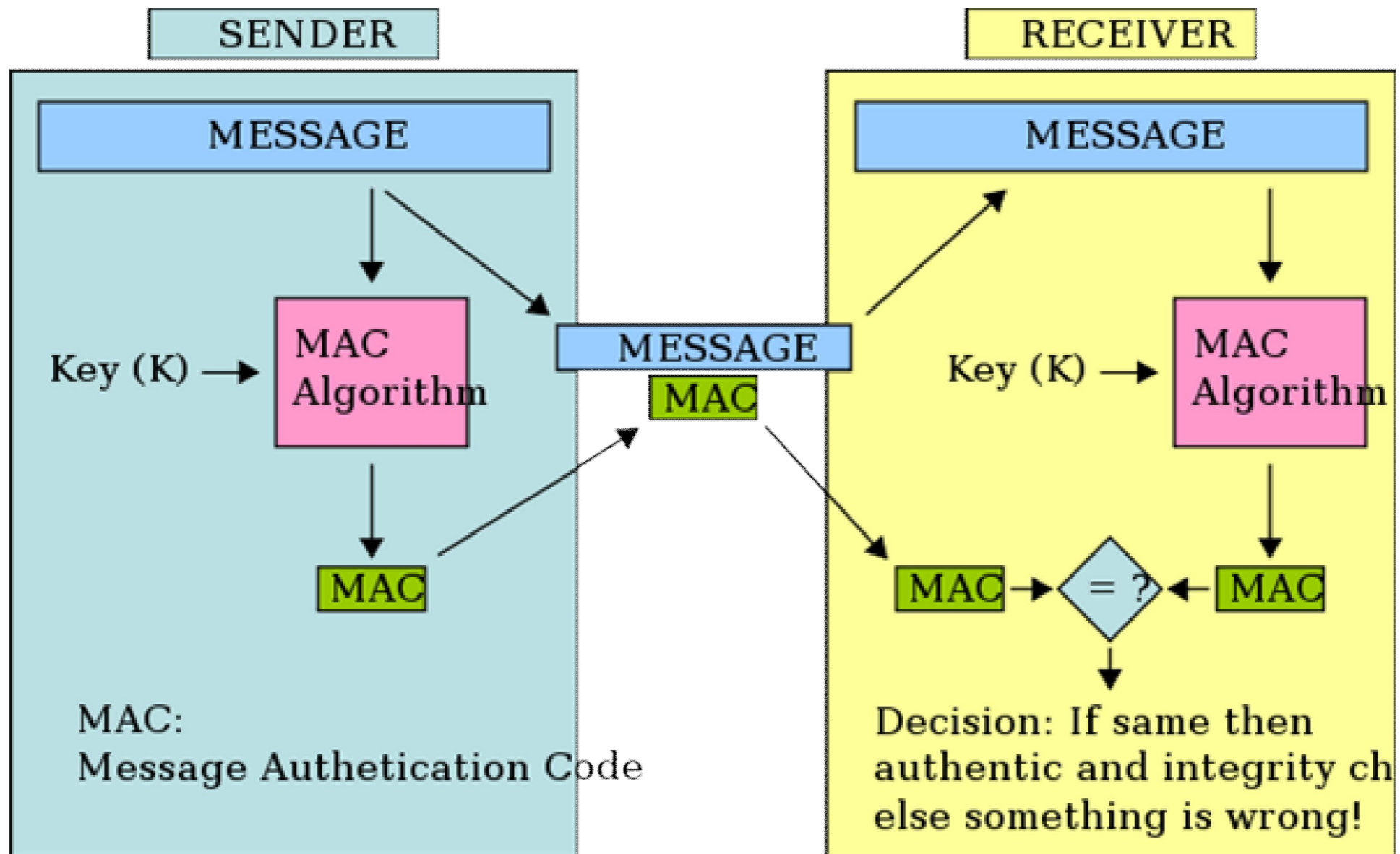
# Проблема аутентификации

- Необходим механизм, который для сообщений произвольной длины
- позволяет убедиться, что сообщение не было изменено
- позволяет проверить, кто является отправителем

# MAC

- MAC: Message Authentication Code
  - Принимает на вход сообщение и *ключ*
  - Генерирует *код аутентификации* или *тег*

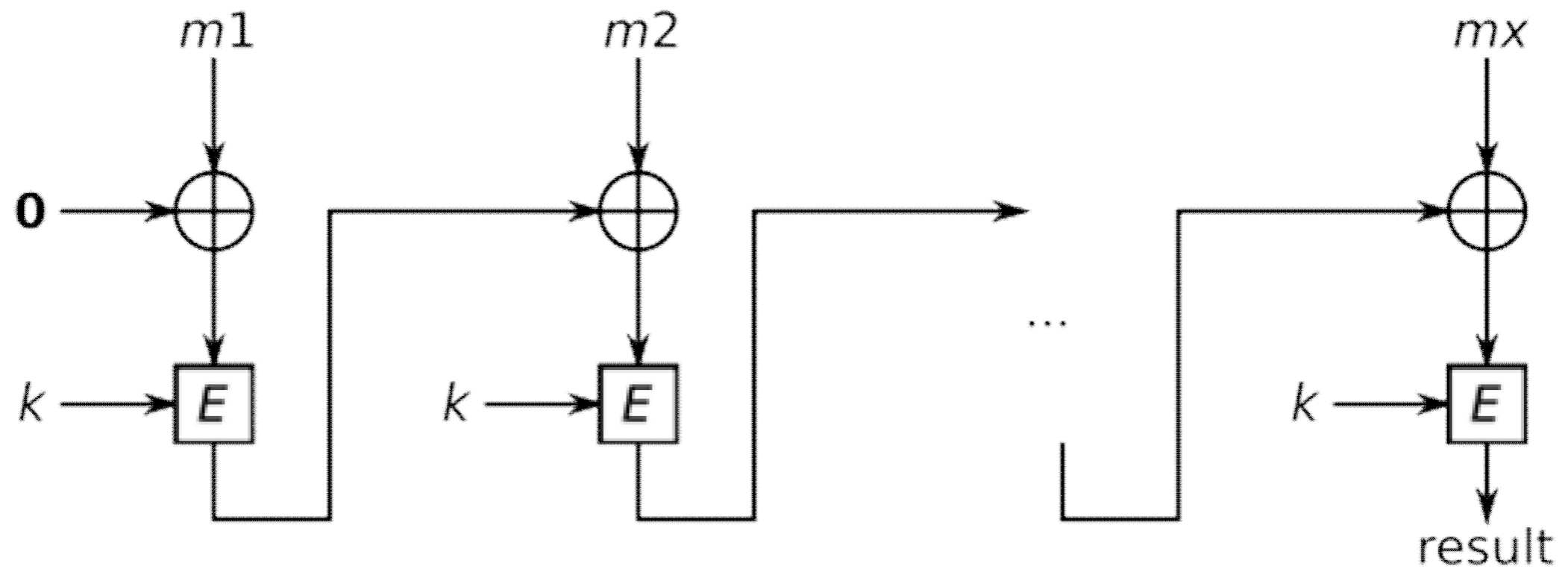
# MAC





- Можно ли использовать для этой цели симметричное шифрование?

# CBC-MAC



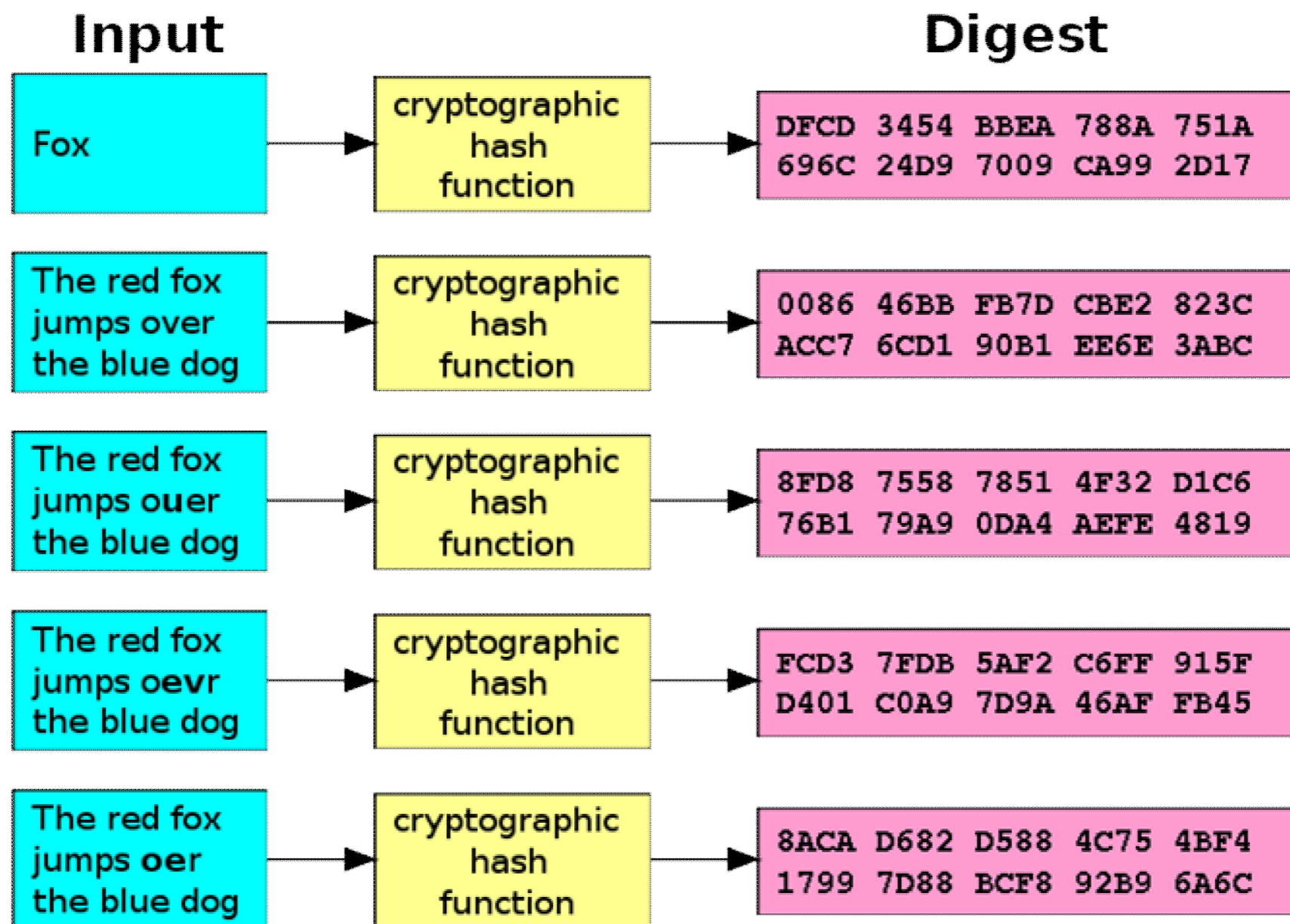
# СВС-МАС

- Что происходит в случае с сообщениями переменной длины?

# Криптографический хеш

- Легко вычислить для любого сообщения переменной длины
- *Невозможно* найти сообщение по известному хешу
- *Невозможно* изменить сообщение, не изменив хеш
- *Невозможно* найти два сообщения с одинаковым хешем

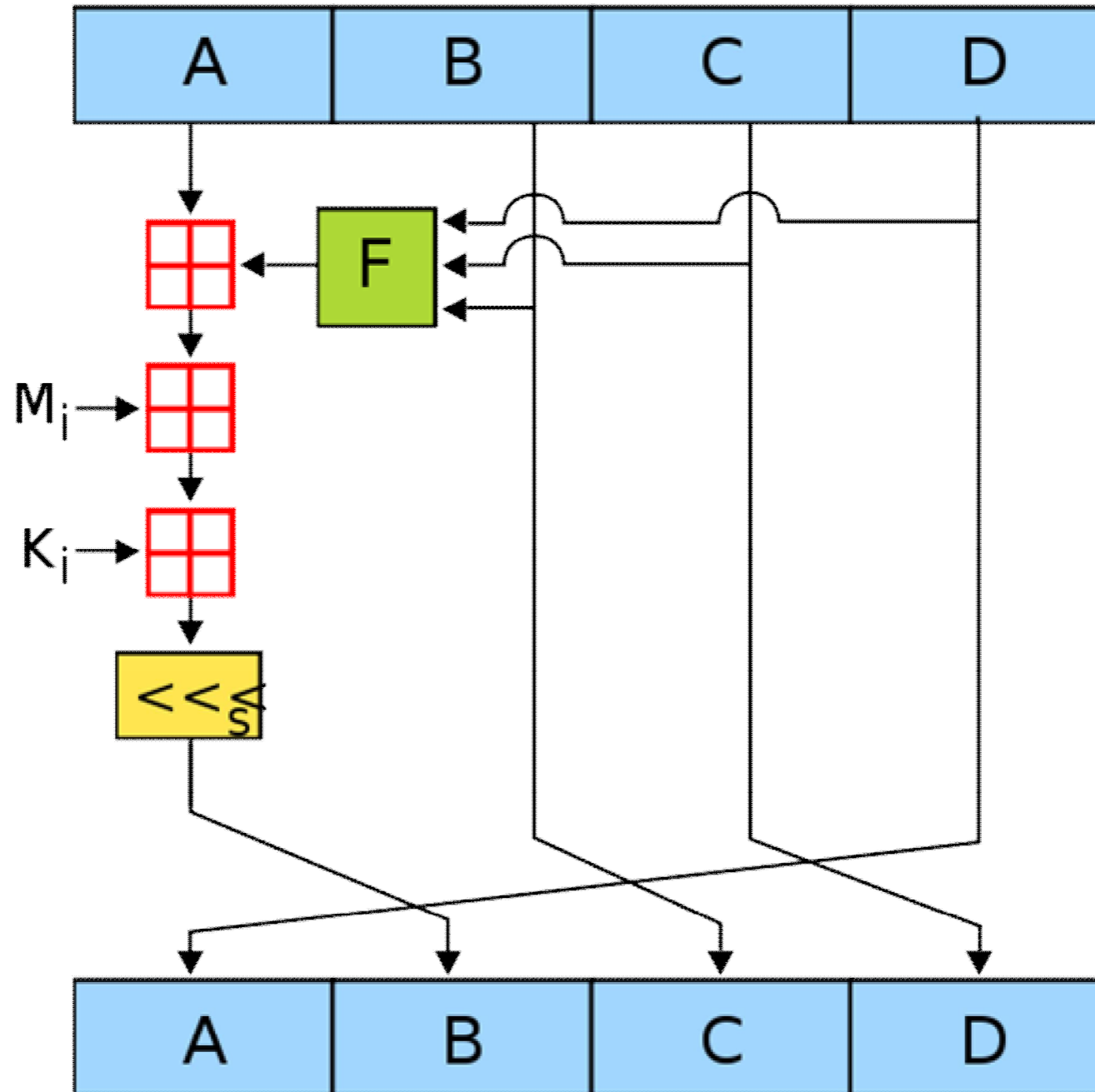
# Криптографический хеш



# Современные хеши

- MD4/MD5
- Семейство SHA
- ГОСТ 34.11-94
- Конкурс на стандартный алгоритм

# MD4



# Применение хеш- функций

- Выработка ключевой информации
- PBKDF2
- Хранение паролей
- Unix `crypt()`, Windows SAM



# Упражнение

- Поиск коллизий в функции MD4