

Класс GrdAM

Задаёт режим работы алгоритма и процесс шифрования.

Синтаксис

```
public class GrdAM
```

Методы

```
public int getValue()
```

Возвращает значение константы статического объекта.

Константы

ECB

```
public static final GrdAM ECB
```

Режим электронной кодовой книги (режим простой замены). Каждый блок открытого текста заменяется блоком шифротекста. Шифрование двух одинаковых блоков даст идентичный результат. Скорость обработки блоков в режиме ECB фиксирована. Недостаток ECB, в сравнении с другими режимами шифрования, — сохранение статистических особенностей открытого текста.

Значение константы: 0

CBC

```
public static final GrdAM CBC
```

Режим сцепления блоков шифротекста. Каждый блок открытого текста (кроме первого) побитово складывается по модулю 2 (операция XOR) с предыдущим результатом шифрования. Таким образом, каждый блок зашифрованного текста зависит от всех блоков открытого текста, обработанных до него. Режим CBC лишён недостатка алгоритма ECB, но всё же имеет ряд недостатков с точки зрения безопасности.

Значение константы: 1

CFB

```
public static final GrdAM CFB
```

Режим обратной связи по шифротексту (режим гаммирования с обратной связью). Для шифрования следующего блока открытого текста он складывается по модулю 2 с перешифрованным (блочным шифром) результатом шифрования предыдущего блока. Криптостойкость CFB определяется криптостойкостью используемого шифра.

Значение константы: 2

OFB

```
public static final GrdAM OFB
```

Режим обратной связи по выходу. В этом режиме открытый текст используется только для конечного сложения. Операции блочного шифра могут быть выполнены заранее, позволяя выполнить заключительное шифрование параллельно с открытым текстом.

Значение константы: 3

Encode
public static final GrdAM Encode

Зашифровать блок данных.

Значение константы: 0

Decode
public static final GrdAM Decode

Расшифровать блок данных.

Значение константы: 0x80

Encrypt
public static final GrdAM Encrypt

Синоним **Encode**

Значение константы: 0

Decrypt
public static final GrdAM Decrypt

Синоним **Decode**

Значение константы: 0x80