CTF_ CRYPTO(Cryptography)_密码学/密码编码学

原创

地热tan 已于 2022-02-21 10:56:40 修改 1961 收藏
文章标签： 安全 web安全 密码学
于 2022-02-04 15:33:04 首次发布

> 奶奶曾说过，教会他人，是验证自己学习的最好方式。

一、 简介：

> 密码学：主要是研究编制密码 和 破译密码的学科
>
> 密码编码学：主要研究对信息进行编码，实现信息的隐蔽。

二、密码学发展历史

古典密码：

古典密码是密码学的源头，古典密码中的密码技术大都比较简单，采用手工操作就可进行加密运算，现已很少使用。

近代密码：

因工业发展而产出的摩斯密码。

手工作业方式已难以满足复杂密码运算的要求，密码研究者设计出了一些复杂的机械和电动机械设备，实现了信息的加解密操作，近代密码时期宣告到来。例如：在二战期间德国的保密通讯技术就靠**恩尼格玛密码机**（Enigma）使德国在二战期间去的领先地位。

而随着德国的Enigma被破译，人们意识到其实真正保证密码安全的往往不是算法，而是密钥。即使算法外泄，但只要密钥保密，密码就不会失效。

现代密码：

在图灵科学家破解了Enigma扭转二战局势之后，密码的研究从帮助战争，逐渐走向生活，密码也逐渐变成了学科，有了成熟的发展，数学家们把编码变成数学问题——各种算法加密、函数加密、数字签名，让密码学这门学科才变得越来越百花齐放，人们对于数据的安全性提出了越来越高的要求。对于密码的载体本身也在变化。

三、基础概念

 总之，作者本人收集这方面的资料的时候看的一脸懵qwq， 他们同一个东西有好多叫法，整的我真心痛苦.....这里我直接整出了关键的几个点，太细了就不好理解，毕竟是衍生学科，各种名词的定义太乱了。就比如我搜的密钥什么意思，有的是说对称和非对称，有的是说，加密和解密，给我整不会了。

相关术语

非对称加密：加密和解密使用**不同**的秘钥，一把作为公开的公钥，另一把作为自己用的私钥。公钥加密的信息，只有私钥才能解密。私钥加密的信息，只有公钥才能解密。

对称加密：需要对加密和解密使用**相同**密钥的加密算法。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用。

密钥：是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。

明文：没有进行加密，能够直接代表原文含义的信息。

密文：经过加密处理处理之后，隐藏原文含义的信息。

加密：将明文转换成密文的实施过程。

解密：将密文转换成明文的实施过程。

密码算法：密码系统采用的加密方法和解密方法，随着基于数学密码技术的发展，加密方法一般称为加密算法，解密方法一般称为解密算法。

加密的基本原理

归根结底主要有两种编码方法：置换和代换。

置换(permutation cipher)：即把明文中的字母重新排列，字母本身的意思不变，但改变其位置，这样编成的密码称为置换密码，又称换位密码（transposition cipher)。

代换（substitution cipher）： 将明文中的字符替代成其他字符。

密码设计规则

- **安全性**

能够保证攻破密码所花费的成本比起破译后获得的利益高

- **机密性**

仅有发送方和指定的接收方能够理解传输的报文内容。窃听者可以截取到加密了的报文，但不能还原出原来的信息 ，即不能得到报文内容。

- **鉴别**

发送方和接收方都应该能证实通信过程所涉及的另一方， 通信的另一方确实具有他们所声称的身份。即第三者不能冒充跟你通信的对方，能对对方的身份进行鉴别。

- **报文完整性**

即使发送方和接收方可以互相鉴别对方，但他们还需要确保其通信的内容在传输过程中未被改变。

- **不可否认性**

如果人们收到通信对方的报文后，还要证实报文确实来自所宣称的发送方，发送方也不能在发送报文以后否认自己发送过报文。

四、密码学产物的发展历史

恺撒密码

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

它是一种替换加密的技术，明文中的所有字母都在字母表上按照一个固定数目（即，密钥）进行偏移后替换成密文。

例如：当密钥是3（偏移量）的时候。

```
Holle world —— Krooh zruog
#明文              #密文
abcd efg—— defg hij
#明文          #密文
```

这个加密方法是以罗马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。

栅栏密码

> 栅栏密码与其他的密码加密方式不太一样，它是直接对明文中的内容进行置换操作并不涉及明文中内容的改变！

加　　密　　原　　理

例如：当密钥是2（组）的时候。

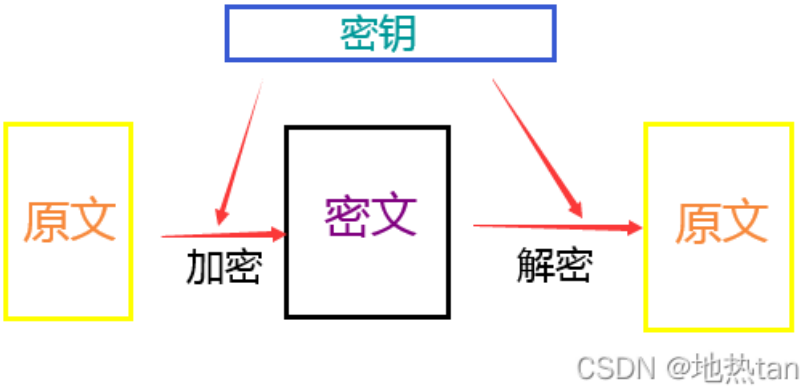
```
I LOVE YOU
 #明文

第一组：IOEO
第二组：LVYU

IOEOLVYU
#密文
```

原理很简单就是，先将明文上下，上下书写，然后横向排列得到密文。

对称加密

特征：加密与解密使用同一密钥

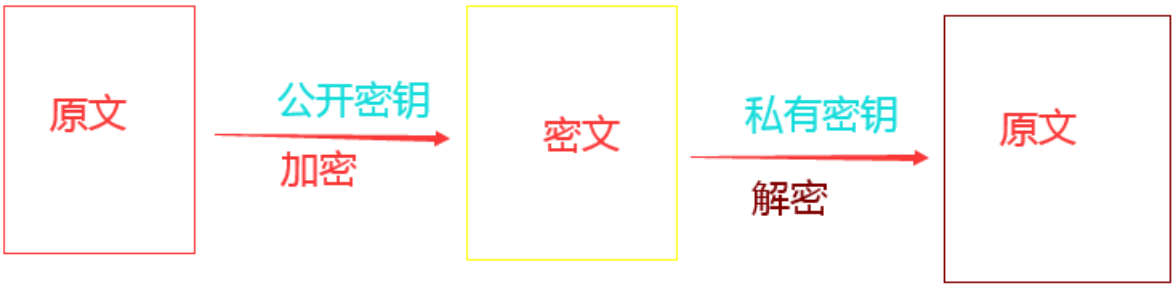
> 假设环境：A用密钥加密了个文件传给B，B收到文件后，用A给的密钥打开文件查看。
>
> 在这个环境里，存在的问题就是，若有人监听了A与B的通信，或拦截到A发给B的密钥，那A与B 的悄悄话就会被第三者C看到。



非对称加密

特征：加密与解密使用两个不同的密钥。

> 与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。



密码学未来发展

量子密码

> 在IBM的龙华实验室里，班奈特（Charles Bennett）是位知名而优秀的理论学家，也是量子计算这个新领域的创始者之一。就像其他多数理论学家一样，他待在实验室的经验并不多。他对于外在的事物漫不经心，有一次甚至把茶壶放在隔水加热器太久，从绿色煮成红色。不过，在1989年，班奈特和同事斯莫林（John A. Smolin）以及布拉萨（Gilles Brassard）决定放手一搏，着手进行一项开创性的实验。他们根据量子力学的原理，展示了一种新的密码技术。
>
> 在这个实验里，他们让光子在一个昵称为“玛莎阿姨的棺材”的光密盒里走了30公分。光子振荡（偏振化）的方向，代表一连串量子位元里的0与1。量子位元构成密码的“钥匙”，可以对讯息加密或解密。窃听者之所以刺探不到钥匙，是由于海森堡的测不准原理—这是量子物理的基础之一，当我们在测量量子态的某个性质时，会使另一个性质受到扰动。在量子密码系统里，任何窃取者在偷看光子束时都会更动到它，而被发送者或接收者察觉。原则上，这种技术可以做出无法破解的秘密钥匙。

简单来说就是，量子这玩意，是真实存在的，而且已经运用在密码学上了，但是按照预计，如果量子计算机研究出来了，那么从它惊人的计算能力，以前的密码形式就变得更加渺小。

但这东西更为概念化，根据量子的设定就是无法被观测、无论多远的两个粒子都能发生相同的改变，所以真的能应用在密码学上我觉得666啊。