Билет: №2

Вопрос: №2

Дать определение:

* Шифрование;
* Рассеивание информации;

Требования к алгоритмам шифрования;

Правило Керкгхоффа;

Ответ:

**Шифрование** – преобразование открытого текста (plain text) в зашифрованный (ciphertext) с целью защитить его конфиденциальность

**Рассеивание информации** – влияние одного знака открытого текста на несколько знаков шифрованного текста;

**Требования к алгоритмам шифрования:**

1. Сложность расшифровки

2. Малое изменение исходного текста/ключа ведёт к значительным изменениям шифрованного текста

3. Не требуется секретность системы

4. Секретность алгоритма определяется секретностью ключа

5. Стоимость дешифрации превышает стоимость данных

6. Область значений ключа должна исключать его перебор

**Правило Кергхоффа** – стойкость алгоритма определяется только секретностью ключа.