GeekPwn2020

少年黑客马拉松大赛

比赛规则

(版本 1.3)

2020 年 GeekPwn 延续青少年安全竞赛的传统，精心准备了少年黑客马拉松大赛，为 10-16 周岁的少年黑客们学习网络安全技术和发挥创新精神提供舞台。

本文档内容已经同步在 GeekPwn 官网 www.geekpwn.org 上发布。

参赛要求

1. 面向 10-16 周岁，对信息技术和安全技术有强烈兴趣，具备较强编程动手实践能力的在校中小学生。
2. 以团队为单位报名参赛，每个团队参赛队员 1~2 人，带队老师 1 人，比赛时带队老师不可上场指导。
3. 参与评奖的所有参赛选手应在评奖前向主办方提交比赛相关设计文档和源代码，相关作品不得侵犯他人知识产权。若发现存在弄虚作假行为，主办方有权取消选手的获奖资格。

比赛形式

本次少年黑客马拉松比赛分为两个单项赛，选手可以分别报名参赛。

单项赛一：“少年黑客加密破解”挑战赛

挑战目标

在现场比赛中，主办方将一段字符格式的文本信息作为明文信息，经过加密处理成字符格式的密文信息后，以信号灯亮灭的方式将密文信息转成光信号发送。

参赛选手的目标是利用主办方提供的器材制作一个自动解密机设备，能够实现下列功能：

1. 自动接收信号灯亮灭的信号将其解析还原成密文信息；
2. 自动破解密文还原成明文信息。

在规定比赛时间内成功实现自动解密机功能并且用时短的选手将获得优胜。

规则说明

1. 比赛中使用的加密算法为古典加密方法，加密前后的信息都以大写英文字符（A~Z）、数字字符（0~9）和空格字符表示。在比赛现场，选手将获得相关加密算法的更多参考信息。选手可以利用这些信息对加密算法进行破解。更多信息可以参考常见问题 FAQ。
2. 信号灯亮灭的规则遵循 Morse 码编码方式，编码方式可以参考常见问题 FAQ。
3. 选手用于制作自动解密机设备的器材仅限主办方在比赛现场提供的硬件器材，主要包括树莓派 4B（Raspbian 系统），传感器如摄像头、发光二极管、光敏电阻等，以及其他外设和连接器材如显示器、鼠标、键盘、面包板、杜邦线等。比赛现场不提供 WiFi 网络，选手可以自带笔记本电脑。
4. 比赛时间限时 3 小时，超过时间则比赛结束。如果在比赛时间内选手提前完成自动解密机设备制作并提交到主办方，提交时间将作为比赛优胜评定依据之一。选手提交的内容包括自动解密机硬件和源代码。提交之后，在功能验证环节前选手不再对自动解密机进行修改。
5. 所有选手结束比赛后，主办方开始功能验证，开始功能验证前选手可以再次确认自动解密机设备工作正常。

6. 功能验证开始后，主办方会以信号灯发送 Morse 码的方式发送新的加密信息，测试选手提交的自动解密机设备。如果自动解密机能够在显示器上自动输出以下全部信息，则判定为功能验证通过。
   - 收到的 Morse 码信号和对应字符
   - 完整的密文信息
   - 破解后的完整明文信息

优胜评定

- 在比赛时间内完成提交自动解密机设备并通过功能验证的选手，按照提交时间先后顺序取前三名：

  第一名：奖学金 5000 元人民币
  第二名：奖学金 4000 元人民币
  第三名：奖学金 3000 元人民币

- 在比赛时间内完成自动解密机制作并验证成功，按照提交时间未进入前三名评选的选手，获得**优胜奖**及奖学金 2000 元人民币。
- 功能验证未通过或者未能在比赛时间内完成加密破解功能，但是能够实现接收 Morse 信号并解析成对应字符的选手，获得**鼓励奖**及奖学金 1000 元人民币。
- 所有参加现场比赛的选手都将在赛后获得决赛优秀证书。

单项赛二：“少年黑客生活卫士”开放赛

比赛主题：用奇思妙想解决生活中的安全问题
作品形式：选手提交基于开源硬件和传感器实现的作品，可以解决生活中可能遇到的安全问题，或者降低其中的安全风险。

生活中和安全相关的问题，可以参考：

- 如果厨房里忘了关火，如何检测可能存在着火的危险？
- 当家里没人的时候如何检测有没有人进入房间？
- 如果保存贵重物品的地方被翻动了，如何及时收到报警？
- 家里水龙头忘关了，如何检测可能会漫水？
- 能否检测到煤气泄漏？
- 在外面碰到危险，如何能安全快速地寻求帮助？
- 如何帮助视觉不便的人判断路上可能有障碍物？
- 如果遇到了坏人，有没有办法将坏人吓跑？

……

提交方式： 选手报名后，由主办方联系报名选手和指导老师确定提交过程。详细信息请参考参赛流程。

优胜评定：

- 参赛选手按年龄区分小学组（10-12 周岁）和中学组（13-16 周岁）分别进行优胜评定。
- 参加现场比赛前，选手必须向主办方提交作品的完整设计实现文档及源代码等。在现场比赛环节，选手向评委介绍演示提交的作品，并解答评委提出的问题。
- 评委从原创性、创新性、完整性、实用性等方面，对比赛选手作品按照小学组和中学组分别进行评审。每个年龄组分别设立一等奖、二等奖、三等奖和优胜奖。

  一等奖：奖学金 5000 元人民币
  二等奖：奖学金 4000 元人民币
  三等奖：奖学金 3000 元人民币
  优胜奖：奖学金 1000 元人民币

- 所有参加现场比赛的选手都将在赛后获得决赛优秀证书。

参赛流程

1. **选手报名**：在线提交 报名表，报名截止日期：9 月 30 日。

2. **线上初审**：收到报名信息后，主办方将联系报名选手和指导老师。选手须根据参加的单项赛提交作品进行线上初审。初审作品提交要求：
   - 报名“少年黑客加密破解”挑战赛的选手应根据现场比赛规则提交相关的参赛思路和方案。
   - 报名“少年黑客生活卫士”开放赛的选手应根据比赛要求提交符合比赛主题的作品。

   在评审过程中，选手可以继续优化其提交的作品。

   所有提交初审作品并符合主办方比赛要求的选手将在赛后获得**参赛纪念证书**。其中表现出色的选手将入围现场决赛，参与现场决赛评奖（与参赛纪念证书不重复发放）。

3. **现场决赛**：通过初审，获得现场决赛资格的选手参与现场决赛，按照现场决赛“优胜评定“原则进行评奖。
   现场决赛比赛日期：2020 年 10 月 24 日。

联系方式

报名参赛过程中有任何疑问，请邮件联系：
cfp@geekpwn.org
关于 GeekPwn 大赛的更多信息，请访问：
www.geekpwn.org
或关注微信公众号：geekpwn

常见问题 FAQ

参加“少年黑客加密破解”挑战赛需要具备哪些计算机和信息安全知识?

参加“少年黑客加密破解”挑战赛，需要对以下基础信息技术知识有一定的了解：

- 树莓派的基本功能，连接鼠标、键盘、显示器，以及利用树莓派、面包板、杜邦线、电阻连接常见的传感器如 LED 灯、光敏电阻等
- 在树莓派上用 Python 或其他编程语言进行编程，通过 GPIO 引脚读取传感器数据
- 密码学基础入门知识和常见古典加密算法原理和破解方法
- 摩尔斯 Morse 编码知识

“少年黑客加密破解”挑战赛里使用的古典加密方法是什么?

古典加密方法是密码学中的一个类型，主要是相对于现代加密方法而言。其大部分加密方法都是基于替换或移位方式，或者是两者的混合。古典加密方法主要在历史中经常使用，在现代加密方法出现之后已经很少使用了。不过古典加密方法理论仍然具有很高的学习价值。通过学习古典加密方法，可以了解前人设计密码的基本思路，及其成功经验和失败教训，从而更好的了解密码学的发展。

密码学中的一些常见术语：
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。
密钥：分为加密密钥和解密密钥，二者可以相同也可以不同。

古典加密方法一般使用**替换**和**移位**方法。**替换**指的是明文的字母用其他字母所代

替。最著名的替代算法是相传为凯撒大帝发明的恺撒密码（Caesar Cipher）。凯撒密码的原理很简单，就是把明文字母按字母表顺序用它后面某个位数的其他字母代替。这个位数只有加密和解密的双方知道，成为恺撒密码的秘钥。如果代替的字母超过了字母表中最后一位，就从字母表从头重新开始。例如，对于字母表“ABCDEFGHIJKLMNOPQRSTUVWXYZ”，位数为 3 的话，明文的 A 将被替换为 D，B 将会被替换为 E，C 将会被替换为 F，D 将会被替换为 G，依次类推，到字母表的最后 X 会被替换为 A，Y 会被替换为 B，Z 会被替换为 C。按照这种替换方法，明文“HIT”会被转换为密文“KLW”。假如要解密的话，只需要将密文中的字母按照约定的替换位数反向逆推回来就行。

移位指的是把明文中的字母重新排列，字母本身不变，但其位置改变了，这样形成的密码称为移位密码。最简单的移位密码是把明文中的字母顺序倒过来，然后截成固定长度的字母组作为密文。例如：

明文：明晨 5 点发动反攻。
MING CHEN WU DIAN FA DONG FAN GONG
密文：GNOGN AFGNO DAFNA IDUWN EHCGN IM

很容易看出上面介绍的古典加密替换和移位方法都很容易被破解。为了改进古典加密方法的安全性，人们又发明了很多基于替代和移位方法的变种。有兴趣的同学可以去网上搜索关于古典密码的更多信息来进一步学习。

比赛中使用的古典加密方法，也是使用类似的加密方式。进入现场决赛的同学将会获得比赛所用加密方法的更多描述信息。根据这些信息在现场通过编程就可以对加密信息进行破解。

“少年黑客加密破解”挑战赛里怎么通过信号灯亮灭的方式表示 Morse 编码？

“少年黑客加密破解”挑战赛通过信号灯亮灭的方式表示 Morse 编码。信号灯亮代

表信号发出，灯灭代表信号间隔或没有信号。灯亮的时间长度代表信号的长度。

Morse 编码规则可以参考下表。其中“-”表示划，“·”表示点。划一般是三个点的时间长度；点划之间的间隔是一个点的时间长度；字符之间的间隔是三个点的时间长度；单词之间的间隔是七个点的时间长度。一个点的具体时间长度在决赛现场确定。

英文字符 A~Z

字符	代码	字符	代码	字符	代码	字符	代码	字符	代码	字符	代码	字符	代码
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	--··				

数字字符 0~9

字符	代码	字符	代码	字符	代码	字符	代码	字符	代码
1	·----	2	··---	3	···--	4	····-	5	·····
6	-····	7	--···	8	---··	9	----·	0	-----

以“MORSE CODE”这段文字作为例子，转换成 Morse 码是这样的:

M O R S E (空格) C O D E

上面这段消息的发报时间可以如下表示（=表示有信号，.代表无信号，每个=和.代表一个点的时间长度)

除上述 Morse 编码外，比赛中不使用其他特殊 Morse 编码。如果信号超过 10 秒没有发生变化，可以视为信号传输结束。

“少年黑客加密破解”挑战赛里可以使用哪些硬件和软件？

“少年黑客加密破解”挑战赛现场比赛用到的硬件器材由主办方提供，主要包括树莓派 4B，树莓派兼容摄像头、发光二极管、光敏电阻等，以及其他外设和连接器材如显示器、鼠标、键盘、面包板、杜邦线等。树莓派 4B 预装 Raspbian 系统，其自带的 Python3.0 和功能库就能够实现比赛目标。除了指定的树莓派硬件外，如果选手对主办方提供的传感器型号有疑问，或想使用其他的传感器，或其他的编程语言和功能库等，可以与主办方确认和协商，在不违反比赛规则的前提下，主办方会提前准备好相关的硬件和软件。