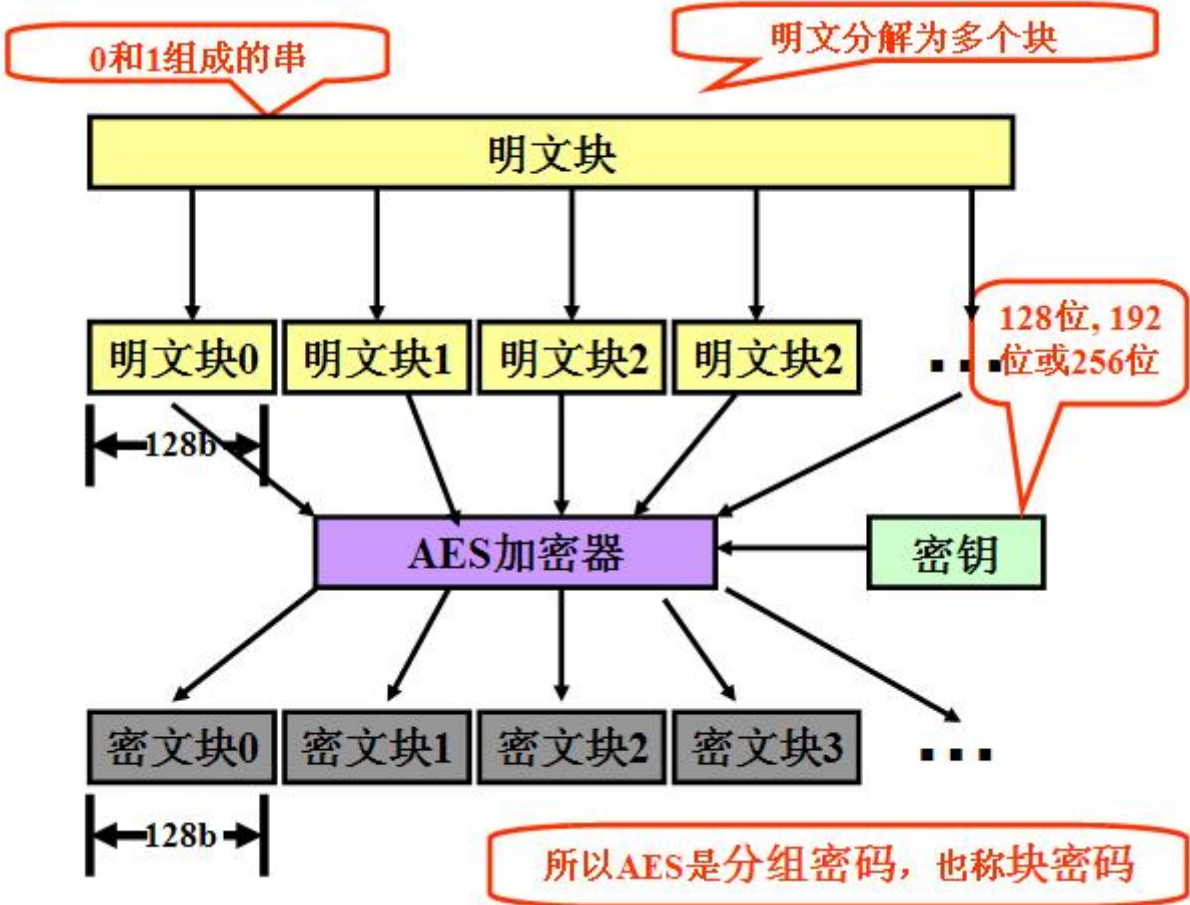


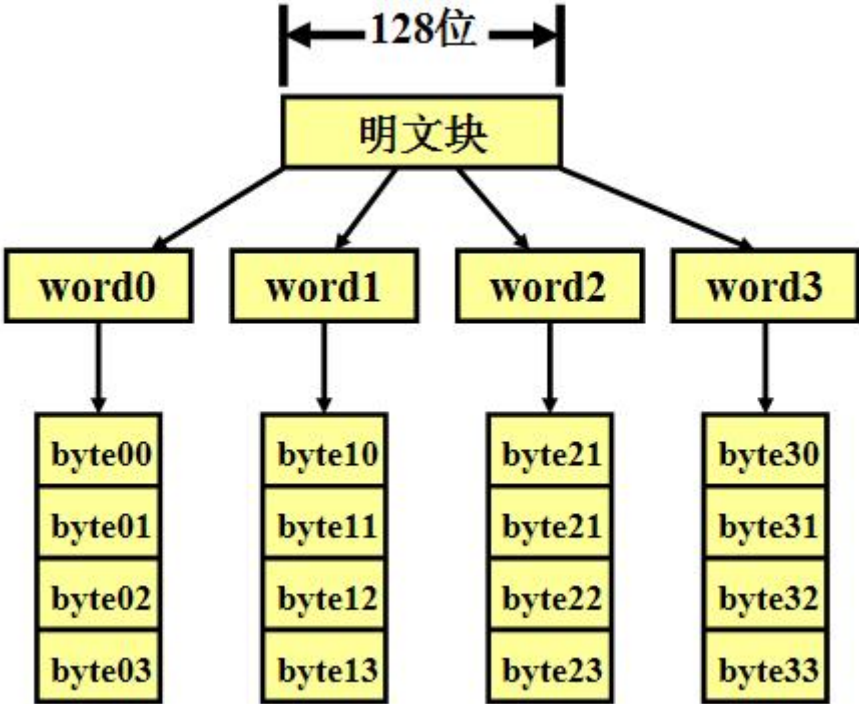
AES加密的四种模式详解 - 小辉辉可爱多

对称加密和分组加密中的四种模式(ECB、CBC、CFB、OFB)

一. AES对称加密:

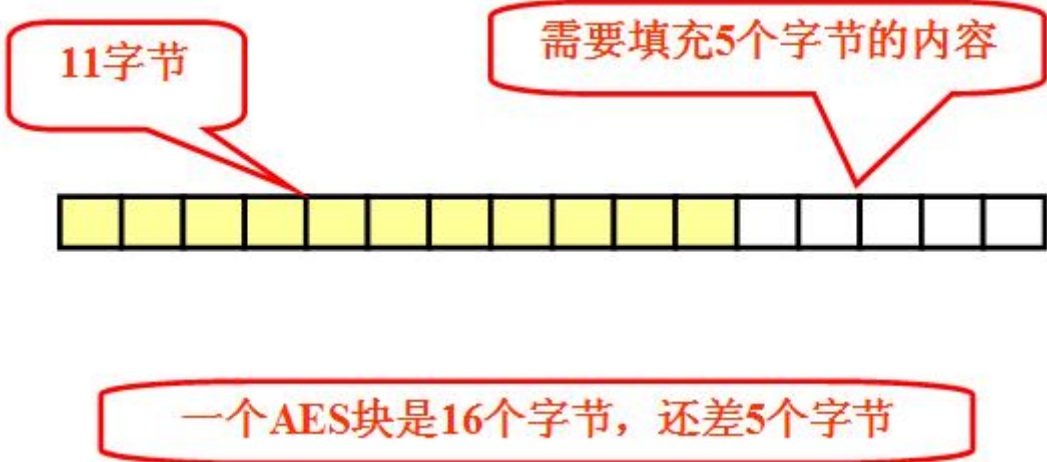


AES加密



分组

二. 分组密码的填充

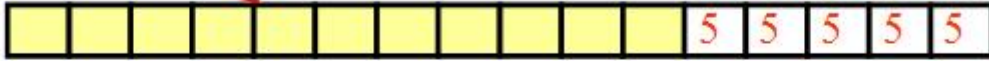


分组密码的填充

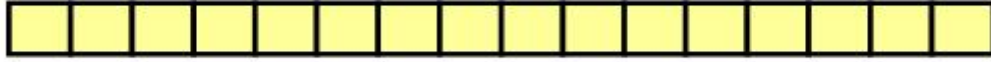
e.g.:

11字节

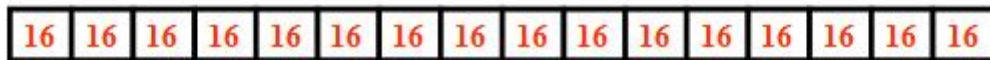
因为有5个字节需要填充, 所以...



新问题: 如果刚好不用填充怎么办

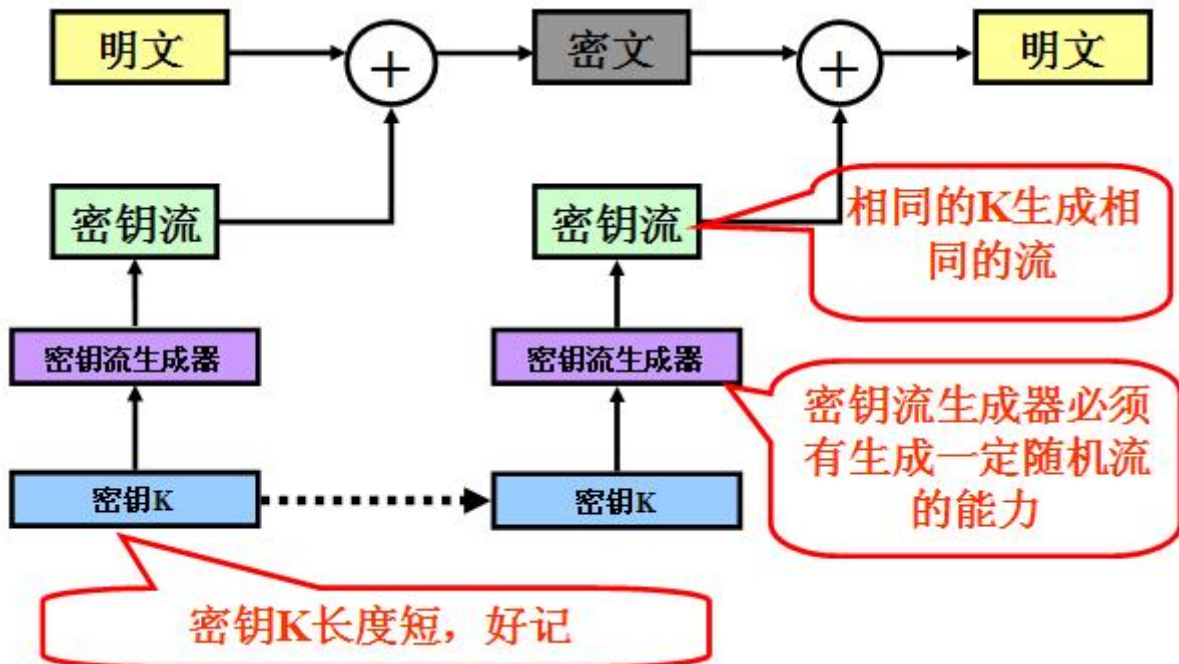


+



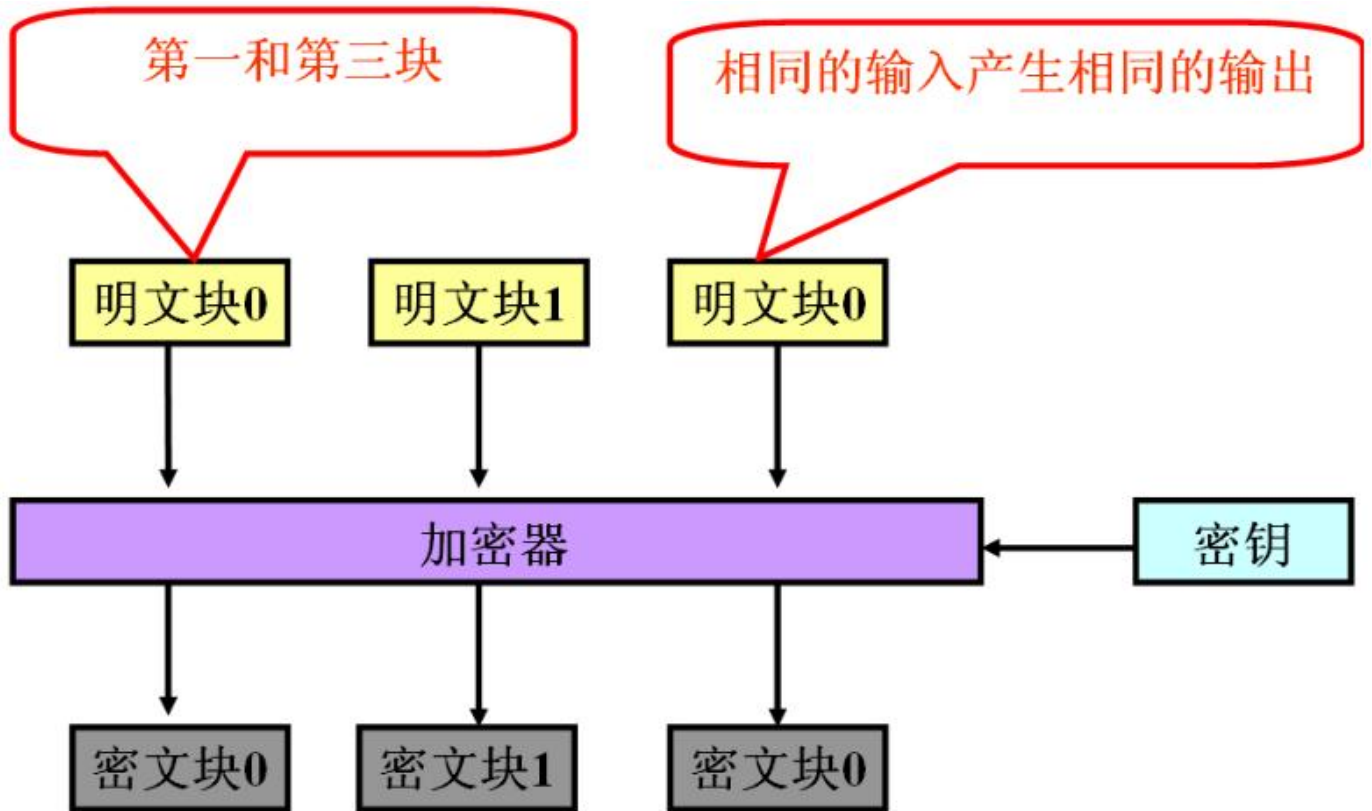
PKCS#5填充方式

三. 流密码:



四. 分组密码加密中的四种模式:

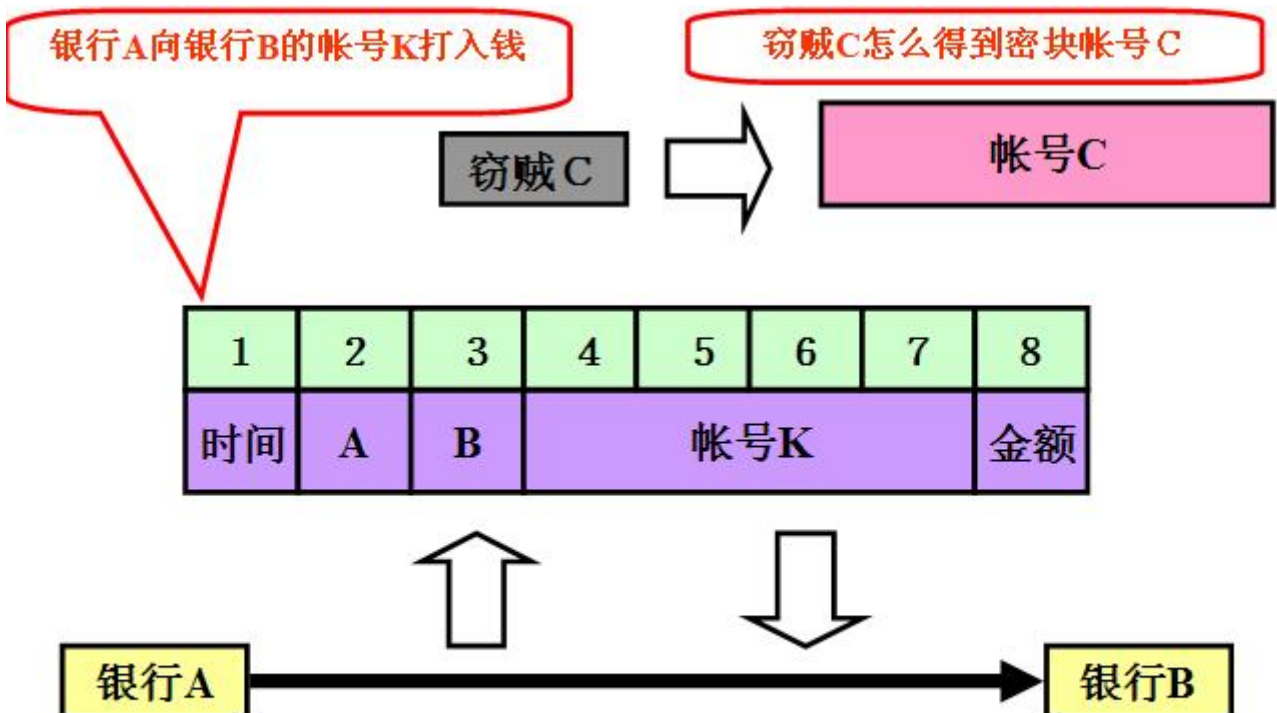
3.1 ECB模式

**优点:**

- 1. 简单;
- 2. 有利于并行计算;
- 3. 误差不会被传送;

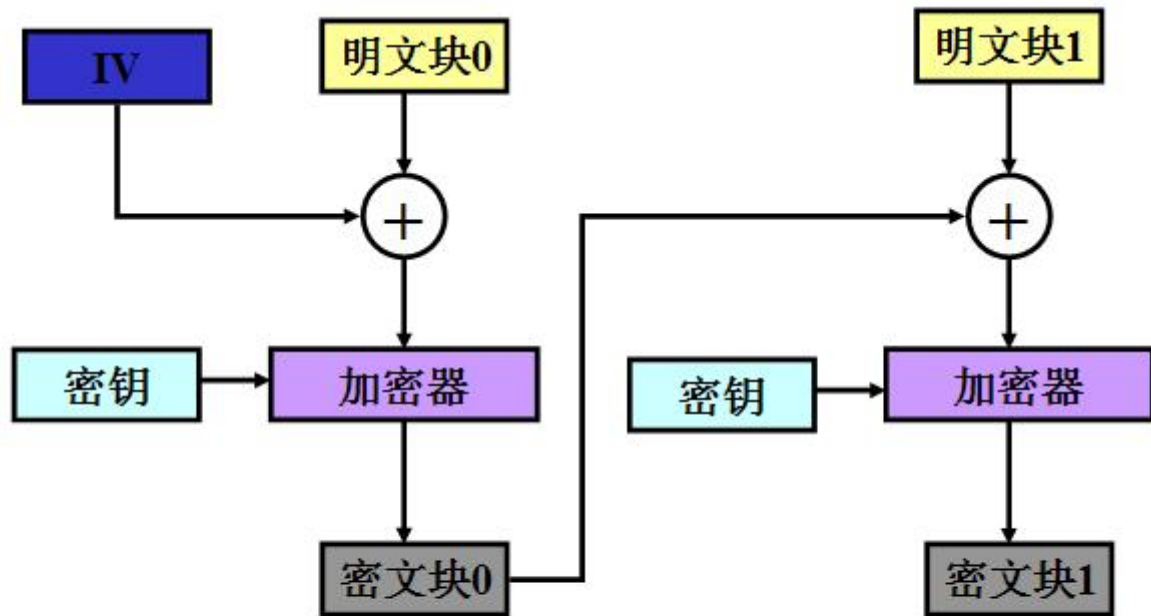
缺点:

- 1. 不能隐藏明文的模式;
- 2. 可能对明文进行主动攻击;



对ECB模式分组重放攻击

3.2 CBC模式:



这种模式称为CBC模式, 又密码分组链接

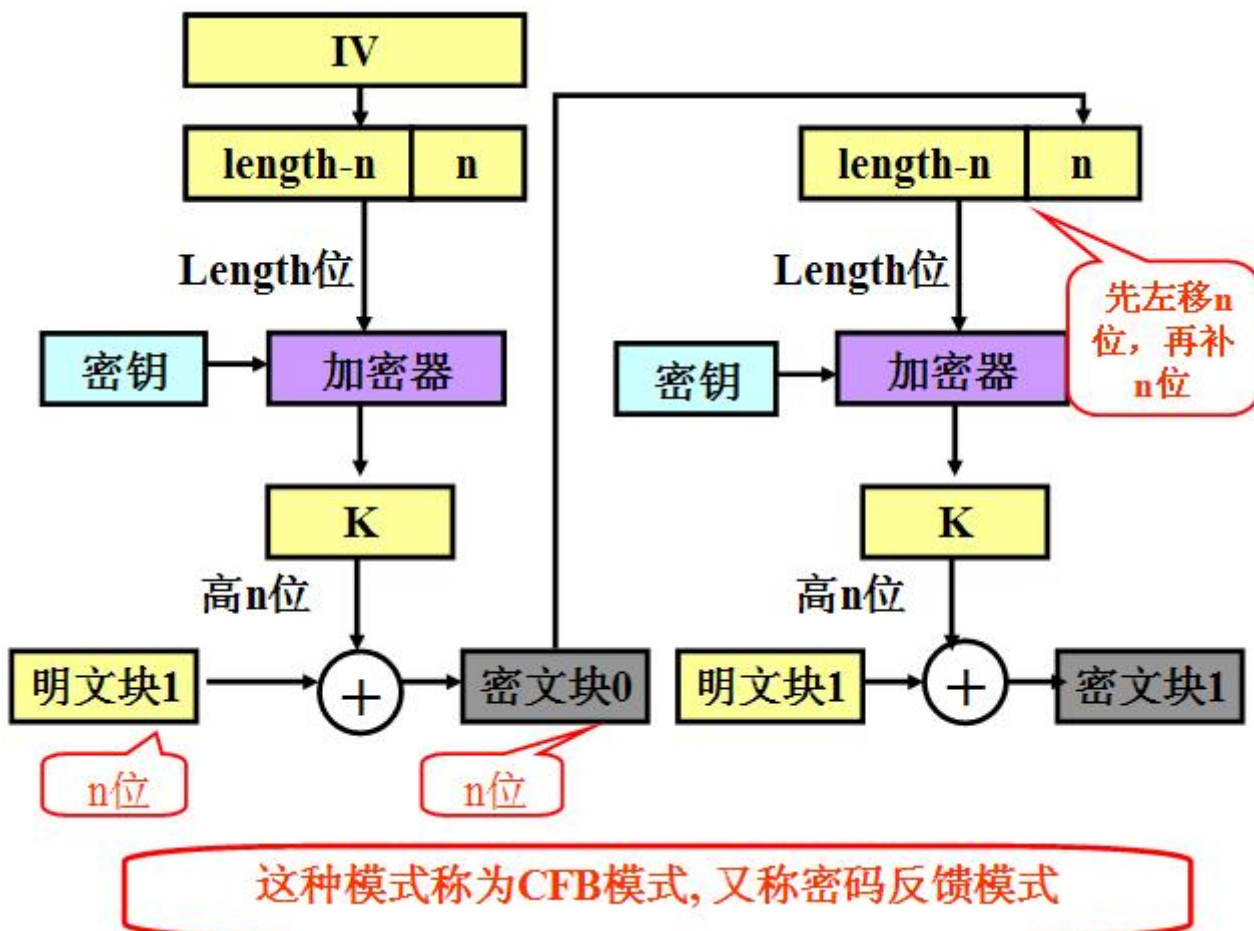
优点:

1. 不容易主动攻击, 安全性好于ECB, 适合传输长度长的报文, 是SSL、IPSec的标准。

缺点:

1. 不利于并行计算;
2. 误差传递;
3. 需要初始化向量IV

3.3 CFB模式:

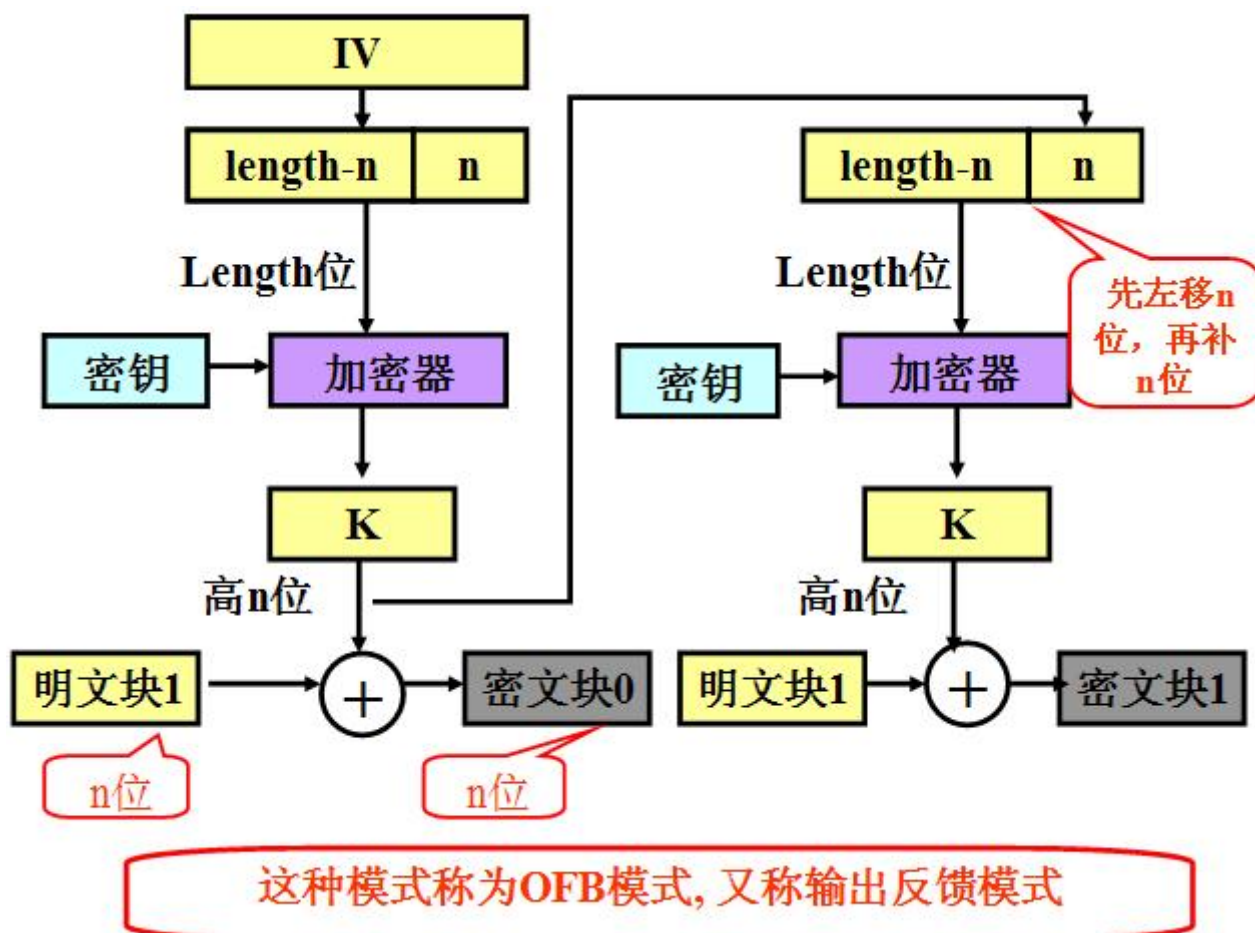
**优点:**

- 1.隐藏了明文模式;
- 2.分组密码转化为流模式;
- 3.可以及时加密传送小于分组的数据;

缺点:

- 1.不利于并行计算;
- 2.误差传送: 一个明文单元损坏影响多个单元;
- 3.唯一的IV;

3.4 OFB模式:

**优点:**

1. 隐藏了明文模式;
2. 分组密码转化为流模式;
3. 可以及时加密传送小于分组的数据;

缺点:

1. 不利于并行计算;
 2. 对明文的主动攻击是可能的;
 3. 误差传送: 一个明文单元损坏影响多个单元;
- 到底是4种还是5种啊
 - --吕吕_Louis
 - 示例图画得很清晰, 但这详解有点简短吧 🤔 🤔 🤔
 - --贼几把大

首先, 在百度API: <http://apistore.baidu.com/> 查找自己想用的api接口, 例如: 翻译:

字典

翻译

API调试工具: 去调试 >>

接口地址: http://apis.baidu.com/apistore/tranlateservice/dictionary

请求方法: GET

请求参数(header):

参数名	类型	必填	参数位置	描述	默认值
apikey	string	是	header	API密钥	您自己的apikey

请求参数(urlParam):

参数名	类型	必填	参数位置	描述	默认值
query	string	是	urlParam	请求的词语, UTF-8, urlencode编码	hello
from	string	是	urlParam	源语言语种, 目前支持中文、英文	en
to	string	是	urlParam	目标语言种, 目前支持中文、英文	zh

利用postman工具进行测试:

The screenshot shows a Postman interface for a GET request to `http://apis.baidu.com/apistore/tranlateservice/dictionary?query=hello&from=en&to=zh`. The request includes a header `apikey: f7be4...ede56...fd25 a0 d0`. The response is a JSON object with status 200 OK and time 384 ms.

```

{
  "errNum": 0,
  "errMsg": "success",
  "retData": {
    "from": "en",
    "to": "zh",
    "dict_result": {
      "word_name": "hello",
      "symbols": [
        {
          "ph_am": "he'lou",
          "ph_en": "hə'ləʊ"
        }
      ]
    }
  }
}
  
```

返回结果为JSON字符串:

```

{
  "errNum": 0,
  "errMsg": "success",
  "retData": {
    "from": "en",
    "to": "zh",
  }
}
  
```



```
"dict_result": {
  "word_name": "hello",
  "symbols": [
    {
      "ph_am": "hə'loʊ",
      "ph_en": "hə'ləʊ",
      "parts": [
        {
          "part": "int.",
          "means": [
            "哈喽, 喂",
            "你好, 您好",
            "表示问候",
            "打招呼"
          ]
        },
        {
          "part": "n.",
          "means": [
            "“喂” 的招呼声或问候声"
          ]
        },
        {
          "part": "vi.",
          "means": [
            "喊 “喂” "
          ]
        }
      ]
    }
  ]
}
```