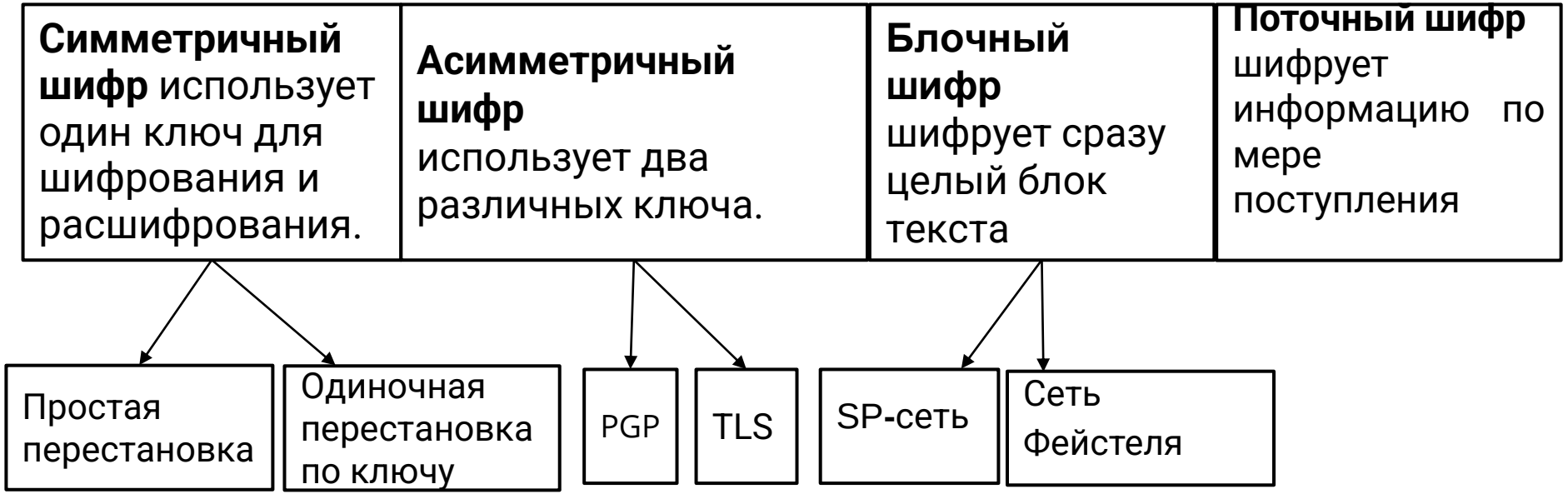
Шифрование

- **Шифр** - система преобразования текста для обеспечения секретности передаваемой информации.
- Процесс засекречивания сообщения с помощью шифра называется **шифрованием**.
- Наука о создании и использовании шифров называется **криптографией**. Наука о методах получения исходного значения зашифрованной информации называется **криптоанализ**.
- Исходное сообщение называется в криптографии открытым **текстом**, или **клером**. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или **криптограммой**.

Ключи и типы шифров

Важным параметром любого шифра является **ключ** — параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма.



Алгоритм замены

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.

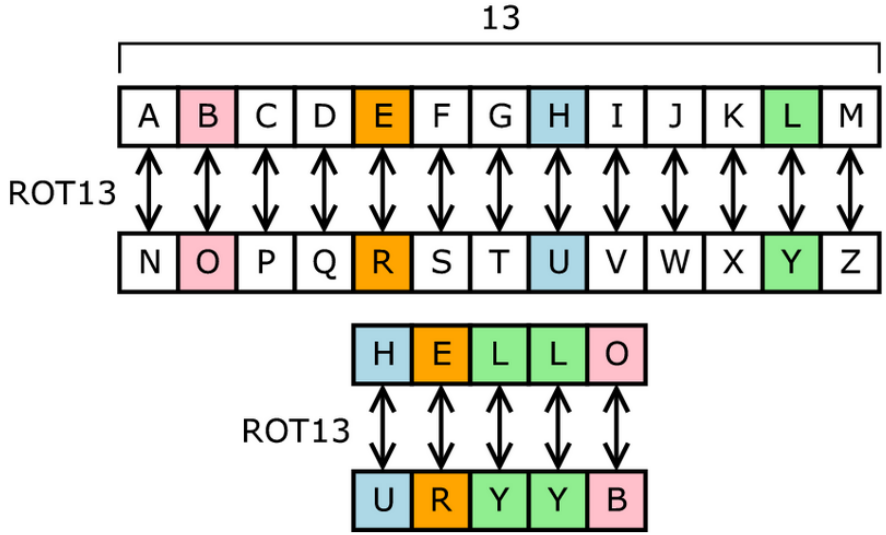
Например:

Открытый Алфавит	А	Л	М	Р	У	Ы
Шифровальный алфавит	А	Б	В	Г	Д	Е

Открытый текст: МАМА МЫЛА РАМУ
Зашифрованный текст: ВАВА ВЕБА ГАВД

Алгоритм замены

```
for(a=0;a<i;a++)// рандомное заполнение ключа
        key[a]=char((rand()%255));
for(a=0;a<i;a++)// шифрование
        text[a]+=key[a];
for(a=0;a<i;a++)// дешифрование
        text[a]-=key[a];
```



Принцип работы программы ROT13 для скрытия информации

Алгоритм перестановки

В криптографическом **алгоритме перестановки** все **буквы** открытого текста остаются без изменений, но **переставляются** согласно заранее оговоренному правилу. Здесь также удобно использовать ключ, управляющий процедурой шифрования.

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

Пример использования алгоритма перестановки

Алгоритм перестановки

- В цикле (строки 1-10) проходимся по всем блокам исходного сообщения длиной в ключ.
- На каждой итерации этого цикла создается символьный массив transposition (строка 3), в который будем заносить зашифрованный текст (переставленные символы) — символы в новом порядке исходя из ключа.
- Затем во внутреннем цикле (строки 5-6) перебираем все символы блока и происходит непосредственно шифрование (перестановка) по ключу (строка 6).
- После в цикле (строки 8-9) посимвольно прибавляем зашифрованный блок к концу строковой переменной с результатом (строка 9).

```
1   for (int i = 0; i < input.Length; i += key.Length)
2   {
3       char[] transposition = new char[key.Length];
4
5       for (int j = 0; j < key.Length; j++)
6           transposition[key[j] - 1] = input[i + j];
7
8       for (int j = 0; j < key.Length; j++)
9           result += transposition[j];
1   }
0
```

Возьмем в качестве ключа для сообщения МАМА МЫЛА РАМУ слово БАЙТ. Пронумеруем буквы ключевого слова в порядке их следования слева направо в русском алфавите. Далее под полученной числовой последовательностью в строках, равных по длине ключевому слову, запишем открытый текст.

Буквы ключевого слова	Б	А	Й	Т
Порядковые номера букв в алфавите	2	1	3	4
Открытый текст	М	А	М	А
	М	Ы	Л	А
	Р	А	М	У

Открытый текст: МАМА МЫЛА РАМУ
Зашифрованный текст: АЫАММРМЛМААУ

Передача зашифрованной информации