



尔真 识理 真释 理尔

加密与解密

广州协和学校 信息技术科 陈钧鉴

2025年4月14日



广州协和学校



尔 识 真 理
真 理 释 尔

视频：都是密码，为什么我的不到1秒被破解，他的要64亿年？

你觉得你的密码足够安全吗



尔 识 真 理
真 理 释 尔

常见的密码盗窃方式

- 肩窥方式
 - 偷窥他人输入密码过程以窃取密码
- 字典破解
 - 密码字典里存储人们经常使用的密码
- 暴力破解
 - 穷举每一个可能的密码





尔 识 真 理
真 理 释 尔

学习任务1：密码防盗窃

- 与同学交流、讨论并使用deepseek，思考这三种盗窃方式相应的防盗措施，填入表中。

盗窃方式	防盗窃措施
肩窥方式	我们可以在输入密码时遮挡自己的操作过程，防止别人偷看密码信息；或者确定环境安全后再操作。
字典破解	
暴力破解	



尔 识 真 理
真 理 释 尔

学习任务1：密码防盗窃

- 与同学交流、讨论并使用deepseek，思考这三种盗窃方式相应的防盗措施，填入表中。

盗窃方式	防盗窃措施
肩窥方式	我们可以在输入密码时遮挡自己的操作过程，防止别人偷看密码信息；或者确定环境安全后再操作。
字典破解	不要用电话号码、身份证号码或生日；不要使用整个用户ID或用户ID的一部分；不要使用字典中的词语。
暴力破解	使用长度不少于8个字符的密码，密码使用字母、数字和特殊字符相结合。



学习任务2：破解密码用时

- 请你打开教师文件夹中的“数据安全性测试.py”，运行并测试穷举搜索一个5位、7位和9位的数字密码，分别需要多长时间，然后填写表2。

tk

输入密码: 12567

破解用时: 0秒0.286毫秒

破解

密码长度	密码值	破解时间
5位	12567	0.289毫秒
	98302	2.134毫秒
7位		
9位		



学习任务2：破解密码用时

- 请你打开教师文件夹中的“数据安全性测试.py”，运行并测试穷举搜索一个5位、7位和9位的数字密码，分别需要多长时间，然后填写表2。

tk

输入密码: 12567

破解用时: 0秒0.286毫秒

破解

密码长度	密码值	破解时间
5位	12567	0.289毫秒
	98302	2.134毫秒
7位	1000000	21.986毫秒
	9999999	226.32毫秒
9位	100000000	2秒266.975毫秒
	999999999	22秒854.013毫秒



尔 识 真 理
真 理 释 尔

创建安全密码的一般技巧

- 使用长度**不少于8个字符**的密码。密码长度越长越不容易被破解。
- 在可能的情况下，**尽量使用字母、数字和特殊字符**（如\$、#）相结合的密码。
- **不要使用电话号码、身份证号码或生日**等信息作为密码。
- **不要使用整个用户ID**或用户ID的一部分作为密码。
- **不要使用字典中能找到的词语**作为密码，即使是字母次序颠倒过来的常用词语也不可以。



尔 识 真 理
真 理 释 尔

加密与解密

- 原始信息（数据）称为**明文**，加密后的信息（数据）称为**密文**。
- **加密**
 - 将原始信息（数据）隐匿起来，使之在缺少特殊信息（数据）时不可读。
- **解密**
 - 将密文还原成明文的过程。
- **密钥**
 - 加密、解密算法中的一组数字。





尔 识 真 理
真 理 释 尔

历史上的加密方法

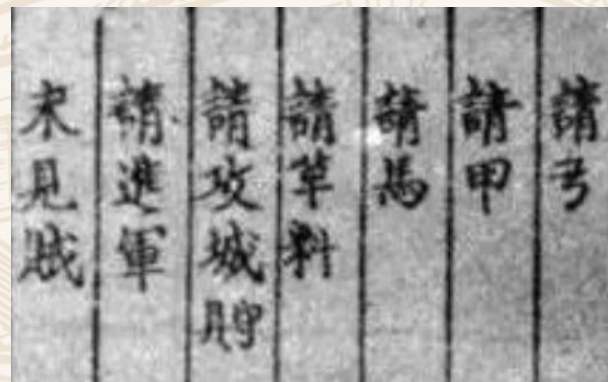
• 阴符

- 周朝，长度不同的竹片代表不同内容，比如，三寸表示溃败，四寸表示将领阵亡，五寸表示请求增援，六寸表示坚守……

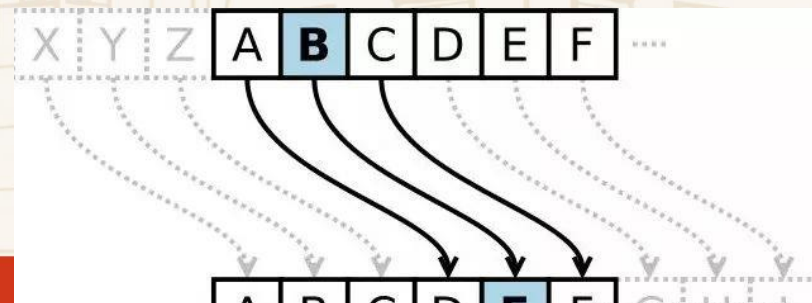


• 字验

- 宋代，后方指挥机关同这位将领约定用一首四十字的五言律诗作为**密钥**，并发给将领一本有40个短语编码顺序的密码本，编码顺序可变化。比如：1.请弓；2.请箭；3.请刀……



• 凯撒加密





凯撒加密

- 恺撒密码作为一种最为古老的**对称加密体制**，在古罗马的时候已经很流行，它是**加法密码**的典型代表。
- 加法密码又被称为移位密码。在加法密码算法中，明文中的所有字母都**在字母表上向后（或向前）按照一个固定数目进行偏移**后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推，将变成A，变成B，变成C。

恺撒密码明文、密文对应表

明文	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
ASCII码	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
密文	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
ASCII码	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	65	66	67



尔 识 真 理
真 理 释 尔

学习任务3

- 恺撒密码是将明文中的每一个字母用字母表中该字母后的第 3 个字母替换。例如，将明文中的 A 用 D 替换，B 用 E 替换，……，Z 用 C 替换，这就是恺撒密码。
- 请思考并回答 “BOY”加密后是什么？登录协和OJ作答。

明文 ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文 DEFGHIJKLMNOPQRSTUVWXYZABC



尔 识 真 理
真 理 释 尔

学习任务4：加密

- 密文的ASCII码=明文的ASCII码+3
- ord函数：将字符转化为ASCII码
- chr函数：将ASCII码转化为字符
- 修改凯撒加密程序
- 实现移 5 位的加法密码。

```
1  # 凯撒密码加密程序（字母向后移动3位，x/y/z绕回a/b/c）
2
3  # 输入明文
4  c = input()
5  b = "" # 初始化空字符串用于存储密文
6
7  for i in range(len(c)):
8      # 处理 a-w 或 A-W 的字母：直接后移3位
9      if "a" <= c[i] <= "w" or "A" <= c[i] <= "W":
10         # ord()获取ASCII码，+3后转回字符
11         b += chr(ord(c[i]) + 3) # 等效于 b = b + ...
12
13     # 处理 x-z 或 X-Z 的字母：后移3位后绕回开头
14     elif "x" <= c[i] <= "z" or "X" <= c[i] <= "Z":
15         # 例如：x(120) -> 123-26=97 -> a
16         b += chr(ord(c[i]) + 3 - 26)
17
18     # 处理非字母字符（数字、符号等）：保持原样
19     else:
20         b += c[i]
21
22 # 输出密文
23 print(b)
```



尔 识 真 理
真 理 释 尔

学习任务5：解密（选做）

- 修改凯撒加密程序，实现凯撒解密程序。（选做）





尔识真理
真理解尔

学习任务5：解密（选做）



- 修改凯撒加密程序，实现凯撒解密程序。（选做）

密文b	d~z	D~Z	a~c	A~C	其他
明文c	a~w	A~W	x~z	X~Z	不变
规律	ASCII码-3	ASCII码-3	ASCII码+23	ASCII码+23	不变
公式	'd'<=b[i]<='z' or 'D'<=b[i]<='Z'		'a'<=b[i]<='c' or 'A'<=b[i]<='C'		
	chr(ord(b[i])-3)		chr(ord(b[i])+23)		b[i]



尔 识 真 理
真 理 释 尔

数据安全和法律社会责任

- 《中华人民共和国网络安全法》第四十二条规定
 - 网络运营者不得泄露、篡改、毁损其收集的个人信息；**未经被收集者同意，不得向他人提供个人信息。但经过处理无法识别特定个人且不能复原的除外。**网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
- 某公司的网站收集了个人和企业等大量公民信息，对于明显存在的数据安全风险，该公司**未采取数据加密**等有效的技术保护措施，来确保其储存的信息安全，导致**约 22 万条个人信息数据被挂在境外论坛售卖**。对涉案公司及其直接负责人分别作出**罚款 20 万元、3 万元**的行政处罚。



尔 识 真 理
真 理 释 尔

总结

- 防盗窃措施

- 肩窥方式：输入密码时**遮挡**操作过程。
- 字典破解：**不用生日、手机号、用户ID**等字典的词语
- 暴力破解：用字母、数字、**特殊符号**且**不少于8个字符**的密码

- 认识数据安全的重要性，学会设置密码的小窍门

- 使用Python体验简单的穷举算法

- 了解加密解密的概念和一般过程

- Python实现加密、解密算法

- 数据安全意识、合法使用意识

