FinTech

数据场景与加密算法的选择

人人聚财 郑创炎

企业为什么要有安全团队

怕数据被窃取

怕被攻击

怕形象受损

怕商业数据泄露

怕业务受损

怕被监管处罚

怕被薅羊毛

怕服务器被入侵

怕被合作方拒绝

怕客户流失

……

……

几个案例

Equifax数据开价600比特币

日本14亿邮箱密码信息泄露

南非有史以来最严重的数据泄露，泄露3000万身份证号码和财...

41家凯悦酒店被黑，客户支付信息等敏感泄露

超过100家汽车厂商敏感信息泄露，通用、丰田、特斯拉等无一...

德勤会计事务所所有员工信息以及管理账户遭泄露

美国最大儿童救助社区Boys Town数十万医疗保险数据泄...

必胜客官网被入侵，支付等敏感信息泄露

其实我只想搜几个而已.....

[redacted]微信手机支付。

ributor

nes (91 sloc) | 3.63 KB

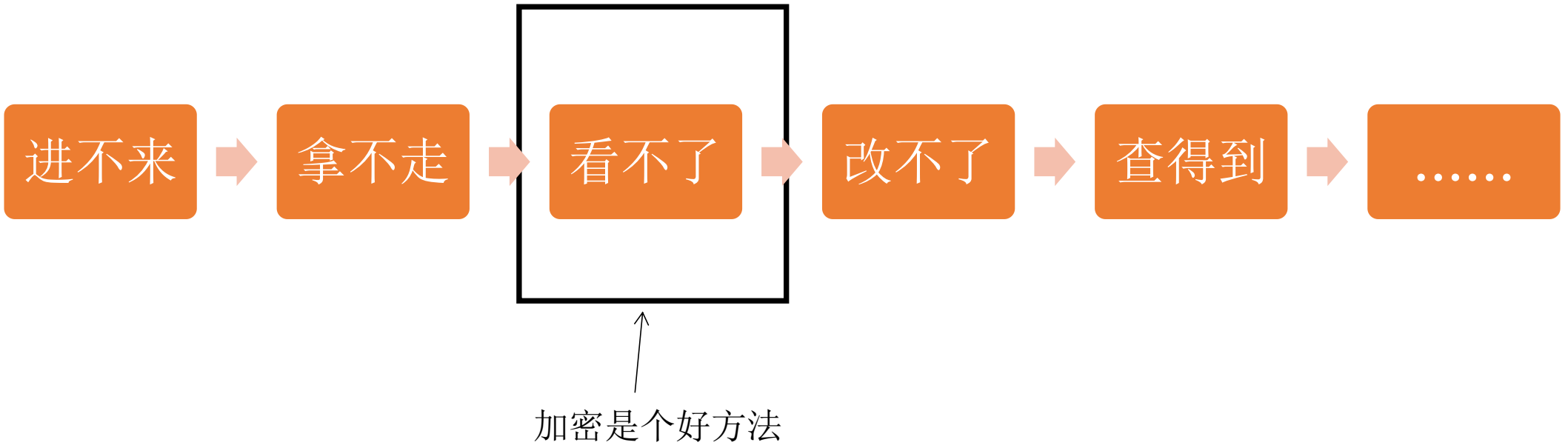
```php
<?php

class [redacted]fuConfig
{
    public static $version = 3;
    //商户ID
    public static $merId = '15[redacted]5';
    //手机充值卡支付数据提交URL
    public static $mobilePostUrl = 'http://pay3.sh
    //游戏点卡支付数据提交URL
    public static $gamecardPostUrl = 'http://pay3.
    //微信PC支付数据提交URL
    public static $weixinPostUrl = 'http://pay3.sh
    //微信手机支付数据提交URL
    public static $weixinMobilePostUrl = 'http://p
    //私钥,用于md5签名
    public static $privateKey = '123456';
    //des key，用于加密卡类信息
    public static $desKey = 'fN[redacted]nUm4=';
    //错误码
    public static $mobileCardErrorCodeText = [
```

[redacted]– conf.php

Showing the top two matches Last indexed 28 days ago

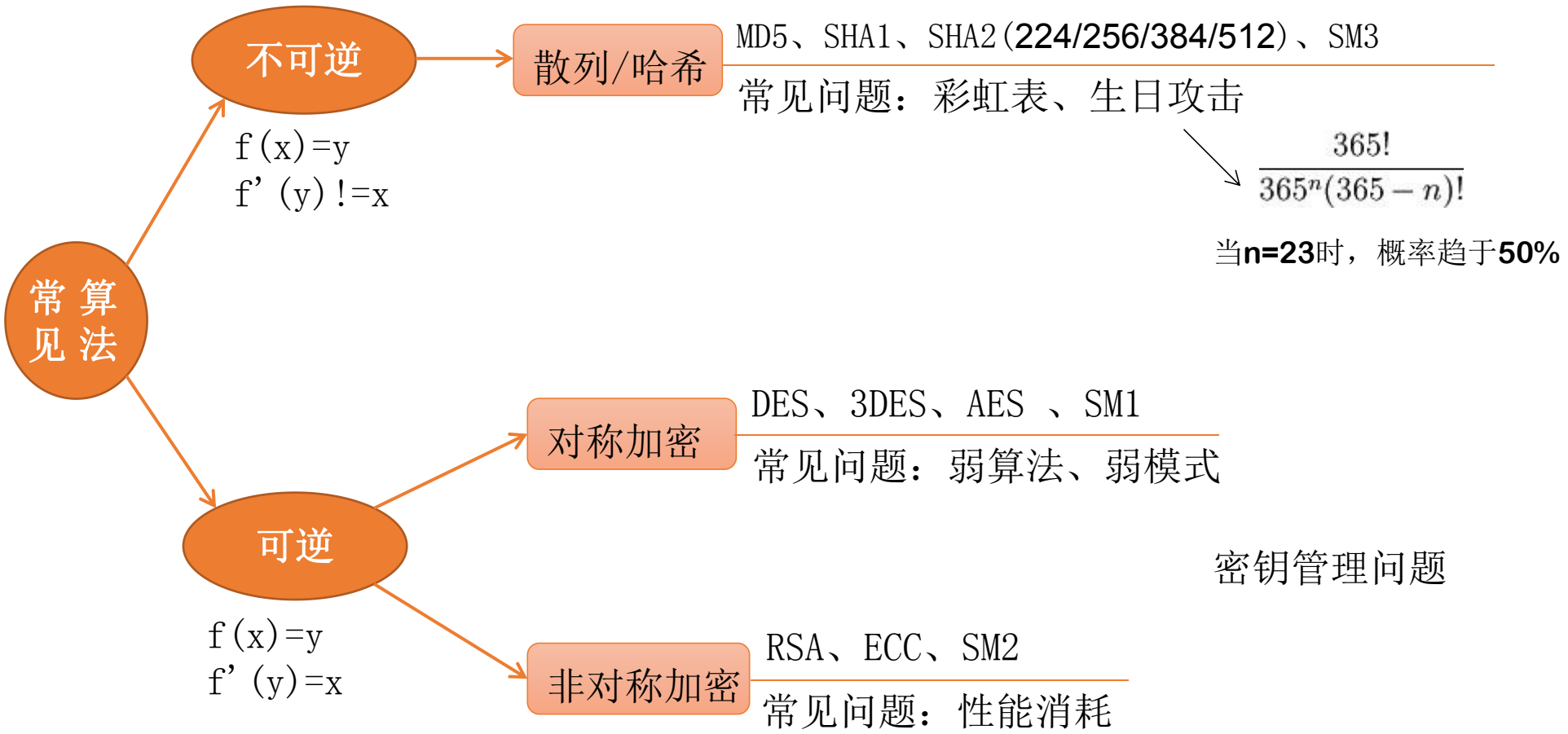
```
12          /*认证密钥，[redacted] 分配*/
13          'verifyKey'=>'9274819a4[redacted]cf9fe457d',
14          /*商户编号，[redacted]分配*/
15          'partnerId'=>'[redacted]',
16          /*应用编号， 商户*/
17          'appId'=>'xjbk',
18          /*生产URL*/
19          'url'=>'https://api[redacted]com/services/decision',
```

几个安全小目标



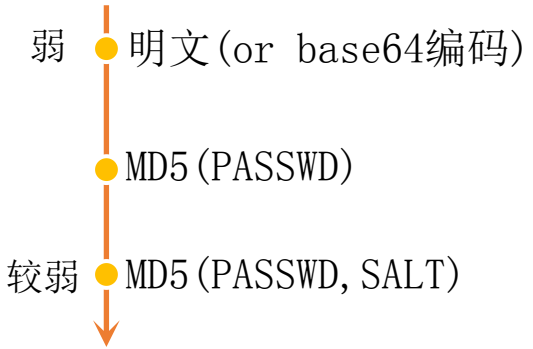
风险接受度决定安全力度

几个基本算法概念和问题



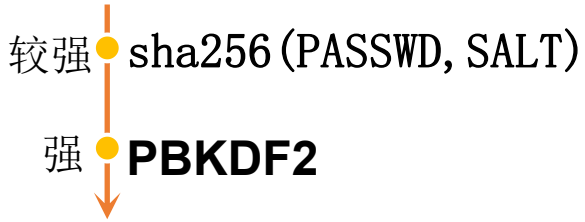
场景:用户密码保存

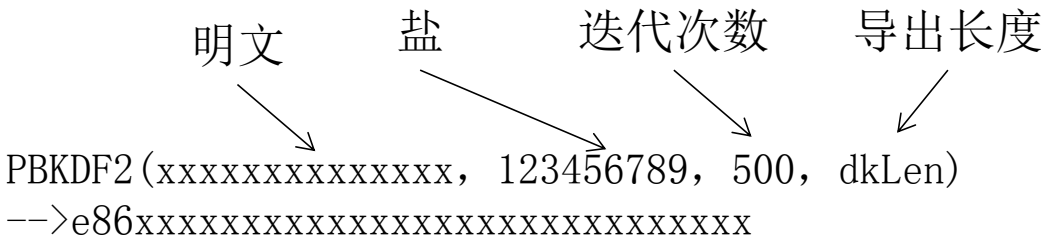
常见:



然后经常可以在cmd5.com上可以查到

推荐:

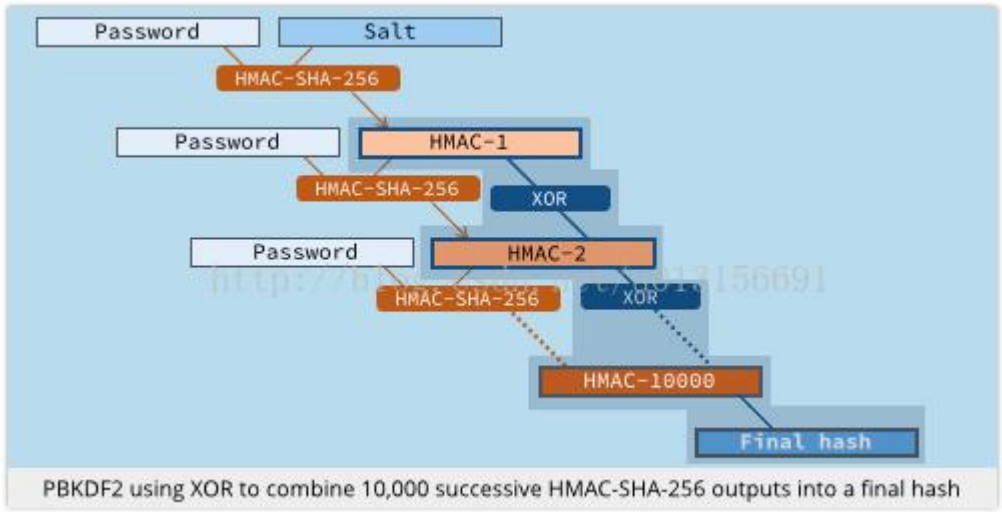




场景:用户密码保存

PBKDF2=Password-Based Key Derivation Function 2

基本原理是通过一个伪随机函数（例如**HMAC**函数），把明文和一个盐值作为输入参数，然后重复进行运算，并最终产生密钥。



PBKDF2 using XOR to combine 10,000 successive HMAC-SHA-256 outputs into a final hash

PBKDF2注意事项：

- 迭代次数500可以满足一般企业需求，当然更加推荐1000、5000、1W次以上
- 盐长度8字节以上
- hash算法采用SHA1或SHA2。

PBKDF2优势：

- 破解难度高，耗时长
- 目前没有公开的彩虹表
- 可以自定义迭代次数
- 计算成本可接受
- 建立一个彩虹表的时间及存储成本很高

场景:个人敏感信息保存-问题

个人财产信息	银行账号、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
网络身份标识信息	系统账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
其他信息	个人电话号码、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

常见敏感信息
- 身份证号
- 手机号码
- 住宅地址
- 住宅电话
- 户口所在地
- 银行卡号
- 电脑社保号
- 公积金号
- 微信、QQ
- 电子邮箱

《网络安全法》
第四十三条　个人……有权要求……删除其个人信息；……有权要求……更正。网络运营者应当采取措施予以删除或者更正。

GDPR第17条第1款，个人数据……不再必要时，数据控制者有责任及时删除其个人数据。

但是这里会有业务难题/坑：

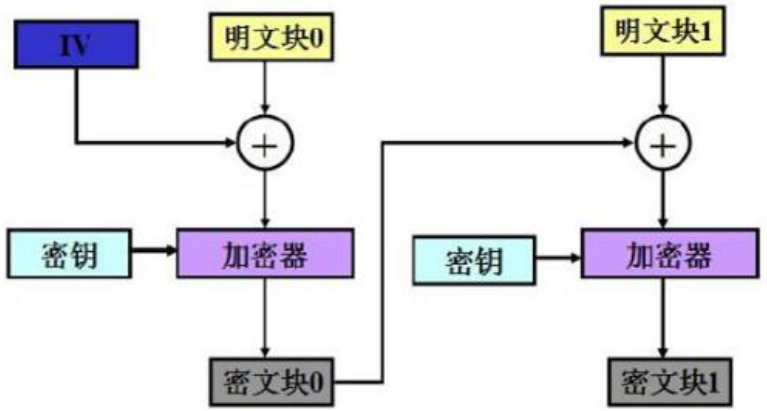
1，业务需要支持模糊搜索

2，法律要求数据删除权，备份的数据怎么删除干净

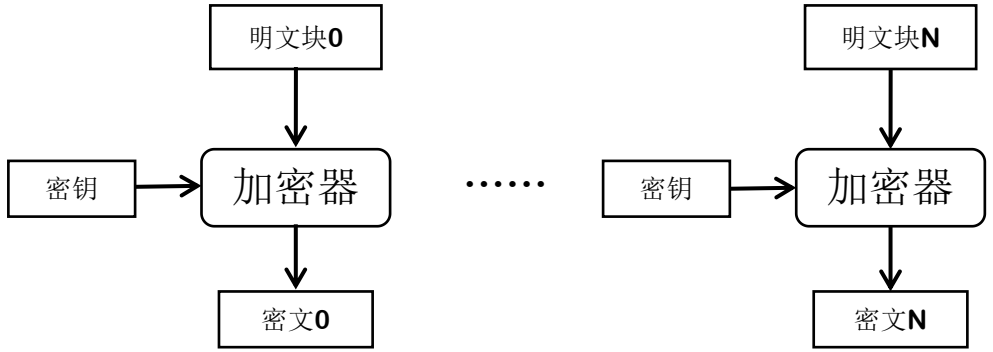
场景:个人敏感信息保存-方法

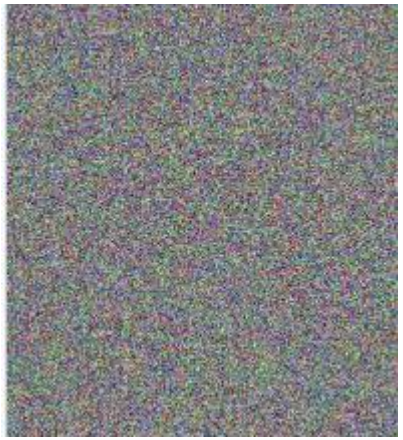
推荐：采用对称加密算法AES128，CBC模式

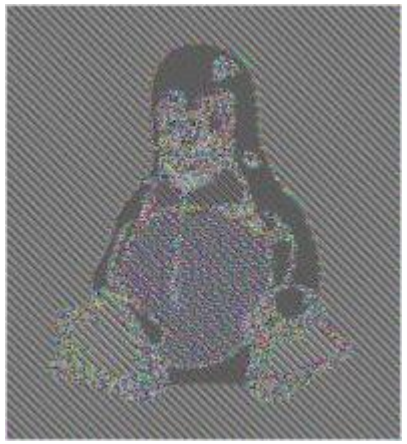
CBC模式



ECB模式

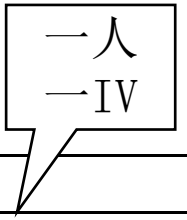






场景:个人敏感信息保存-实现

AESkey=123456



ID	昵称	住宅1	住宅2	IV
01	A1	广东深圳	U2Fxxxxx/Ac5KNHTLjlakbxxxxxR/41Norfh2**xxxxxx**	abcdef……
02	A2	广东广州	xxxxxVkXOdE+NgWTxxxxxxO5ZFZ2mtsxxxxxxxx	xyz123……

1，只加密部分关键字段，如住宅详细地址。
2，将单用户的IV删除，即可保证隐私数据不可恢复，满足删除权。

场景:配置文件里VerifyKEY的简单保护

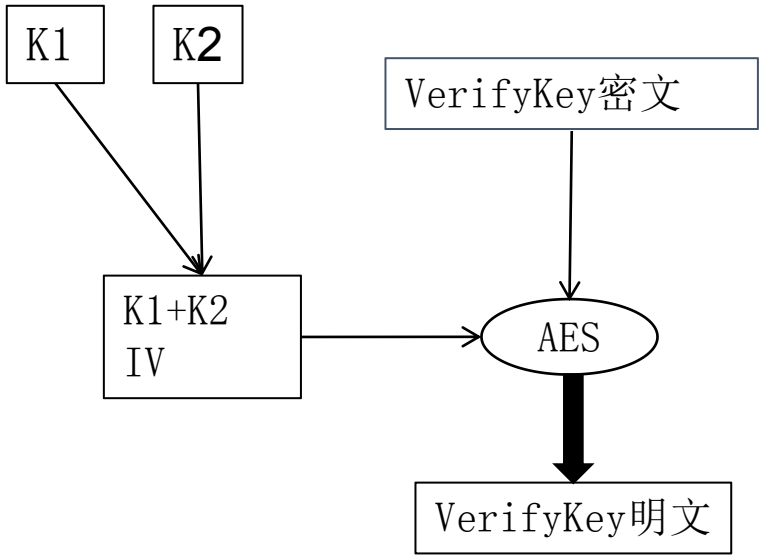
Verifykey=第三方认证**KEY**，前面用到的**AESKEY**，……

生成**Verifykey**密文：
AES_cbc_enc(k1+k2,iv,verify明文**)**

配置文件段存放:
K1=aaaaa
IV=vvvvvvv
VerifyKey密文=PPPPPPPP

代码段存放:
{
……
K2=XXXXXX
……
}

解密**Verifykey**：
AES_cbc_dec(k1+k2,iv,verify密文**)**



当然，你还可以使用更高级的密钥管理系统……

安全问题是可能发生的，

网络威胁是必然存在的。

欢迎交流