

# 2016年12月·第1套 英语四级长篇阅读（信息匹配） 第1篇·36-45 题答案与解析

STATEMENTS & ANALYSIS • 信息匹配题和解析

## 信息匹配题和解析·36-45 题

本页 36-45 题的段落匹配答案与逐句解析由懒笔记基于2016年12月·第1套 英语四级长篇阅读（信息匹配）原卷逐题核对整理。与试卷排版同一卷面：先是 Directions 与 11 段字母标号长文（逐段附中文翻译）；之后 10 句陈述逐句排列，每句英文陈述后紧接本句解析——陈述句中译、信息所在段落、锚点强弱、定位句中英对照、陈述句与原文的同义改写对照与易混相邻段辨析。

真题卷第1套(2016-12)·四级

Part III Section B

**Directions:** In this section, you are going to read a passage with ten statements attached to it. Each statement contains information given in one of the paragraphs. Identify the paragraph from which the information is derived. You may choose a paragraph more than once. Each paragraph is marked with a letter. Answer the questions by marking the corresponding letter on **Answer Sheet 2**.

### Can Burglars Jam Your Wireless Security System?

- A) Any product that promises to protect your home deserves careful examination. So it isn't surprising that you'll find plenty of strong opinions about the potential vulnerabilities of popular home-security systems.

任何承诺保护您家庭安全的产品都值得仔细审查。因此，您会发现关于流行家庭安全系统潜在漏洞的大量强烈意见也就不足为奇了。

- B) The most likely type of burglary(入室盗窃) by far is the unsophisticated crime of opportunity, usually involving a broken window or some forced entry. According to the FBI, crimes like these accounted for roughly two-thirds of all household burglaries in the US in 2013. The wide majority of the rest were illegal, unforced entries that resulted from something like a window being left open. The odds of a criminal using technical means to bypass a security system are so small that the FBI doesn't even track those statistics.

到目前为止，最可能发生的入室盗窃类型是不复杂的机会性犯罪，通常涉及破窗或某种强行进入。根据FBI的数据，2013年美国所有家庭入室盗窃案中，此类犯罪约占三分之二。其余大部分是非法的、非强制性进入，源于诸如窗户未关之类的情况。犯罪分子使用技术手段绕过安全系统的可能性非常小，以至于FBI甚至不追踪这些统计数据。

- C) One of the main theoretical home-security concerns is whether or not a given system is vulnerable to being blocked from working altogether. With wired setups, the fear is that a burglar(入室盗贼) might be able to shut your system down simply by cutting the right cable. With a wireless setup, you stick battery-powered sensors up around your home that keep an eye on windows, doors, motion, and

more. If they detect something wrong while the system is armed, they'll transmit a wireless alert signal to a base station that will then raise the alarm. That approach will eliminate most cord-cutting concerns—but what about their wireless equivalent, jamming? With the right device tuned to the right frequency, what's to stop a thief from jamming your setup and blocking that alert signal from ever reaching the base station?

家庭安全的主要理论担忧之一是特定系统是否容易被完全阻断。对于有线装置，人们担心入室盗贼可能只需切断正确的电缆就能让您的系统瘫痪。而无线装置则是在家中各处安装电池供电的传感器，监控窗户、门、动作等。如果系统处于布防状态时检测到异常，它们会向基站传输无线警报信号，然后基站会发出警报。这种方法将消除大部分剪线担忧——但它们的无线等价物，即干扰呢？有了调谐到正确频率的合适设备，什么能阻止小偷干扰您的装置并阻止警报信号到达基站呢？

- D) Jamming concerns are nothing new, and they're not unique to security systems. Any device that's built to receive a wireless signal at a specific frequency can be overwhelmed by a stronger signal coming in on the same frequency. For comparison, let's say you wanted to "jam" a conversation between two people—all you'd need to do is yell in the listener's ear.

干扰问题并不新鲜，也不是安全系统独有的。任何为接收特定频率无线信号而设计的设备都可能被同一频率上更强的信号压制。作为对比，假设您想“干扰”两个人之间的对话——您所需要做的就是听者耳边大喊。

- E) Security devices are required to list the frequencies they broadcast on—that means that a potential thief can find what they need to know with minimal Googling. They will, however, need to know what system they're looking for. If you have a sign in your yard declaring what setup you use, that'd point them in the right direction, though at that point, we're talking about a highly targeted, semi-sophisticated attack, and not the sort of forced-entry attack that makes up the majority of burglaries. It's easier to find and acquire jamming equipment for some frequencies than it is for others.

安全设备被要求列出它们广播的频率——这意味着潜在的小偷只需稍微搜索一下就能找到所需信息。然而，他们需要知道自己要找的是什么系统。如果您的院子里有标牌声明您使用的装置，那会为他们指明正确方向，尽管到那时，我们谈论的是高度针对性的、半复杂的攻击，而不是构成大多数入室盗窃的那种强行进入攻击。某些频率的干扰设备比其他频率更容易找到和获取。

- F) Wireless security providers will often take steps to help combat the threat of jamming attacks. SimpliSafe, winner of our Editors' Choice distinction, utilizes a special system that's capable of separating incidental RF interference from targeted jamming attacks. When the system thinks it's being jammed, it'll notify you via push alert(推送警报). From there, it's up to you to sound the alarm manually.

无线安全提供商通常会采取措施帮助对抗干扰攻击的威胁。SimpliSafe是我们编辑之选奖的获得者，它采用了一种特殊系统，能够将偶然的射频干扰与针对性干扰攻击区分开来。当系统认为自己正在被干扰时，它会通过推送警报通知您。接下来，由您手动发出警报。

- G) SimpliSafe was singled out in one recent article on jamming, complete with a video showing the entire system being effectively bypassed with hand-held jamming equipment. After taking appropriate measures to contain the RF interference to our test lab, we tested the attack out for ourselves, and were able to verify that it's possible with the right equipment. However, we also verified that SimpliSafe's anti-jamming system works. It caught us in the act, sent an alert to my smart phone,

and also listed our RF interference on the system's event log. The team behind the article and video in question makes no mention of the system, or whether or not it detected them.

SimpliSafe在最近一篇关于干扰的文章中被单独提及，附带的视频显示整个系统被手持干扰设备有效绕过。在采取适当措施将射频干扰控制在我们的测试实验室内后，我们自己测试了这种攻击，并能够验证使用正确设备确实可行。然而，我们也验证了SimpliSafe的反干扰系统有效。它当场抓住了我们，向我的智能手机发送了警报，还在系统的事件日志中列出了我们的射频干扰。该文章和视频背后的团队没有提及该系统，也没有提及它是否检测到了他们。

- H) We like the unique nature of that software. It means that a thief likely wouldn't be able to Google how the system works, then figure out a way around it. Even if they could, SimpliSafe claims that its system is always evolving, and that it varies slightly from system to system, which means there wouldn't be a universal magic formula for cracking it. Other systems also seem confident on the subject of jamming. The team at Frontpoint addresses the issue in a blog on its site, citing their own jam protection software and claiming that there aren't any documented cases of a successful jam attack since the company began offering wireless security sensors in the 1980s.

我们喜欢该软件的独特性。这意味着小偷很可能无法通过搜索了解系统的工作原理，然后找出绕过它的方法。即使他们能做到，SimpliSafe声称其系统一直在进化，而且各系统之间略有不同，这意味着不存在破解它的通用魔法公式。其他系统在干扰问题上似乎也很有信心。Frontpoint的团队在其网站的博客中讨论了这个问题，提到了他们自己的防干扰软件，并声称自公司在20世纪80年代开始提供无线安全传感器以来，没有任何成功干扰攻击的记录案例。

- I) Jamming attacks are absolutely possible. As said before, with the right equipment and the right know-how, it's possible to jam any wireless transmission. But how probable is it that someone will successfully jam their way into your home and steal your stuff?

干扰攻击绝对是可能的。如前所述，有了正确的设备和正确的专业知识，干扰任何无线传输都是可能的。但是，有人成功干扰进入您家并偷走您的东西的可能性有多大呢？

- J) Let's imagine that you live in a small home with a wireless security setup that offers a functional anti-jamming system. First, a thief is going to need to target your home, specifically. Then, he's going to need to know the technical details of your system and acquire the specific equipment necessary for jamming your specific setup. Presumably, you keep your doors locked at night and while you're away, so the thief will still need to break in. That means defeating the lock somehow, or breaking a window. He'll need to be jamming you at this point, as a broken window or opened door would normally release the alarm. So, too, would the motion detectors in your home, so the thief will need to continue jamming once he's inside and searching for things to steal. However, he'll need to do so without tripping the anti-jamming system, the details of which he almost certainly does not have access to.

让我们想象一下，您住在一个配备了具有功能性反干扰系统的无线安全装置的小房子里。首先，小偷需要专门针对您的家。然后，他需要了解您系统的技术细节，并获取干扰您特定装置所需的特定设备。据推测，您在夜间和外出时会锁门，因此小偷仍然需要破门而入。这意味着要以某种方式破坏锁，或者打破窗户。此时他需要对您进行干扰，因为破窗或开门通常会触发警报。您家中的运动探测器也会如此，因此小偷进入室内搜寻要偷的东西时需要继续干扰。然而，他需要在不触发反干扰系统的情况下这样做，而他几乎肯定无法获取该系统的详细信息。

K) At the end of the day, these kinds of systems are primarily designed to protect against the sort of opportunistic smash-and-grab attack that makes up the majority of burglaries. They're also only a single layer in what should ideally be a many-sided approach to securing your home, one that includes commonsense things like sound locks and proper exterior lighting at night. No system is impenetrable, and none can promise to eliminate the worst case completely. Every one of them has vulnerabilities that a knowledgeable thief could theoretically exploit. A good system is one that keeps that worst-case setting as improbable as possible while also offering strong protection in the event of a less extraordinary attack.

归根结底，这类系统主要设计用于防范构成大多数入室盗窃的那种机会性砸抢攻击。它们也只是理想情况下保护您家庭的多方面方法中的单一层面，该方法包括诸如坚固的锁和夜间适当的外部照明等常识性措施。没有系统是无懈可击的，也没有系统能承诺完全消除最坏情况。每个系统都有知识丰富的小偷理论上可以利用的漏洞。一个好的系统是既能使最坏情况尽可能不可能发生，又能在发生不太极端的攻击时提供强有力保护的系统。

## 陈述句与逐句解析

36. It is possible for burglars to make jamming attacks with the necessary equipment and skill.

窃贼有可能利用必要的设备和技术实施干扰攻击。

【答案】 I 段（弱锚点）

【锚点】 必要装备+技能才能干扰

【定位】 Jamming attacks are absolutely possible. As said before, with the right equipment and the right know-how, it's possible to jam any wireless transmission.

干扰攻击是完全可能的。如前所说，只要有合适的设备和相应的专业知识，任何无线传输都可以被干扰。

【改写】 It is possible for burglars to make jamming attacks ↔ Jamming attacks are absolutely possible possible 原样复现

with the necessary equipment and skill ↔ with the right equipment and the right know-how necessary↔right、skill↔know-how 双重同义替换

【辨邻】 E E 段聚焦 Security devices are required to list the frequencies they broadcast on, 处理的是「信息获取」，并未给出「干扰攻击是否可能」的总判断。

a potential thief can find what they need to know with minimal Googling

D Any device that's built to receive a wireless signal at a specific frequency can be overwhelmed by a stronger signal coming in on the same frequency 是机制描述，没有像 I 段那样给出「absolutely possible」的总结性判断。

Jamming concerns are nothing new, and they're not unique to security systems

37. Interfering with a wireless security system is similar to interfering with a conversation.

干扰无线安全系统类似于干扰谈话。

【答案】 D 段（强锚点）

【锚点】 类比对话干扰

【定位】 For comparison, let's say you wanted to "jam" a conversation between two people—all you'd need to do is yell in the listener's ear.

为了对照，假设你想「干扰」两个人之间的对话——你要做的就是冲着听者的耳朵大喊。

【改写】 Interfering with a wireless security system ↔

**Any device that's built to receive a wireless signal at a specific frequency can be overwhelmed by a stronger signal**

interfere↔jam 同义、wireless security system↔接收无线信号的设备

is similar to interfering with a conversation ↔

**let's say you wanted to "jam" a conversation between two people—all you'd need to do is yell in the listener's ear**

similar to 对应 For comparison/let's say

【辨邻】 C what's to stop a thief from jamming your setup and blocking that alert signal from ever reaching the base station 只是抛出问题，没有 similar to / for comparison / like 这类类比信号。

but what about their wireless equivalent, jamming

38. A burglar has to continuously jam the wireless security device to avoid triggering the alarm, both inside and outside the house.

窃贼必须持续干扰无线安全设备以避免触发警报,无论在室内还是室外。

【答案】 J 段（强锚点）

【锚点】 屋内屋外持续干扰

【定位】 He'll need to be jamming you at this point, as a broken window or opened door would normally release the alarm. So, too, would the motion detectors in your home, so the thief will need to continue jamming once he's inside and searching for things to steal.

此时他必须正在干扰你的系统，因为破窗或开门通常会触发警报。屋里的动作探测器也会触发警报，所以小偷进屋找东西时也得继续干扰下去。

【改写】 continuously jam the wireless security device ↔

**continue jamming once he's inside and searching for things to steal**

continuously↔continue 同根同义

to avoid triggering the alarm ↔

**a broken window or opened door would normally release the alarm**

avoid triggering↔为了不让 release

both inside and outside the house ↔ **He'll need to be jamming you at this point**

上下文构成「屋外（破门时）+屋内（搜寻时）」二元结构

【辨邻】 C what's to stop a thief from jamming your setup 只是发问，未涉及陈述句要的「continuously」与「both inside and outside」两个时空维度。

blocking that alert signal from ever reaching the base station

I it's possible to jam any wireless transmission 是抽象结论，未推演任何「破门/搜屋」的动作细节。

But how probable is it that someone will successfully jam their way into your home and steal your stuff

39. SimpliSafe provides devices that are able to distinguish incidental radio interference from targeted jamming attacks.

SimpliSafe提供能够区分偶然无线电干扰和针对性干扰攻击的设备。

【答案】 F 段（强锚点）

【锚点】 SimpliSafe 区分偶发与针对性干扰

【定位】 SimpliSafe, winner of our Editors' Choice distinction, utilizes a special system that's capable of separating incidental RF interference from targeted jamming attacks.

SimpliSafe（本刊编辑推荐奖得主）采用了一套特殊系统，能够把偶发的射频干扰和针对性的干扰攻击区分开来。

【改写】 SimpliSafe provides devices ↔ **SimpliSafe...utilizes a special system**  
provides devices↔utilizes a special system  
distinguish incidental radio interference from targeted jamming attacks ↔  
**separating incidental RF interference from targeted jamming attacks**  
distinguish↔separating 同义；RF↔radio 缩写还原

【辨邻】 G we also verified that SimpliSafe's anti-jamming system works 是「验证有效」，sent an alert to my smart phone 是发警报，未涉及「区分两类干扰」。

It caught us in the act, sent an alert to my smart phone, and also listed our RF interference on the system's event log

H SimpliSafe claims that its system is always evolving 是难破解论据，与「区分偶发与针对性干扰」无关。

there wouldn't be a universal magic formula for cracking it

40. Only a very small proportion of burglaries are committed by technical means.

只有极小比例的入室盗窃是通过技术手段实施的。

【答案】 B 段（强锚点）

【锚点】 技术手段作案的比例极低

【定位】 The odds of a criminal using technical means to bypass a security system are so small that the FBI doesn't even track those statistics.

罪犯用技术手段绕过安防系统的概率太小，以至于 FBI 都不去统计这类数据。

【改写】 Only a very small proportion of burglaries ↔

**The odds of a criminal using technical means to bypass a security system are so small**  
small proportion ↔ odds...so small

committed by technical means ↔ **using technical means to bypass a security system**  
technical means 原样复现

【辨邻】 I Jamming attacks are absolutely possible 给的是可能性判断，没有像 B 段那样给出「在所有盗窃中占比极小」的统计性结论。

But how probable is it that someone will successfully jam their way into your home and steal your stuff

41. It is difficult to crack SimpliSafe as its system keeps changing.

SimpliSafe 难以破解, 因为其系统不断变化。

【答案】 H 段 (强锚点)

【锚点】 SimpliSafe 系统在变所以难破解

【定位】 Even if they could, SimpliSafe claims that its system is always evolving, and that it varies slightly from system to system, which means there wouldn't be a universal magic formula for cracking it.

即便他们能查到, SimpliSafe 声称其系统一直在演进, 而且各台设备之间略有差异, 这意味着没有一个万能的破解公式。

【改写】 difficult to crack SimpliSafe ↔ **there wouldn't be a universal magic formula for cracking it**  
难破解 ↔ 没有万能破解公式

its system keeps changing ↔ **its system is always evolving**  
keeps changing ↔ always evolving

【辨邻】 F separating incidental RF interference from targeted jamming attacks 是讲「区分干扰类型」, 未涉及陈述句的「难破解、系统在变」。

When the system thinks it's being jammed, it'll notify you via push alert

G we also verified that SimpliSafe's anti-jamming system works 是一次性验证, 未涉及陈述句的核心「keeps changing」。

It caught us in the act, sent an alert to my smart phone

42. Wireless devices will transmit signals so as to activate the alarm once something wrong is detected.

无线设备一旦检测到异常就会发送信号以激活警报。

【答案】 C 段 (弱锚点)

【锚点】 无线设备探测异常→发信号→报警

【定位】 If they detect something wrong while the system is armed, they'll transmit a wireless alert signal to a base station that will then raise the alarm.

如果它们（无线传感器）在系统启动时检测到异常，就会向基站发送一个无线警报信号，基站随后触发警报。

【改写】 once something wrong is detected ↔ **If they detect something wrong while the system is armed**  
once↔if、wrong↔wrong 原样

Wireless devices will transmit signals ↔ **they'll transmit a wireless alert signal to a base station**  
transmit signals↔transmit a wireless alert signal

so as to activate the alarm ↔ **that will then raise the alarm**  
activate↔raise 同义动词

【辨邻】 **F** When the system thinks it's being jammed, it'll notify you via push alert 是「被干扰时通知」这一特定场景，并非陈述句要的「探测到任何异常都报警」的通用机制。

it'll notify you via push alert

**G** It caught us in the act, sent an alert to my smart phone 是单次实验复现，没有像C段那样完整给出「探测→传信号→报警」的设备工作机制。

After taking appropriate measures to contain the RF interference to our test lab, we tested the attack out for ourselves

43. Different measures should be taken to protect one's home from burglary in addition to the wireless security system.

除了无线安全系统之外,还应采取不同措施来保护住宅免遭入室盗窃。

【答案】 **K** 段（强锚点）

【锚点】 除无线安防外还应采取别的防盗措施

【定位】 They're also only a single layer in what should ideally be a many-sided approach to securing your home, one that includes commonsense things like sound locks and proper exterior lighting at night.

它们（无线安防系统）也只是一个理想的多层防护方法中的一层，理想做法还应包括好锁和夜间合理户外照明这类常识性举措。

【改写】 Different measures should be taken to protect one's home from burglary ↔

**a many-sided approach to securing your home, one that includes commonsense things like sound locks and proper exterior lighting at night**

different measures↔many-sided approach + 列举具体措施

in addition to the wireless security system ↔

**They're also only a single layer in what should ideally be a many-sided approach to securing your home**

in addition to↔only a single layer in a many-sided approach

【辨邻】 **B** crimes like these accounted for roughly two-thirds of all household burglaries 是统计描述，未给出「还应采取何种额外措施」的建议性论断。

The wide majority of the rest were illegal, unforced entries that resulted from something like a window being left open

44. SimpliSafe's device can send a warning to the house owner's cellphone.

SimpliSafe的设备可以向房主的手机发送警告。

【答案】 **G** 段（强锚点）

【锚点】 向房主手机发警告

【定位】 It caught us in the act, sent an alert to my smart phone, and also listed our RF interference on the system's event log.

它当场抓住了我们，发警报到我的智能手机，并把我们的射频干扰记录进系统事件日志。

【改写】 SimpliSafe's device can send a warning ↔ **sent an alert to my smart phone**  
warning↔alert 同义

to the house owner's cellphone ↔ **to my smart phone**

house owner's cellphone↔my smart phone

【辨邻】 **F** it'll notify you via push alert 只笼统提到推送警报，没有把「手机」作为具体的收件设备写出，与陈述句的 cellphone 缺少对位词。

When the system thinks it's being jammed, it'll notify you via push alert

45. Burglars can easily get a security device's frequency by Internet search.

窃贼可以通过互联网搜索轻易获取安全设备的频率。

【答案】 **E** 段（强锚点）

【锚点】 网上轻易查到设备频率

【定位】 Security devices are required to list the frequencies they broadcast on—that means that a potential thief can find what they need to know with minimal Googling.

安防设备被强制要求公开它们使用的广播频率——这意味着潜在的小偷只要稍微 Google 一下就能找到所需信息。

【改写】 Burglars can easily get a security device's frequency ↔

a potential thief can find what they need to know

burglars↔potential thief、easily↔minimal、get↔find

by Internet search ↔ with minimal Googling

Internet search↔Googling 上下位等值

a security device's frequency ↔ the frequencies they broadcast on

frequency↔frequencies 原样复现

【辨邻】 H a thief likely wouldn't be able to Google how the system works 中 Google 的对象是「系统如何运作」，不是陈述句所问的「频率」。

a thief likely wouldn't be able to Google how the system works, then figure out a way around it

PARAGRAPH MAP • 段落主旨图

## 11 个段落各讲了什么

逐段一句主旨 + 该段最具区分度的「信息指纹」，是逐句回扫定位的工作台。

A 开篇引入：任何号称能保护家庭的产品都应该被仔细审视，因此关于热门家庭安防系统潜在弱点的强烈观点很多。本段是全文的引子，不涉及任何具体技术或案例。

信息指纹 无强指纹，靠语义

B 用 FBI 数据说明：绝大多数入室盗窃是砸窗或强行闯入这类机会型犯罪，靠技术手段绕过安防系统的比例小到 FBI 都不统计。

信息指纹 FBI 与 2013 三分之二数据

C 对比有线与无线安防：有线怕剪线，无线靠电池传感器把警报信号无线发到基站，一旦发现异常就报警；由此引出无线场景下的隐患——jamming（信号干扰）。

信息指纹 无线传感器→基站发警报信号

D 解释 jamming 原理：任何接收特定频率信号的设备，都会被同一频率的更强信号压过；并用「在听者耳边大喊以干扰两人对话」作类比。

信息指纹 干扰两人对话的类比

E 安防设备必须公开自己的发射频率，所以小偷只要稍微 Google 一下就能查到；但要先知道是哪套系统，例如院子里的标牌会暴露。

信息指纹 频率必须公开+Google 可查

F 介绍 SimpliSafe 的反干扰机制：能把偶发的射频干扰和针对性干扰区分开，被干扰时通过推送警报通知用户，由用户决定是否手动报警。

信息指纹 SimpliSafe 区分偶发干扰与针对性干扰

G 作者复现实验：用手持设备确实可以干扰 SimpliSafe，但其反干扰系统当场识破——给作者手机发了警报、并把干扰记录进事件日志；原文章/视频却没提这件事。

信息指纹 向作者手机发警报+事件日志

H 强调 SimpliSafe 的软件独特性：小偷难以靠 Google 摸清；系统不断进化、各家略有差异，没有「万能破解公式」；并提到 Frontpoint 也号称自家有反干扰软件、自 1980s 起无成功干扰案例。

信息指纹 系统持续进化+无万能破解公式

I 承认干扰攻击在技术上完全可能：只要有合适的设备和 know-how，任何无线传输都能被干扰；但随即抛出「实际成功入室的概率有多大」这一反问。

信息指纹 有设备+know-how 即可干扰

J 推演一个具体场景，列出小偷为了真正得手必须连续完成的全部步骤：锁定目标家、了解你这套具体系统并备齐器材、破门破窗、在屋外屋内全程持续干扰、还得不触发反干扰机制。

信息指纹 屋外屋内全程持续干扰

K 收尾结论：无线安防主要应对机会型砸抢，本就该和好锁、户外照明等常识性手段配合使用；没有系统是无懈可击的，好系统是把最坏情况发生的概率压到最低。

信息指纹 多重防护+常识性手段

SENTENCE INSIGHTS • 句子精讲

## 10 句真题句逐层精讲

下列真题句各有独立的句子解析页——中文翻译、结构树逐层拆解、成分与时态、考点讲解与真题高频词。点击句子进入完整解析。

According to the FBI, crimes like these accounted for roughly two-thirds of all household burglaries in the US in 2013.

B段，第2句

简单句 + 介词短语作状语和定语的组合在四六级和考研阅读中较为常见,尤其是引用数据来源的 "According to" 结构和分数表达 "two-thirds of" 是新闻和学术语体的典型句式,有一定代表性和迁移价值。

The odds of a criminal using technical means to bypass a security system are so small that the FBI doesn't even track those statistics.

B段，第4句

"so ... that" 引导的结果状语从句是四六级和考研阅读中的高频句式，主语带介词短语和非谓语后置定语的结构也十分常见；本句的主系表 + 结果状语从句框架具有较强的代表性和可迁移性，掌握后能够应对大量同类句子，是较为典型的考试常见结构。

One of the main theoretical home-security concerns is whether or not a given system is vulnerable to being blocked from working altogether.

C段，第1句

主句加表语从句的结构在四六级和考研阅读中较为常见，尤其是用 "whether" 引导表语从句表达不确定性或选择性问题的。动名词被动结构 "being blocked" 也是常考点。掌握此句型后可迁移到类似的 "问题是..."、"关注点是..." 等表达，具有较好的典型性。

For comparison, let's say you wanted to "jam" a conversation between two people —all you'd need to do is yell in the listener's ear.

D段，第3句

本句成分丰富，涵盖主语、谓语、宾语、表语、状语、定语从句等多种成分，且有多处易错点：宾语从句省略引导词、定语从句修饰主语、表语是动词原形（省略 "to"）、不定式作宾语。这些特征使本句成为较好的成分划分练习材料，能帮助学生识别省略和非典型结构。

If you have a sign in your yard declaring what setup you use, that'd point them in the right direction, though at that point, we're talking about a highly targeted, semi-sophisticated attack, and not the sort of forced-entry attack that makes up the majority of burglaries.

E段, 第3句

覆盖主谓宾、状语、宾语从句、定语从句、条件和让步状语从句、并列结构等多种成分,且包含指示代词 that 作主语回指、现在分词短语 declaring 作定语、介词短语作状语等易错点,成分丰富且具有典型训练价值。

SimpliSafe was singled out in one recent article on jamming, complete with a video showing the entire system being effectively bypassed with hand-held jamming equipment.

G段, 第1句

被动语态 + 介词短语状语的组合在四六级和考研阅读中高频出现,"be + 过去分词 + in/by/with" 是典型的学术和新闻文体句式。逗号后补充说明的用法(类似独立主格或同位语性质的状语)也是常见的长难句特征。本句结构具有较强的代表性,掌握后可迁移到大量同类句子的理解中。

It means that a thief likely wouldn't be able to Google how the system works, then figure out a way around it.

H段, 第2句

主句 + 宾语从句 + 嵌套宾语从句的结构在四六级和考研阅读中较为常见,尤其是 means that 这种引出观点的句式,以及 how 引导的间接疑问句作为宾语从句的用法,都是典型的考试句式,掌握后可迁移到大量类似句子。

Even if they could, SimpliSafe claims that its system is always evolving, and that it varies slightly from system to system, which means there wouldn't be a universal magic formula for cracking it.

H段, 第3句

"主句 + 并列宾语从句 + 非限定性定语从句"是四六级和考研阅读中的高频句式,让步状语从句前置、定语从句补充说明主句整体内容,都是常考结构。宾语从句并列且省略第二个 that、定语从句嵌套宾语从句,这些都是真题中反复出现的组合模式。掌握本句结构后,可直接迁移到大量类似长句的分析中,典型性很高。

At the end of the day, these kinds of systems are primarily designed to protect against the sort of opportunistic smash-and-grab attack that makes up the majority of burglaries.

K段，第1句

被动语态加不定式作目的状语的结构在四六级和考研阅读中非常常见,限制性定语从句修饰宾语也是典型句式,句子整体结构具有较强的代表性,掌握后可在大量真题句子中复用识别方法。

A good system is one that keeps that worst-case setting as improbable as possible while also offering strong protection in the event of a less extraordinary attack.

K段，第5句

本句成分较为丰富：主句包含主系表结构，表语由定语从句修饰；定语从句内部包含主语、谓语、宾语、宾语补足语以及方式状语（并列动作结构），覆盖了多种常见成分；特别是宾语补足语 "as improbable as possible" 以及 "while also offering" 引导的伴随状语，是学生容易混淆或忽略的点，具有较好的训练价值；但缺少从句作主语、宾语等更复杂的成分嵌套，因此评分中上。

HIGH-FREQUENCY • 真题高频词

## 本篇出现的 103 个英语四级真题高频词

下列单词既在本篇真题中出现，又是 **英语四级** 历年真题的高频词（在该考试真题中出现的句子数均不少于 8）。每个词标注本篇 出现次数与该考试真题句频，点击可查看该词的释义、音标、词形与真题例句。

**system**

A2

n. 系统

本篇28次 · 真题 162 句

**jam**

A2

n. 果酱

本篇13次 · 真题 50 句

**wireless**

B1

adj. 无线的

本篇13次 · 真题 15 句

**security**

B1

n. 安全

本篇11次 · 真题 62 句

**attack**

A2

v. 攻击

本篇11次 · 真题 55 句

**jamming**

B2

n. (信号) 干扰, 阻塞

本篇10次 · 真题 9 句

**device** B1

n. 设备

本篇8次·真题 60 句

**thief** A2

n. 小偷

本篇7次·真题 10 句

**equipment** B1

n. 设备

本篇6次·真题 32 句

**frequency** B2

n. 频率

本篇6次·真题 9 句

**signal** B1

n. 信号

本篇5次·真题 20 句

**alarm** A2

n. 警报器

本篇5次·真题 11 句

**would** A1

aux. (will 的过去式) 将要, 会

本篇4次·真题 466 句

**alert** B2

adj. 警觉的

本篇4次·真题 17 句

**concern** B1

v. 涉及

本篇3次·真题 79 句

**specific** B2

adj. 具体的

本篇3次·真题 42 句

**majority** B2

n. 大多数, 大部分

本篇3次·真题 40 句

**detect** B2

v. 发现, 察觉 (难以察觉的事物)

本篇3次·真题 14 句

**likely** A2

adj. 很可能的

本篇2次·真题 224 句

**base** A2

n. 基础

本篇2次·真题 95 句

**case** A2

n. 情况

本篇2次·真题 89 句

**measure** B1

v. 测量

本篇2次·真题 68 句

**event** A2

n. 事件

本篇2次 · 真题 66 句

**potential** B2

adj. 潜在的

本篇2次 · 真题 63 句

**claim** B1

v. 声称

本篇2次 · 真题 56 句

**wrong** A2

adj. 错误的

本篇2次 · 真题 54 句

**approach** B1

v. 靠近, 接近 (在空间或时间上)

本篇2次 · 真题 50 句

**detail** B1

n. 细节

本篇2次 · 真题 45 句

**software** B1

n. 软件 (计算机程序)

本篇2次 · 真题 35 句

**unique** B2

adj. 独特的

本篇2次 · 真题 35 句

**protection** B1

n. 保护

本篇2次 · 真题 32 句

**means** A2

n. 方法

本篇2次 · 真题 30 句

**acquire** B2

v. 获得

本篇2次 · 真题 24 句

**block** A2

n. 街区

本篇2次 · 真题 24 句

**crime** A2

n. 犯罪行为

本篇2次 · 真题 22 句

**eliminate** B2

v. 消除

本篇2次 · 真题 16 句

**interfere** B2

v. 干涉, 介入 (他人事务)

本篇2次 · 真题 9 句

**crack** B1

v. 破裂

本篇2次 · 真题 8 句

**less** A1

det. 较少的

本篇1次·真题 224 句

**design** B1

n. 设计

本篇1次·真题 132 句

**product** A2

n. 产品

本篇1次·真题 128 句

**type** A2

n. 类型

本篇1次·真题 97 句

**simply** B1

adv. 仅仅，只不过

本篇1次·真题 90 句

**opportunity** B1

n. 机会

本篇1次·真题 89 句

**according** B1

prep. 根据

本篇1次·真题 88 句

**access** B1

n. 进入

本篇1次·真题 83 句

**issue** B1

n. 问题

本篇1次·真题 83 句

**sign** A1

n. 标志

本篇1次·真题 78 句

**involve** B1

v. 包含

本篇1次·真题 65 句

**account** A2

n. 账户

本篇1次·真题 61 句

**internet** A2

n. 互联网

本篇1次·真题 55 句

**contain** B1

v. 包含，含有

本篇1次·真题 50 句

**easily** A2

adv. 容易地

本篇1次·真题 47 句

**figure** A2

n. 数字

本篇1次·真题 44 句

**site** A2

n. 地点

本篇1次·真题 37 句

**completely** B1

adv. 完全地

本篇1次·真题 34 句

**household** B1

n. 家庭

本篇1次·真题 33 句

**track** A2

n. 小路

本篇1次·真题 33 句

**release** B1

v. 释放

本篇1次·真题 31 句

**vary** B1

v. 不同

本篇1次·真题 31 句

**opinion** A2

n. 观点

本篇1次·真题 29 句

**highly** B1

adv. 非常

本篇1次·真题 28 句

**threat** B1

n. 威胁

本篇1次·真题 28 句

**formula** B2

n. 公式

本篇1次·真题 27 句

**addition** A2

n. 增加

本篇1次·真题 25 句

**warning** A2

n. 警告

本篇1次·真题 25 句

**target** B1

n. 目标,靶子

本篇1次·真题 24 句

**vulnerable** C1

adj. 易受伤害的

本篇1次·真题 23 句

**stuff** A2

n. 东西

本篇1次·真题 22 句

**slightly** B1

adv. 稍微, 略微, 轻微地

本篇1次·真题 21 句

**capable** B1

adj. 有能力的

本篇1次·真题 20 句

**criminal** B1

n. 罪犯

本篇1次·真题 20 句

**entire** B1

adj. 整个的

本篇1次·真题 19 句

**roughly** B1

adv. 大约, 大概

本篇1次·真题 19 句

**combat** B2

n. 战斗

本篇1次·真题 18 句

**setting** B1

n. 环境

本篇1次·真题 18 句

**commit** B2

v. 承诺、保证做某事

本篇1次·真题 17 句

**effectively** B2

adv. 有效地

本篇1次·真题 17 句

**evolve** B2

v. 逐渐发展;进化

本篇1次·真题 17 句

**listener** B1

n. 听者

本篇1次·真题 17 句

**certainly** A2

adv. 当然

本篇1次·真题 15 句

**distinguish** B2

v. 区分

本篇1次·真题 15 句

**secure** B2

adj. 安全的

本篇1次·真题 15 句

**deserve** B1

v. 应得

本篇1次·真题 14 句

**odd** B1

adj. 奇怪的

本篇1次·真题 14 句

**specifically** B2

adv. 明确地

本篇1次·真题 14 句

**statistic** B2

n. 统计数字

本篇1次·真题14句

**extraordinary** B2

adj. 非凡的

本篇1次·真题13句

**primarily** B2

adv. 主要地

本篇1次·真题13句

**absolutely** B1

adv. 完全地

本篇1次·真题12句

**appropriate** B2

adj. 合适的

本篇1次·真题12句

**cite** B2

v. 引用, 引证

本篇1次·真题12句

**provider** B2

n. 供应者

本篇1次·真题12句

**layer** B1

n. 层

本篇1次·真题11句

**blog** B1

n. 博客, 网络日志

本篇1次·真题10句

**normally** A2

adv. 通常

本篇1次·真题10句

**proportion** B2

n. 部分

本篇1次·真题10句

**successfully** B1

adv. 成功地

本篇1次·真题10句

**surprising** A2

adj. 令人惊讶的

本篇1次·真题10句

**universal** B2

adj. 普遍的

本篇1次·真题10句

**distinction** B2

n. 区别

本篇1次·真题9句

**trigger** B2

v. 引发

本篇1次·真题9句

**overwhelm**

B2

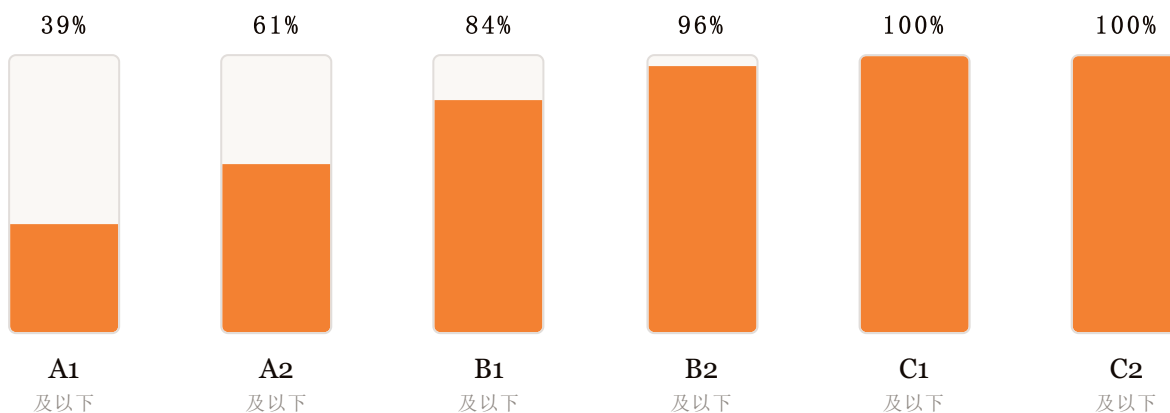
v. 使不知所措

本篇1次 · 真题 8 句

VOCABULARY · 词汇难度分布

## 全文 340 词按 CEFR 难度累积覆盖

全文去重后共 **340** 个单词，按欧框 CEFR 等级统计。每根柱表示「该等级及以下」的累积占比（CDF），最右一柱为 100%。B2 以上（C1/C2）为高阶词，本篇共 14 个 · 约 4%。



每柱为「按 CEFR 等级及以下」的累积覆盖率（CDF）· 数据为全文去重词 340 个 · 末柱为 100%

去重总词数

**340**

B2 以上难词

**4%**

B1 及以下覆盖

**84%**

英语四级 2016年12月·第1套 · 全卷构成

|                           |            |                        |
|---------------------------|------------|------------------------|
| Part I                    | 写作         | <a href="#">题目解析 →</a> |
| Part II                   | 听力         | <a href="#">题目解析 →</a> |
| Part III Section A        | 完形填空（选词填空） | <a href="#">题目解析 →</a> |
| <b>Part III Section B</b> | 长篇阅读（信息匹配） | <a href="#">本题</a>     |
| Part III Section C (1)    | 阅读理解（四选一）  | <a href="#">题目解析 →</a> |
| Part III Section C (2)    | 阅读理解（四选一）  | <a href="#">题目解析 →</a> |
| Part IV                   | 汉译英（段落翻译）  | <a href="#">题目解析 →</a> |