Методы перестановки

Методы перестановки

- d=6
- K = 436215
- ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ

_ОЕТЭТ_ТЛСКДИШР_ЯФНАЯВОИ

Перестановка по таблице

ЭТО ТЕКСТ ДЛЯ ШИФРОВАНИЯ

4 столбца и 3 строки
(размер блока равен 3*4=12 символов).

ЭТТТЕ ОКД СЛЯФА РНШОИИВЯ

1 блок			
Э	Т	О	
Т	Е	К	С
Т		Д	Л
2 блок			
Я		Ш	И
Ф	Р	О	В
А	Н	И	Я

Сообщение не кратно размеру блока

ПЕРЕМЕНКА

ПМАЕЕРНЕК

Ключевые термины

- **Гаммирование** – метод шифрования, основанный на "наложении" гамма-последовательности на *открытый текст*. Обычно это суммирование в каком-либо конечном *поле* (суммирование *по* модулю). Например, в *поле* GF(2) такое суммирование принимает вид обычного "исключающего ИЛИ". При расшифровке операция проводится повторно, в результате получается *открытый текст*.
- **Пропорциональные** или **монофонические шифры** – методы замены, в которых уравнивается частота появления зашифрованных знаков.
- **Шифры замены (подстановки)** основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.
- **Шифр многоалфавитной замены (или подстановки)** – *группа* методов шифрования подстановкой, в которых для замены символов исходного текста используется не один, а несколько алфавитов *по* определенному правилу.

Ключевые термины

- **Шифры перестановки** основаны на том, что *входной поток* исходного текста делится на блоки, в каждом из которых выполняется *перестановка* символов. Ключом такого шифра является используемая при шифровании перестановочная *матрица* или *вектор*, указывающий правило перестановки.
- **Шифр простой (или одноалфавитной) замены, простой подстановочный шифр, моноалфавитный шифр**— *группа*методов шифрования, которые сводятся к созданию *по* определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква *шифртекста*. Само *шифрование*заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать *алгоритм*, *по*которой она генерируется.
- **Симметричное шифрование (шифрование с закрытым ключом)** – методы обратимого преобразования данных, в которых используется один и тот же *ключ*, который обе стороны информационного обмена должны хранить в секрете от противника. Все известные из истории шифры, например, *шифр* Цезаря – это шифры с закрытым ключом.