S&H BOX

密码算法核心组件分析软件

使用说明书

目录

1、引言

1.1 编写目的

为帮助用户更好地理解 S&H BOX 密码算法核心组件分析软件的操作方法和运行流程、更加方便地使用此产品进行需要的密码学性质测试，我们编写了此产品说明书。依照本说明书，无论是密码设计人员、密码分析人员还是密码学习人员均可快速掌握使用方法及项目基本组织过程。

1.2 项目背景

本作品为第三十二届“冯如杯”竞赛主赛道参赛作品，不涉及国家秘密，不触犯国家法律法规。

1.3 定义与参考

以下给出本软件支持测试的密码学性质、各参考值与代表性举例测试结果数值。

S 盒：

	参考值	AES	对应攻击/性能
SAC	**0.5**	**0.5048828125**	**扩散**
BIC	**0**	**0**	**混淆**
双射	**True**	**True**	**混淆**
平衡性	**True**	**True**	**混淆**
不动点	**0**	**0**	**混淆**
分支数	**m+1(↑)**	**3**	**线性/扩散**
扩散准则	**True**	**False**	**扩散**
相关免疫性	**True**	**True**	**混淆**
代数正规型	**——**	**——**	**表达形式**
代数次数	**n-1(↑)**	**7**	**差分**
代数项数	**(↑)**	**126.625**	**线性**
差分均匀性	**(↓)**	**0.015625**	**差分**

差分分布表	**——**	**——**	**差分**
非线性度	$2^{n-1}-2^{\frac{n}{2}-1}$**(↑)**	**112**	**线性**
线性逼近优势	**(↓)**	**0.0625**	**线性**
线性逼近表	**——**	**——**	**线性**

Hash 函数：

	参考值	MD5	对应攻击/性能
均匀分布	**True**	**True**	**均匀分布/输出随机**
完备度	**1**	**1**	**混乱和扩散**
严格雪崩准则度	**1**	**0.982450**	**混乱和扩散**
平均变化比特	**n**	**63.9862**	**混乱和扩散**
比特变化概率	**0.5**	**0.4999**	**混乱和扩散**
平均绝对距离	**↑**	**1361.1030**	**抗碰撞性**
单位字平均距离	**↑**	**85.0689**	**抗碰撞性**
平均运行速度	**——**	**0.007684**	**运行速度**

2、软件概述

2.1 目标

本作品聚焦密码算法中的核心组件——S 盒及哈希函数的密码学性质，实现了常见分析方法的集成和完善，制作了直观实用的分析软件。

2.2 功能

该密码性质分析检测的实用性软件能够根据相应理论，具体测试密码学 S 盒包括平衡性、非线性度、差分均匀性、代数表达式在内的 14 种密码学性质的分析、哈希函数均匀分布性、初值敏感性、抗碰撞程度等多类型性质指标。使用者可通过说明手册后续介绍详细了解软件使用方法及测试反馈数值的含义和参考值，从而针对性地根据反馈建议做出密码设计、密码分析上的调整改进。

2.3 性能优势

- 支持多文件类型输入
- 运行环境迁移
- 各形式 S 盒（压缩+非压缩）及 Hash 函数

3、运行环境

含“C:\Users\Public”文件地址的 64 位 Windows 环境。

4、使用说明

4.1 安装和初始化

直接或从产品网页 http://sh-assessbox.com/页面获取软件压缩包，解压后即可使用。

./dist：可执行文件.exe 所在目录，双击.exe 文件开始运行（可创建快捷方式使用）

./Sboxtest：S 盒测试模块源码

./Hashtest：Hash 函数测试模块源码

4.2 输入

4.2.1 文件背景

本产品支持输入 Python、等多种编程语言编写的测试，出于调用需要，文件命名存在一定要求。

4.2.2 文件格式

Python：

输入文件名：Sbox.py / hash.py

其中　Sbox.py 中需要有可使用的函数，命名为 sbox；

Hash.py 中需要有可使用的函数，命名为 hash_function。

C：

输入文件名：Sbox.so / hash.so

将 Sbox.c 转换为 Sbox.so：在 cmd 命令窗口中存储 Sbox.c 文件的路径文件夹下输入 gcc Sbox.c -shared -o Sbox.so

例：

```
C:\Users\Administrator\Desktop>gcc Sbox.c -shared -o Sbox.so
```

将 hash.c 转换为 hash.so：在 cmd 命令窗口中存储 hash.c 文件的路径文件夹下输入：gcc hash.c -shared -o hash.so

```
C:\Users\Administrator\Desktop>gcc hash.c -shared -o hash.so
```

其中 Sbox.c 里需要有可使用的函数，命名为 sbox；

Hash.c 里需要有可使用的函数，命名为 hash。

MATLAB：

输入文件名：sbox.m/ hash_function.m

其中 Sbox.py 中需要有可使用的函数，命名为 sbox；

Hash.py 中需要有可使用的函数，命名为 hash_function。

4.3 输出

4.3.1 文件背景

输出结果被统一保存在地址"C:\Users\Public\testSH"，含一份结果反馈文档、文档中性质展示图片及文档中不便展示的性质具体数据。

4.3.2 文件格式

反馈文档：测试结果.docx

图片：.png

具体数据文档：.txt

其中，反馈文档含有测试数据和根据测试数据提出的建议，用户可根据建议对所测试的密码学核心组件进行进一步认识、修改或分析。

4.4 出错和恢复

若软件无法正常运行，请检查以下方面是否符合输入需求：

• 软件安装环境是否符合：请选择适用操作系统。

• 软件安装是否完整：请对照压缩包包含项目表，补全或重装文件。

• 程序输入及函数定义名称是否符合 4.2.2:请合理转换输入格式及命名。

• 相应输入框输入数据是否完整和正确：此输入框对应 S 盒出入比特长度，请根据待测试 S 盒设计思路相应填充。

• 是否点击分析开始、完成对应的“OK”按钮：待本页面操作完成后点击“OK”按键。

若以上操作后软件仍无法正常运行，可尝试等待重启操作，也欢迎您向我们及时反馈问题。

4.5 求助查询

本作品开发者联系方式：

联系方式 1：458882509@qq.com

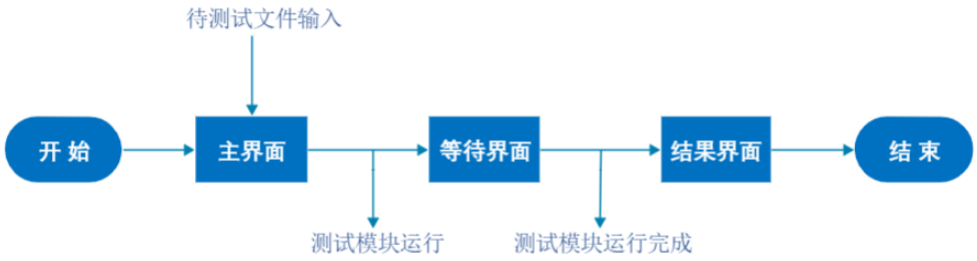
联系方式 2：guoying__gy@163.com

联系方式 3：2498421345@qq.com

如有问题，欢迎联系告知，也欢迎共同学习密码学知识。

5、运行说明

本产品运行时界面跳转如下：

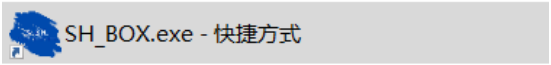


整体运行时，用户选择待测试文件、键入输入输出比特数后，点击主界面

“OK”按键，选择的测试文件被保存到指定运行地址、测试模块刷新文件模块的导入并开始运行，含进度条的等待界面弹出。关联测试模块运行进度的进度条加载完毕后点击等待界面“OK”按键，结果提示窗口弹出，显示反馈文件存放地址。

6、用户操作举例

解压压缩包，找到初始文件夹路径下的快捷方式，如下图所示。



也可以通过路径 unlock\dist\SH_BOX\SH_BOX.exe 找到可执行文件的原文件。双击 exe 可执行文件，出现测试主页面。打开的默认页面是 S 盒测试页面，可以通过左上角的选择按钮切换到 Hash 函数测试页面。如下图：

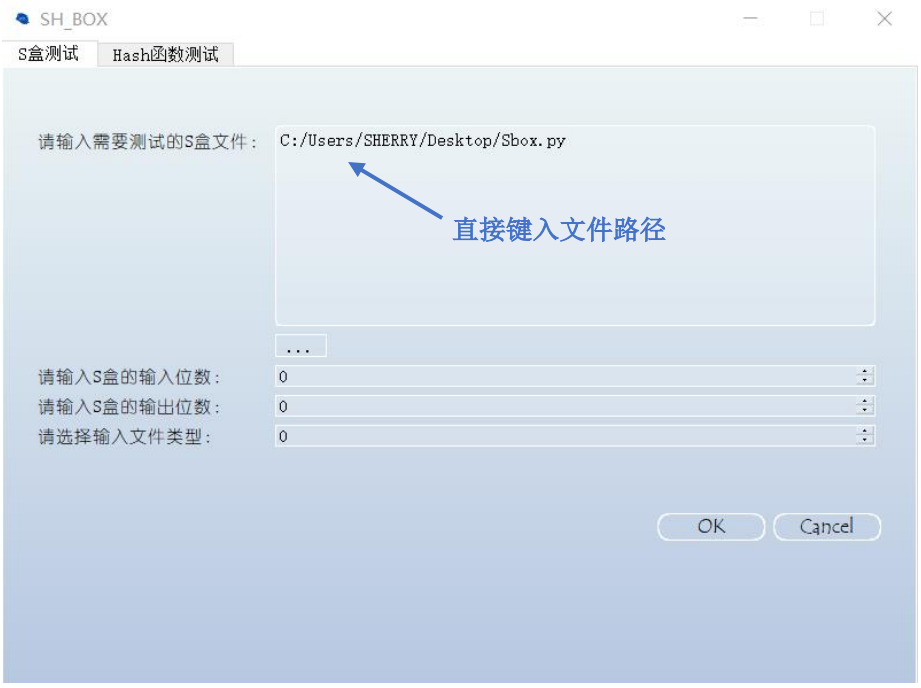
S 盒测试页面

Hash 函数测试页面

（1）S 盒测试步骤：

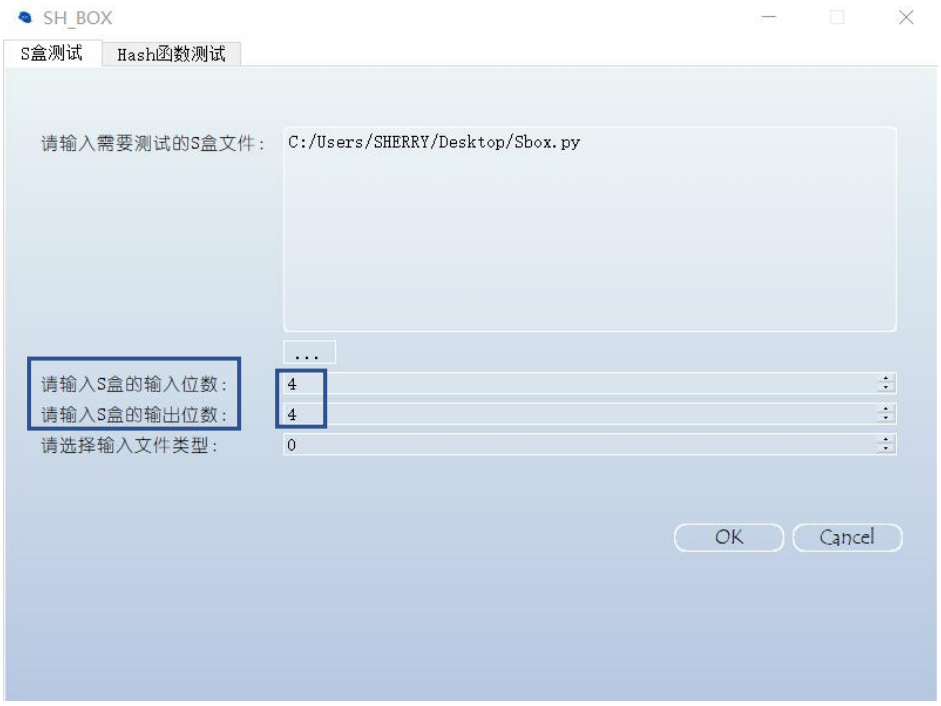
①点击“...”键选择 S 盒文件，或者在第一个输入框中直接输入 S 盒文件路径。

S 盒待测试文件输入（方法一）



S 盒待测试文件输入（方法二）

②根据待测 S 盒，正确填写输入输出的 bit 位数，这是程序正确运行的关键，请确保填写正确。



输入输出位数填写

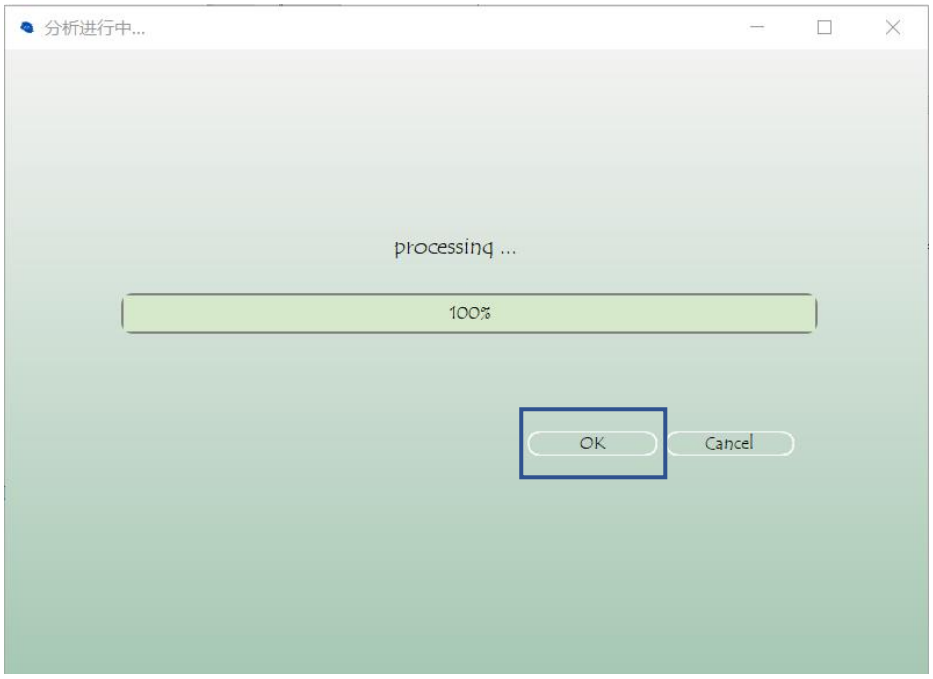
③选择输入文件类型，0 表示输入文件为 python 的.py 文件，1 表示输入文件为 C 生成的.so 文件，2 表示输入文件为 MATLAB 对应的.m 文件。默认值为 0，可以直接在输入框输入文件类型对应编号，或者通过右侧选择按键选择。

文件类型选择

④点击“OK”键，开始检测 S 盒性质。

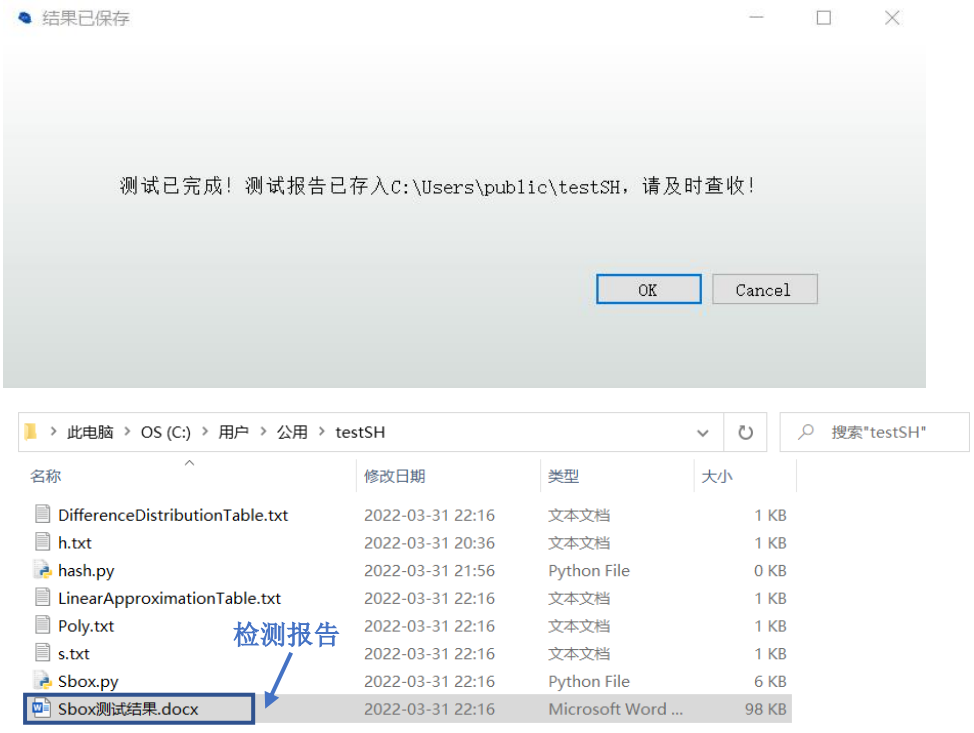
“OK”测试开始

⑤等待检测完成，进度条达到 100%，点击“OK”键。



“OK”结果显示

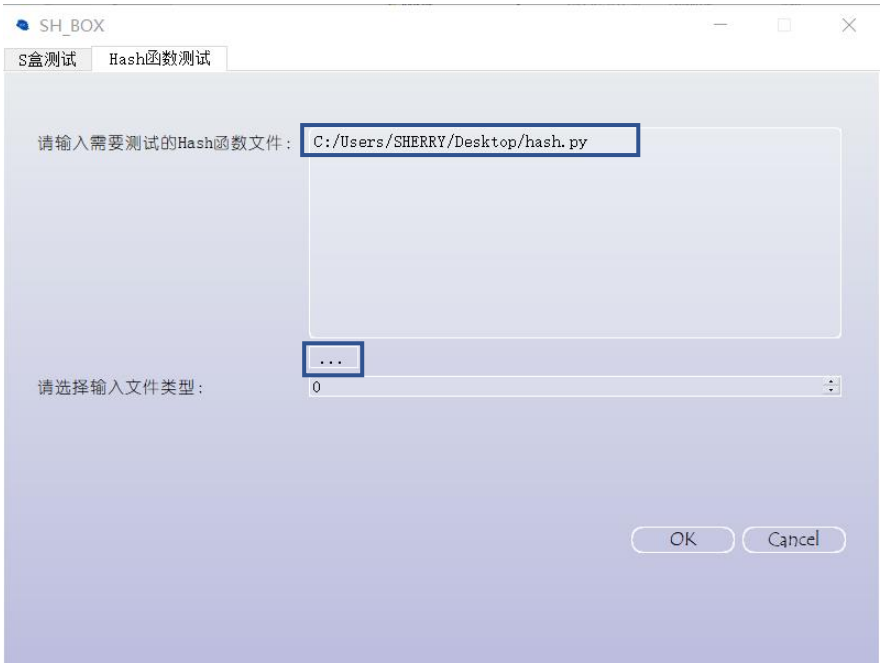
⑥显示检测完成，生成的检测报告的存储路径为 C:\Users\public\testSH，文件名为“Sbox 测试结果.docx”



报告生成与存储

（2）Hash 盒测试步骤：

①点击“...”键选择 Hash 函数待测试文件，或者在第一个输入框中直接输入 Hash 函数待测试文件路径。

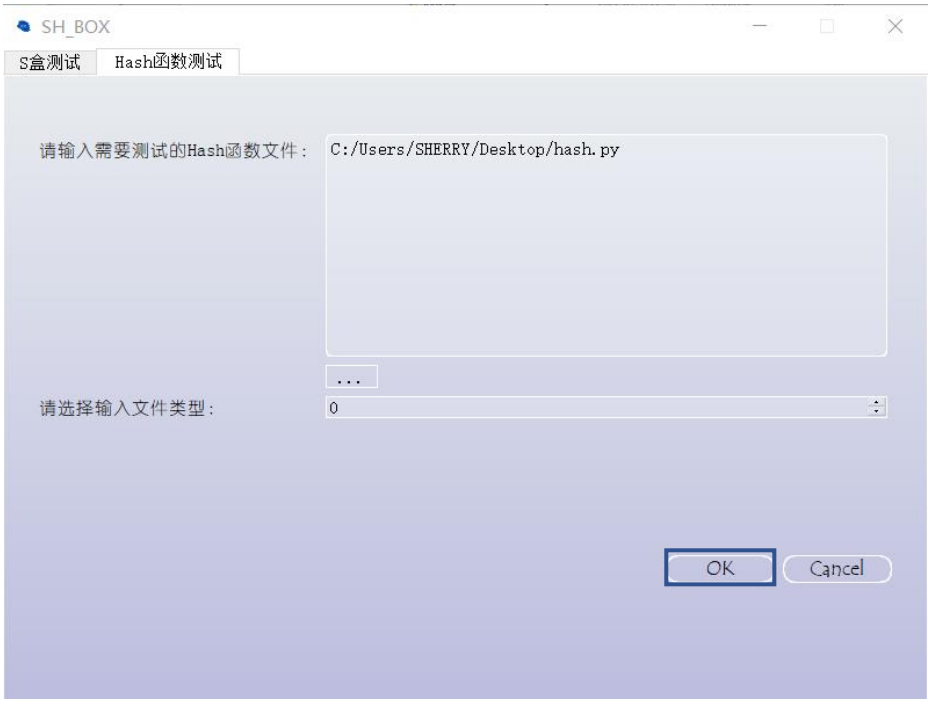


Hash 函数待测试文件输入

②选择输入文件类型，0 表示输入文件为 python 的.py 文件，1 表示输入文件为 C 生成的.so 文件，2 表示输入文件为 MATLAB 对应的.m 文件。默认值为 0，可以直接在输入框输入文件类型对应编号，或者通过右侧选择按键选择。

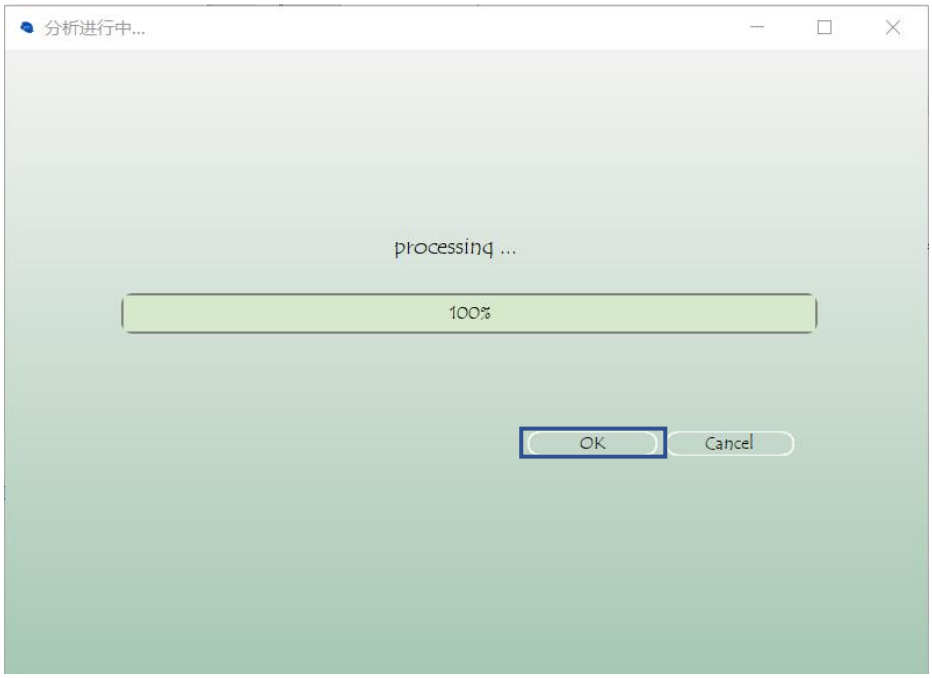
文件类型选择

③点击“OK”键，开始检测 Hash 函数性质。



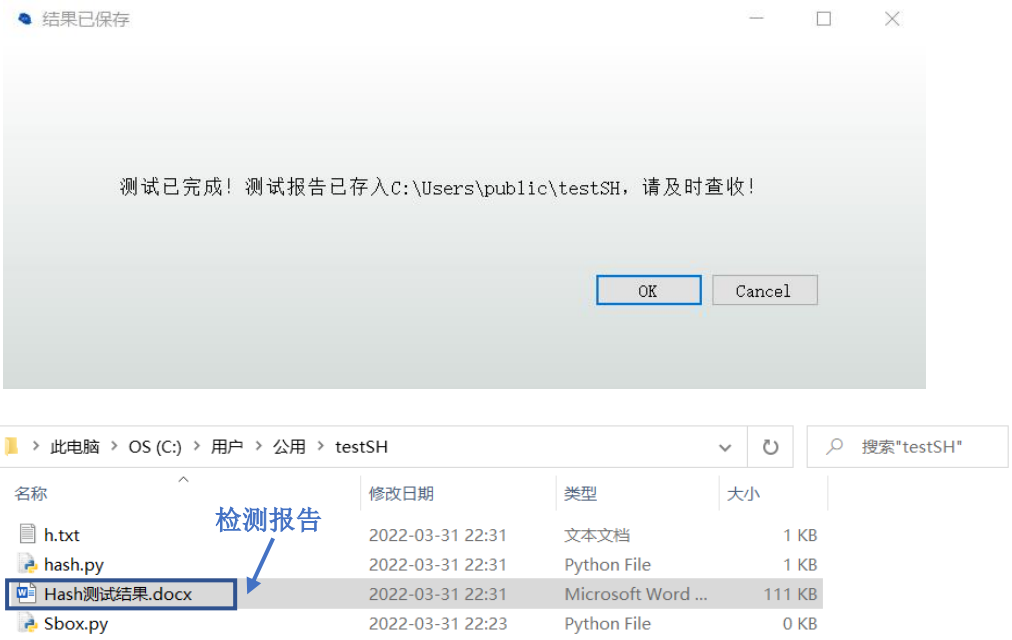
“OK”测试开始

④等待检测完成，进度条达到 100%，点击“OK”键。



“OK”结果显示

⑤显示检测完成，生成的检测报告的存储路径为 C:\Users\public\testSH，文件名为‘Hash 测试结果.docx’



报告生成与存储