Класс GrdAM

Класс позволяет выбрать режим работы криптографического алгоритма, тип операции шифрования и номер блока данных для методов GrdTransformEx и GrdCryptEx

Пространство имен: Guardant

Синтаксис

```
public class GrdAM
```

Конструкторы

```
public static GrdAM operator +(GrdAM op1, GrdAM op2)
public static GrdAM operator +(GrdAM op1, GrdSC op2)
public static GrdAM operator +(GrdSC op1, GrdAM op2)
```

Методы

```
public int Value
```

Возвращает значение константы статического объекта.

Константы

Класс содержит предопределенные статические объекты, которые соответствуют режимам работы криптографического алгоритма и типу операции шифрования.

Имя	Значение	Описание
ECB	0	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.
CBC	1	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.
CFB	2	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.
OFB	3	Режим обратной связи по выходу. В этом режиме открытый текст используются только для конечного сложения. Операции блочного шифра могут быть выполнены заранее, позволяя выполнить заключительное шифрование параллельно с открытым текстом.
Encode	0	Зашифровать блок данных.
Decode	0x80	Расшифровать блок данных.

Encrypt	0	Синоним **Encode**.
Decrypt	0x80	Синоним **Decode**.

Описание

Класс служит для одновременной передачи методам Guardant API режима работы криптографического алгоритма, типа операции шифрования и номера блока данных (см. описание класса GrdSC). Например, чтобы программно зашифровать один блок в режиме электронной кодовой книги, методу GrdCryptEx в параметре *method* достаточно передать **GrdAM.ECB** + **GrdAM.Encrypt** + **GrdSC.ALL** .

См. методы: GrdCryptEx , GrdTransformEx