

2017年12月·第3套 英语六级长篇阅读（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2017年12月·第3套 英语六级长篇阅读（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 16 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3套(2017-12)·六级

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**.

Apple's Stance Highlights a More Confrontational Tech Industry

A) The battle between Apple and law enforcement officials over unlocking a terrorist's smartphone is the culmination of a slow turning of the tables between the technology industry and the United States government.

苹果公司与执法官员之间围绕解锁一名恐怖分子智能手机的斗争,是科技行业与美国政府之间力量对比缓慢转变的高潮。

B) After revelations by the former National Security Agency contractor Edward J. Snowden in 2013 that the government both coozied up to(讨好) certain tech companies and hacked into others to gain access to private data on an enormous scale, tech giants began to recognize the United States government as a hostile actor. But if the confrontation has crystallized in this latest battle, it may already be heading toward a predictable conclusion: In the long run, the tech companies are destined to emerge victorious.

2013年前国家安全局承包商Edward J. Snowden披露政府既讨好某些科技公司又侵入其他公司以大规模获取私人数据后,科技巨头开始将美国政府视为敌对势力。但如果这场对抗在最近的斗争中明朗化,它可能已经走向一个可预见的结论:从长远来看,科技公司注定会取得胜利。

C) It may not seem that way at the moment. On the one side, you have the United States government's mighty legal and security apparatus fighting for data of the most sympathetic sort: the secrets buried in a dead mass murderer's phone. The action stems from a federal court order issued on Tuesday

requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, California, in December.

目前看来可能并非如此。一方面,你看到美国政府强大的法律和安全机构正在为最具同情色彩的数据而战:埋藏在一名已故大规模杀人犯手机中的秘密。这一行动源于周二发布的联邦法院命令,要求苹果公司帮助联邦调查局解锁12月在加利福尼亚州San Bernardino杀害14人的两名袭击者之一使用的iPhone。

- D) In the other corner is the world's most valuable company, whose chief executive, Timothy Cook, has said he will appeal the court's order. Apple argues that it is fighting to preserve a principle that most of us who are addicted to our smartphones can defend: Weaken a single iPhone so that its contents can be viewed by the American government and you risk weakening all iPhones for any government intruder, anywhere.

另一方是世界上最有价值的公司,其首席执行官Timothy Cook表示他将对法院命令提出上诉。苹果公司辩称,它是在为维护一项我们这些智能手机成瘾者大多数人都能捍卫的原则而战:削弱单一iPhone使其内容可以被美国政府查看,就有削弱所有iPhone、使其面临任何地方任何政府入侵者威胁的风险。

- E) There will probably be months of legal confrontation, and it is not at all clear which side will prevail in court, nor in the battle for public opinion and legislative favor. Yet underlying all of this is a simple dynamic: Apple, Google, Facebook and other companies hold most of the cards in this confrontation. They have our data, and their businesses depend on the global public's collective belief that they will do everything they can to protect that data.

可能会有数月的法律对抗,而且完全不清楚哪一方会在法庭上胜出,也不清楚在争取公众舆论和立法支持的战斗中谁会获胜。然而所有这一切背后是一个简单的动态:苹果、Google、Facebook和其他公司在这场对抗中掌握着大部分牌。他们拥有我们的数据,而他们的业务依赖于全球公众的集体信念,即他们会竭尽所能保护这些数据。

- F) Any crack in that front could be fatal for tech companies that must operate worldwide. If Apple is forced to open up an iPhone for an American law enforcement investigation, what is to prevent it from doing so for a request from the Russians or the Iranians? If Apple is forced to write code that lets the FBI get into the iPhone 5c used by Syed Rizwan Farook, the male attacker in the San Bernardino attack, who would be responsible if some hacker got hold of that code and broke into its other devices?

这条战线上的任何裂缝都可能对必须在全球运营的科技公司造成致命打击。如果苹果公司被迫为美国执法调查打开一部iPhone,有什么能阻止它对俄罗斯或伊朗的请求这样做呢?如果苹果公司被迫编写代码让FBI进入San Bernardino袭击中男性袭击者Syed Rizwan Farook使用的iPhone 5c,如果某个黑客获得了那段代码并侵入其他设备,谁该负责?

- G) Apple's stance on these issues emerged post-Snowden, when the company started putting in place a series of technologies that, by default, make use of encryption(加密) to limit access to people's data. More than that, Apple—and, in different ways, other tech companies, including Google, Facebook, Twitter and Microsoft—have made their opposition to the government's claims a point of corporate pride.

苹果公司在这些问题上的立场出现在Snowden事件之后,当时该公司开始实施一系列技术,默认使用加密来限制对人们数据的访问。不仅如此,苹果——以及以不同方式的其他科技公司,包括Google、Facebook、Twitter和Microsoft——已经将他们对政府主张的反对作为企业自豪感的一部分。

- H) Apple's emerging global brand is privacy; it has staked its corporate reputation, not to mention the investment of considerable technical and financial resources, on limiting the sort of mass surveillance that was uncovered by Mr. Snowden. So now, for many cases involving governmental intrusions into data, once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world.

苹果公司新兴的全球品牌是隐私;它将企业声誉,更不用说大量技术和财务资源的投入,押在限制 Snowden先生揭露的那种大规模监控上。所以现在,在许多涉及政府侵入数据的案件中,曾经孤独的隐私倡导者发现自己正与世界上最强大的公司并肩作战。

- I) "A comparison point is in the 1990s battles over encryption," said Kurt Opsahl, general counsel of the Electronic Frontier Foundation, a privacy watchdog group. "Then you had a few companies involved, but not one of the largest companies in the world coming out with a lengthy and impassioned post, like we saw yesterday from Timothy Cook. Its profile has really been raised."

隐私监督组织Electronic Frontier Foundation的总法律顾问Kurt Opsahl说:"一个比较点是20世纪90年代关于加密的斗争。那时你有几家公司参与,但没有一家世界上最大的公司发表冗长而充满激情的帖子,就像我们昨天从Timothy Cook那里看到的那样。它的形象确实得到了提升。"

- J) Apple and other tech companies hold another ace: the technical means to keep making their devices more and more inaccessible. Note that Apple's public opposition to the government's request is itself a hindrance to mass government intrusion. And to get at the contents of a single iPhone, the government says it needs a court order and Apple's help to write new code; in earlier versions of the iPhone, ones that were created before Apple found religion on(热衷于) privacy, the FBI might have been able to break into the device by itself.

苹果公司和其他科技公司还握有另一张王牌:使其设备越来越难以访问的技术手段。请注意,苹果公司对政府请求的公开反对本身就是对政府大规模侵入的阻碍。为了获取单一iPhone的内容,政府表示它需要法院命令和苹果公司的帮助来编写新代码;在iPhone的早期版本中,那些在苹果公司热衷于隐私之前创建的版本,FBI可能能够自己破解设备。

- K) You can expect that noose(束缚) to continue to tighten. Experts said that whether or not Apple loses this specific case, measures that it could put into place in the future will almost certainly be able to further limit the government's reach.

你可以预期这种束缚会继续收紧。专家表示,无论苹果公司是否在这个具体案件中败诉,它未来可以采取的措施几乎肯定能够进一步限制政府的触及范围。

- L) That is not to say that the outcome of the San Bernardino case is insignificant. As Apple and several security experts have argued, an order compelling Apple to write software that gives the FBI access to the iPhone in question would establish an unsettling precedent. The order essentially asks Apple to hack its own devices, and once it is in place, the precedent could be used to justify law enforcement efforts to get around encryption technologies in other investigations far removed from national security threats.

这并不是说San Bernardino案件的结果无关紧要。正如苹果公司和几位安全专家所辩称的,强制苹果公司编写软件使FBI能够访问相关iPhone的命令将树立一个令人不安的先例。该命令本质上是要求苹果公司入侵自己的设备,一旦到位,这一先例可能被用来为执法部门在远离国家安全威胁的其他调查中绕过加密技术的努力辩护。

M) Once armed with a method for gaining access to iPhones, the government could ask to use it proactively(先发制人地), before a suspected terrorist attack—leaving Apple in a bind as to whether to comply or risk an attack and suffer a public-relations nightmare. "This is a brand new move in the war against encryption," Mr. Opsahl said. "We have had plenty of debates in Congress and the media over whether the government should have a backdoor, and this is an end run(迂回战术) around that—here they come with an order to create that backdoor."

一旦掌握了获取iPhone访问权限的方法,政府可以要求先发制人地使用它,在疑似恐怖袭击发生之前——这让苹果公司陷入两难,是遵守命令还是冒着遭受袭击和公关噩梦的风险。Opsahl先生说:"这是反加密战争中的全新举措。我们在国会和媒体上就政府是否应该有后门进行了大量辩论,而这是对此的迂回战术——他们带着创建该后门的命令来了。"

N) Yet it is worth noting that even if Apple ultimately loses this case, it has plenty of technical means to close a backdoor over time. "If they are anywhere near worth their salt as engineers, I bet they are rethinking their threat model as we speak," said Jonathan Zdziarski, a digital expert who studies the iPhone and its vulnerabilities.

然而值得注意的是,即使苹果公司最终在此案中败诉,它也有大量技术手段随着时间推移关闭后门。研究iPhone及其漏洞的数字专家Jonathan Zdziarski说:"如果他们作为工程师有任何价值,我打赌他们现在正在重新思考他们的威胁模型。"

O) One relatively simple fix, Mr. Zdziarski said, would be for Apple to modify future versions of the iPhone to require a user to enter a passcode before the phone will accept the sort of modified operating system that the FBI wants Apple to create. That way, Apple could not unilaterally introduce a code that weakens the iPhone—a user would have to consent to it.

Zdziarski先生说,一个相对简单的修复方法是,苹果公司修改iPhone的未来版本,要求用户在手机接受FBI希望苹果公司创建的那种修改过的操作系统之前输入密码。这样,苹果公司就不能单方面引入削弱iPhone的代码——用户必须同意它。

P) "Nothing is 100 percent hacker-proof," Mr. Zdziarski said, but he pointed out that the judge's order in this case required Apple to provide "reasonable security assistance" to unlock Mr. Farook's phone. If Apple alters the security model of future iPhones so that even its own engineers' "reasonable assistance" will not be able to crack a given device when compelled by the government, a precedent set in this case might lose its lasting force. In other words, even if the FBI wins this case, in the long run, it loses.

Zdziarski先生说:"没有什么是百分之百防黑客的",但他指出,本案中法官的命令要求苹果公司提供"合理的安全协助"来解锁Farook先生的手机。如果苹果公司改变未来iPhone的安全模型,使得即使是其自己工程师的"合理协助"在受到政府强制时也无法破解特定设备,那么本案树立的先例可能会失去其持久效力。换句话说,即使FBI赢得此案,从长远来看,它输了。

陈述句与逐句解析

36. It is a popular belief that tech companies are committed to protecting their customers' private data.

人们普遍认为科技公司致力于保护其客户的私人数据。

【答案】 E 段(弱锚点)

【锚点】 popular belief + 公司护数据

【定位】 They have our data, and their businesses depend on the global public's collective belief that they will do everything they can to protect that data.

它们手里握着我们的数据，而它们的生意建立在全球公众的一种集体信念之上——即相信它们会竭尽全力保护这些数据。

【改写】 a popular belief ↔ **the global public's collective belief**

popular = public 的同义改写

tech companies are committed to protecting their customers' private data ↔

they will do everything they can to protect that data

committed to = do everything they can to

【辨邻】 **H** 本段讲 once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world, 主语是隐私倡导者与苹果，谈的是品牌与同盟，没说 popular belief 这一层「公众集体信念」。

Apple's emerging global brand is privacy

G 本段 make use of encryption(加密) to limit access to people's data 描述的是苹果采取的技术动作，缺少陈述句中 popular belief 这一「公众信念」维度，因此只覆盖局部、错位命中。

by default, make use of encryption(加密) to limit access to people's data

37. The US government believes that its access to people's iPhones could be used to prevent terrorist attacks.

美国政府认为其获取人们iPhone的权限可以用来防止恐怖袭击。

【答案】 **M** 段 (强锚点)

【锚点】 政府以接触 iPhone 防恐袭

【定位】 Once armed with a method for gaining access to iPhones, the government could ask to use it proactively, before a suspected terrorist attack—leaving Apple in a bind as to whether to comply or risk an attack and suffer a public-relations nightmare.

一旦掌握了进入 iPhone 的手段，政府可能会要求先发制人地使用它，即在疑似恐怖袭击发生之前就用——这会让苹果陷入两难：是顺从，还是冒袭击发生与公关噩梦的风险。

【改写】 its access to people's iPhones ↔ **armed with a method for gaining access to iPhones**

名词化的 access 对应动词性 gain access

could be used to prevent terrorist attacks ↔

could ask to use it proactively(先发制人地), before a suspected terrorist attack

before 袭击 + proactively = prevent 袭击

【辨邻】 C 本段 the two attackers who killed 14 people in San Bernardino, California, in December 说的是袭击已经发生、政府才请求解锁，缺少「在袭击发生前就先用」这一前置时间，因此与 prevent terrorist attacks 错位。

unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, California, in December

F 本段 what is to prevent it from doing so for a request from the Russians or the Iranians? 谈的是连锁开口子的风险，缺少 prevent terrorist attacks 这一独特概念。

what is to prevent it from doing so for a request from the Russians or the Iranians?

38. A federal court asked Apple to help the FBI access data in a terrorist's iPhone.

一家联邦法院要求Apple帮助FBI获取一名恐怖分子iPhone中的数据。

【答案】 C 段（强锚点）

【锚点】 联邦法院 + 帮 FBI 进 iPhone

【定位】 The action stems from a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, California, in December.

此次行动源于周二一道联邦法院命令，该命令要求苹果协助美国联邦调查局解锁圣贝纳迪诺枪击案中一名袭击者所使用的 iPhone。

【改写】 A federal court asked Apple to help the FBI ↔

a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI)

asked = requiring 的同义改写

access data in a terrorist's iPhone ↔

unlock an iPhone used by one of the two attackers who killed 14 people

unlock + attackers 上位概括为 access data + terrorist

【辨邻】 M 本段 the government could ask to use it proactively(先发制人地), before a suspected terrorist attack 用情态动词 could 表假设，没有 A federal court asked 这一已经下达的事实动作。

Once armed with a method for gaining access to iPhones, the government could ask to use it proactively

D 本段 has said he will appeal the court's order 是对法院命令的反应，没有再次陈述命令的内容，属下游动作。

has said he will appeal the court's order

39. Privacy advocates now have Apple fighting alongside them against government access to personal data.

隐私倡导者现在有**Apple**与他们并肩作战,反对政府获取个人数据。

【答案】 **H** 段 (强锚点)

【锚点】 隐私倡导者 + 苹果并肩

【定位】 So now, for many cases involving governmental intrusions into data, once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world.

于是如今,在许多政府入侵数据的案件中,曾经孤军作战的隐私倡导者发现自己正与世界上最强大的公司并肩作战。

【改写】 Privacy advocates now have Apple fighting alongside them ↔

once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world

视角调换的同义重写

against government access to personal data ↔ **governmental intrusions into data**

intrusions 上位 = access 反向同义

【辨邻】 **B** 本段 tech giants began to recognize the United States government as a hostile actor 缺少 Privacy advocates 这一独有角色,因此话题相邻但不命中。

tech giants began to recognize the United States government as a hostile actor

G 本段 made their opposition to the government's claims a point of corporate pride 立场虽与陈述句一致,但缺少 Privacy advocates 这一独有角色。

made their opposition to the government's claims a point of corporate pride

40. Snowden revealed that the American government had tried hard to access private data on a massive scale.

Snowden揭露了美国政府曾大力试图大规模获取私人数据。

【答案】 **B** 段 (强锚点)

【锚点】 斯诺登 + 政府大规模取数据

【定位】 After revelations by the former National Security Agency contractor Edward J. Snowden in 2013 that the government both cozied up to certain tech companies and hacked into others to gain access to private data on an enormous scale, tech giants began to recognize the United States government as a hostile actor.

在前国家安全局承包商爱德华·斯诺登于 2013 年揭露政府既讨好部分科技公司、又黑入其他公司以前所未有的规模获取私人数据之后,科技巨头开始把美国政府视为敌对方。

【改写】 Snowden revealed ↔

revelations by the former National Security Agency contractor Edward J. Snowden in 2013

动词 revealed = 名词 revelations

tried hard to access private data on a massive scale ↔

hacked into others to gain access to private data on an enormous scale

hacked + gain access = tried hard to access

【辨邻】 G 本段 Apple's stance on these issues emerged post-Snowden 中 Snowden 只承担「之后」这一时间状语，没陈述他「揭露了什么」。

Apple's stance on these issues emerged post-Snowden

41. The FBI might have been able to access private data in earlier iPhones without Apple's help.

FBI可能在没有Apple帮助的情况下就能够获取早期iPhone中的私人数据。

【答案】 J 段（强锚点）

【锚点】 早期 iPhone + FBI 无需苹果帮助

【定位】 And to get at the contents of a single iPhone, the government says it needs a court order and Apple's help to write new code; in earlier versions of the iPhone, ones that were created before Apple found religion on privacy, the FBI might have been able to break into the device by itself.

为了取得单部 iPhone 的内容，政府称它需要一份法院命令以及苹果的帮助来写新代码；而在更早期的 iPhone 上——即在苹果热衷隐私之前生产的那些——FBI 本可能自己就能闯入这部设备。

【改写】 earlier iPhones ↔ earlier versions of the iPhone

复数 iPhones = versions of the iPhone

access private data ... without Apple's help ↔

the FBI might have been able to break into the device by itself

break into + by itself = access ... without ... help

【辨邻】 K 本段 measures that it could put into place in the future will almost certainly be able to further limit the government's reach 把方向定为「未来 + 更收紧」，与陈述句的「过去 + FBI 能自己破」时间方向相反。

measures that it could put into place in the future will almost certainly be able to further limit the government's reach

C 本段 requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone 谈的是本案「必须靠苹果」，与陈述句「早期不必靠苹果」在时间维度上对立。

requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone

42. After the Snowden incident, Apple made clear its position to counter government intrusion into personal data by means of encryption.

Snowden事件之后,Apple明确表明了其通过加密手段对抗政府侵入个人数据的立场。

【答案】 G 段 (强锚点)

【锚点】 斯诺登事件后 + 加密对抗政府

【定位】 Apple's stance on these issues emerged post-Snowden, when the company started putting in place a series of technologies that, by default, make use of encryption to limit access to people's data.

苹果在这些议题上的立场出现在斯诺登事件之后——当时该公司开始部署一系列默认采用加密的技术,以限制对人们数据的访问。

【改写】 After the Snowden incident ↔ post-Snowden

after = post 同义改写

Apple made clear its position to counter government intrusion ↔

Apple's stance on these issues emerged post-Snowden

stance emerged = made clear position

by means of encryption ↔ make use of encryption(加密) to limit access to people's data

by means of = make use of 同义改写

【辨邻】 B 本段 tech giants began to recognize the United States government as a hostile actor 只讲态度,没有 by means of encryption 这一具体手段。

tech giants began to recognize the United States government as a hostile actor

H 本段 Apple's emerging global brand is privacy 是品牌层面的陈述,缺少 by means of encryption 这一手段词。

Apple's emerging global brand is privacy

43. According to one digital expert, no iPhone can be entirely free from hacking.

据一位数字专家称,没有任何iPhone能够完全免于被黑客攻击。

【答案】 P 段 (强锚点)

【锚点】 数字专家 + 没 iPhone 完全免黑

【定位】 "Nothing is 100 percent hacker-proof," Mr. Zdziarski said, but he pointed out that the judge's order in this case required Apple to provide "reasonable security assistance" to unlock Mr. Farook's phone.

Zdziarski 说,没有任何东西是百分之百防黑的,但他指出本案的法官命令要求苹果提供合理的安全协助,以解锁 Farook 的手机。

【改写】 According to one digital expert ↔ **Mr. Zdziarski said**

数字专家 = Zdziarski 引出方

no iPhone can be entirely free from hacking ↔ **Nothing is 100 percent hacker-proof**

100 percent hacker-proof = entirely free from hacking

【辨邻】 **N** 本段 I bet they are rethinking their threat model as we speak 是 Zdziarski 关于威胁模型重思的观点，没有 no iPhone can be entirely free from hacking 这一含义。

I bet they are rethinking their threat model as we speak

44. Timothy Cook's long web post has helped enhance Apple's image.

Timothy Cook的长篇网络帖子帮助提升了Apple的形象。

【答案】 **I** 段（强锚点）

【锚点】 库克长帖 + 抬高苹果形象

【定位】 "Then you had a few companies involved, but not one of the largest companies in the world coming out with a lengthy and impassioned post, like we saw yesterday from Timothy Cook. Its profile has really been raised."

他说，那时也有几家公司卷入，但没有一家像我们昨天看到的蒂姆·库克这样、来自世界上最大公司之一、发出一篇长篇又激情澎湃的网帖。它的知名度真的被抬高了。

【改写】 Timothy Cook's long web post ↔

a lengthy and impassioned post, like we saw yesterday from Timothy Cook

long = lengthy 同义改写

helped enhance Apple's image ↔ **Its profile has really been raised**

profile raised = image enhanced

【辨邻】 **D** 本段 Timothy Cook, has said he will appeal the court's order 是关于上诉的动作，没出现 long web post 与 enhance Apple's image。

Timothy Cook, has said he will appeal the court's order

45. Apple's CEO has decided to appeal the federal court's order to unlock a user's iPhone.

Apple的CEO已决定对联邦法院要求解锁用户iPhone的命令提起上诉。

【答案】 **D** 段（强锚点）

【锚点】 苹果 CEO + 上诉法院命令

【定位】 In the other corner is the world's most valuable company, whose chief executive, Timothy Cook, has said he will appeal the court's order.

另一角站的是世界上最有价值的公司，其首席执行官蒂姆·库克已表示将对法院命令提出上诉。

【改写】 Apple's CEO ↔ **chief executive, Timothy Cook**

CEO = chief executive 同义

appeal the federal court's order to unlock a user's iPhone ↔

has said he will appeal the court's order

will appeal = has decided to appeal

【辨邻】 I 本段 a lengthy and impassioned post, like we saw yesterday from Timothy Cook 谈库克的长帖与知名度抬升，没有 appeal 这一独特动词。

a lengthy and impassioned post, like we saw yesterday from Timothy Cook

C 本段 a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone 讲的是命令本身，主语是法院；陈述句主语是苹果 CEO，动作是上诉。

a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone

PARAGRAPHMAP • 段落主旨图

16 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 开篇定调：苹果与执法部门就解锁恐怖分子手机的对峙，是科技业与美国政府之间力量天平慢慢翻转的顶点。

信息指纹 力量翻转的顶点

B 斯诺登 2013 年揭露政府讨好部分科技公司、又黑入其他公司以大规模获取私人数据后，科技巨头开始把美国政府视为敌对方；长远看科技公司必胜。

信息指纹 斯诺登 2013 揭露

C 联邦法院周二下令要求苹果协助 FBI 解锁圣贝纳迪诺枪击案凶手之一使用的 iPhone。

信息指纹 联邦法院命令 + 圣贝纳迪诺案

D 苹果 CEO 蒂姆·库克表示将对法院命令提出上诉；苹果主张：削弱单部 iPhone 会让所有 iPhone 面临被任何政府入侵者攻破的风险。

信息指纹 库克声明上诉

E 胜负未卜，但底层逻辑很简单：苹果、谷歌、Facebook 等手握用户数据，其业务依赖于公众相信它们会尽全力保护数据。

信息指纹 公众相信会尽力护数据

F 一旦在保护数据这条战线上出现裂缝，对必须在全球运营的科技公司是致命的——为美国开了口子，俄罗斯、伊朗也会照样要求。

信息指纹 全球开口子的连锁后果

G 斯诺登事件后，苹果开始默认部署一系列加密技术来限制对用户数据的访问，并把反对政府主张作为企业骄傲。

信息指纹 斯诺登事件后默认加密

H 隐私已成为苹果的全球品牌；如今在不少涉政府入侵数据的案子里，原本孤军作战的隐私倡导者发现自己与全球最强公司并肩作战。

信息指纹 孤军隐私倡导者与苹果并肩

I 电子前沿基金会总顾问 Kurt Opsahl 将本案与 1990 年代加密之战对比：当年没有像库克这样来自全球最大公司之一的长篇激情贴文，事件知名度因此被大大抬高。

信息指纹 库克长贴抬高知名度

J 苹果手里还有一张王牌：用技术手段让设备越来越难被进入。当下取 iPhone 内容要靠法院令加苹果写新代码；而在更早期的 iPhone 上，FBI 本可能不靠苹果自己破解。

信息指纹 早期 iPhone 上 FBI 可自破

K 无论本案输赢，苹果未来还能再加码：把政府的触手限制得更死。

信息指纹 未来措施继续收紧束缚

L 本案结果并非无足轻重：迫使苹果写软件给 FBI 开口子会形成令人不安的先例，可能被援引到与国家安全无关的其他调查上。

信息指纹 形成令人不安的先例

M 一旦掌握进入 iPhone 的手段，政府可能在嫌疑恐袭发生前先发制人地使用；Opsahl 称这是绕开后门之争的迂回战术——直接下令制造后门。

信息指纹 先发制人 + 直接下令造后门

N 即便苹果最终输掉本案，它在技术上仍有大量手段随时间关闭后门；数字专家 Jonathan Zdziarski 称苹果工程师此刻应已在重新思考威胁模型。

信息指纹 工程师重思威胁模型

O Zdziarski 给出一种相对简单的对策：让未来的 iPhone 要求用户先输入密码，才能接受 FBI 想让苹果造的那种修改版操作系统；这样苹果就无法单方面装上削弱手机的代码。

信息指纹 用户输密码后才接受改版系统

P Zdziarski 强调没有任何东西百分之百防黑；若苹果让未来 iPhone 连自家工程师的合理协助都破不开，那么本案先例的长期效力就会失去——FBI 即便赢了本案，长期看也是输。

信息指纹 没东西百分之百防黑

SENTENCE INSIGHTS • 句子精讲

22 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。

After revelations by the former National Security Agency contractor Edward J. Snowden in 2013 that the government both coozied up to(讨好) certain tech companies and hacked into others to gain access to private data on an enormous scale, tech giants began to recognize the United States government as a hostile actor.

B段，第1句

本句体现四六级和考研阅读中的典型复杂句式：长时间状语从句前置 + 同位语从句嵌套 + 主句宾补结构。这种“前置修饰 + 主干后置”的句式以及同位语从句解释抽象名词的用法，在真题长难句中反复出现。掌握本句结构后，学习者可直接迁移到大量同类句型。

The action stems from a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, California, in December.

C段，第3句

本句主句成分完整（主语 + 谓语 + 状语），状语内部包含大量定语修饰（后置定语、分词短语作定语、不定式作定语），且定语从句嵌套在定语短语内部，覆盖了主谓宾、状语、定语、定语从句等多种成分类型。句中存在多个非谓语动词形式（过去分词、现在分词、不定式）易与谓语混淆，学习者需仔细区分；定语从句的先行词 "attackers" 距离关系代词 "who" 较远，也是常见的易错点。作为成分划分练习句，本句能帮助学习者熟悉复杂修饰结构中的成分识别方法。

In the other corner is the world's most valuable company, whose chief executive, Timothy Cook, has said he will appeal the court's order.

D段，第1句

这句话在结构上有明显训练点，难度中上但仍可控，既能练主干识别，也能练从属层级和时态切换。对于句子结构与时态训练，属于很值得优先讲解的一类材料。

Apple argues that it is fighting to preserve a principle that most of us who are addicted to our smartphones can defend: Weaken a single iPhone so that its contents can be viewed by the American government and you risk weakening all iPhones for any government intruder, anywhere.

D段，第2句

宾语从句 + 多层定语从句嵌套 + 目的状语从句的组合，是四六级和考研阅读中的高频典型结构；冒号引出解释性内容、“祈使句 + and + 陈述句”表条件结果的并列用法也是常考句式，掌握后可大量复用于真题长难句分析。

Yet underlying all of this is a simple dynamic: Apple, Google, Facebook and other companies hold most of the cards in this confrontation.

E段，第2句

句子涵盖了倒装结构中的主语、系动词、表语识别，同位语的判定，以及常规主谓宾结构中的并列主语、宾语、地点状语划分，成分种类丰富。倒装和同位语都是易错点，适合作为成分划分练习的典型材料。

If Apple is forced to write code that lets the FBI get into the iPhone 5c used by Syed Rizwan Farook, the male attacker in the San Bernardino attack, who would be responsible if some hacker got hold of that code and broke into its other devices?

F段，第3句

这句在结构拆解和时态辨认上都有明显训练价值，难度高但不是偏怪句，适合作为重点练习材料。尤其适合训练“先找连接标志，再穿透修饰，最后还原主干”的读句顺序。

Apple's emerging global brand is privacy; it has staked its corporate reputation, not to mention the investment of considerable technical and financial resources, on limiting the sort of mass surveillance that was uncovered by Mr. Snowden.

H段，第1句

结构典型性很高。分号连接并列句、限制性定语从句修饰名词、现在完成时强调过去动作的持续影响、插入语补充说明,这些都是四六级和考研阅读中的常见句式。尤其是 "stake...on..." 搭配、"not to mention" 插入语、关系代词 that 引导定语从句,都是高频考点结构。掌握本句的分析方法,可以迁移到大量类似长难句的理解中,实用性强。

Apple and other tech companies hold another ace: the technical means to keep making their devices more and more inaccessible.

J段，第1句

主谓宾加同位语解释的结构在四六级和考研阅读中较为常见，尤其是用冒号引出同位语的表达方式；不定式作后置定语、“keep doing”结构也是高频考点；掌握此句型有助于应对同类长难句。

And to get at the contents of a single iPhone, the government says it needs a court order and Apple's help to write new code; in earlier versions of the iPhone, ones that were created before Apple found religion on(热衷于) privacy, the FBI might have been able to break into the device by itself.

J段，第3句

覆盖目的状语、宾语从句、时间状语、同位语、定语从句、时间状语从句等多种成分，且存在易错点：目的状语前置、宾语从句省略 "that"、同位语插入打断主干、情态动词复合谓语的识别。适合作为成分划分的综合练习句，训练价值较高

Experts said that whether or not Apple loses this specific case, measures that it could put into place in the future will almost certainly be able to further limit the government's reach.

K段，第2句

高度典型的四六级和考研真题句式:主句加宾语从句,宾语从句内嵌套主语从句和定语从句,且定语从句修饰主语名词,这种多层嵌套结构在真题中频繁出现,掌握后可大量复用到同类长难句的理解中

As Apple and several security experts have argued, an order compelling Apple to write software that gives the FBI access to the iPhone in question would establish an unsettling precedent.

L段，第2句

本句在结构和时态两个维度都具备较高训练价值。主干识别难度适中偏高，嵌套层级清晰但主语内部修饰密集，时态覆盖三种常见形式，成分种类丰富且包含多个易错点，结构高度典型。综合来看，本句作为句子结构和时态训练材料非常合适，既有一定挑战性又不会过分艰深，且能有效提升学生应对真题长难句的能力。强烈推荐作为重点训练句优先练习。

Yet it is worth noting that even if Apple ultimately loses this case, it has plenty of technical means to close a backdoor over time.

N段，第1句

"it is + 形容词 + that 从句" 是四六级和考研阅读中的高频句式,主语从句内嵌套让步状语从句的结构也是长难句的典型模式,学生掌握后可直接迁移到大量真题句,代表性很强

One relatively simple fix, Mr. Zdziarski said, would be for Apple to modify future versions of the iPhone to require a user to enter a passcode before the phone will accept the sort of modified operating system that the FBI wants Apple to create.

O段，第1句

覆盖主语、系动词、表语、状语从句、定语从句、宾语、宾语补足语等多种成分,表语为复杂不定式结构,定语从句中关系代词充当宾语,成分种类丰富且包含易错的嵌套和复合结构,训练价值高。

"Nothing is 100 percent hacker-proof," Mr. Zdziarski said, but he pointed out that the judge's order in this case required Apple to provide "reasonable security assistance" to unlock Mr. Farook's phone.

P段，第1句

本句成分丰富且实用:涵盖主谓宾、主系表、宾语从句、宾语补足语、目的状语等多种成分,尤其第二个宾语从句中 required Apple to provide 的宾补结构和 to unlock 的目的状语是常考且易混淆的点,适合作为成分划分的训练材料

If Apple alters the security model of future iPhones so that even its own engineers' "reasonable assistance" will not be able to crack a given device when compelled by the government, a precedent set in this case might lose its lasting force.

P段，第2句

本句的 If 条件句 + so that 目的句 + when 时间句的多层嵌套结构，以及主句使用情态动词表推测的模式，在四六级和考研阅读中极为常见。掌握这种复杂条件句的分析方法，可以直接迁移到大量真题长难句的理解上，实用性很高。

In other words, even if the FBI wins this case, in the long run, it loses.

P段，第3句

让步状语从句插在主句中间是四六级和考研中常见的句式,"even if" 引导让步条件也是高频考点,这种结构在议论文和说明文中出现频率高,学习后可迁移到大量类似句子。

It is a popular belief that tech companies are committed to protecting their customers' private data.

第36题题干

"It is + 名词 + that从句"的形式主语句型在四六级和考研阅读中高频出现,常用于表达观点、信念、事实等。本句结构非常典型,掌握后可直接迁移到大量类似句式(如It is a fact that... / It is common knowledge that...等)。

The US government believes that its access to people's iPhones could be used to prevent terrorist attacks.

第37题题干

"主句 + that引导宾语从句" 是四六级和考研阅读中的高频句式，从句内使用情态被动结构也很常见，掌握后可大量迁移。

The FBI might have been able to access private data in earlier iPhones without Apple's help.

第41题题干

简单句 + 情态动词 + 完成式的组合在四六级和考研阅读中较为常见，尤其用于表达对过去情况的推测或假设。“主语 + 情态动词短语 + 宾语 + 状语”的线性排列是典型句式，学会后可迁移到大量类似结构。虽无从句增加复杂度，但作为情态完成式的代表句仍有较高复用价值。

After the Snowden incident, Apple made clear its position to counter government intrusion into personal data by means of encryption.

第42题题干

本句展示了简单句中常见的时间状语前置、“make + 宾语 + 宾补”句型以及不定式作后置定语的结构，这些都是四六级和考研阅读中的高频句式，掌握后可直接迁移到大量类似句子的分析中

According to one digital expert, no iPhone can be entirely free from hacking.

第43题题干

本句为简单句，使用情态动词加系表结构，属于四六级和考研阅读中常见的基本句式。情态动词表达可能性或能力的用法在真题中频繁出现，主系表结构也是基础句型之一。句首介词短语作状语的用法同样典型。掌握本句结构后，可迁移到大量类似句式中。

Apple's CEO has decided to appeal the federal court's order to unlock a user's iPhone.

第45题题干

“主语 + 现在完成时谓语 + 不定式宾语”是四六级和考研阅读中常见的句式，且不定式作定语修饰名词（“order to unlock...”）也是高频考点。但整体结构偏简单，缺乏从句嵌套等更典型的复杂句式，代表性中等偏上。

HIGH-FREQUENCY • 真题高频词

本篇出现的 126 个英语六级真题高频词

下列单词既在本篇真题中出现，又是 **英语六级** 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。

data B1

n. 数据

本篇10次 · 真题 181 句

access B1

n. 进入

本篇9次 · 真题 101 句

tech B1

n. 技术

本篇8次 · 真题 73 句

case A2

n. 情况

本篇7次 · 真题 97 句

court A2

n. 法院

本篇6次 · 真题 31 句

device B1

n. 设备

本篇5次 · 真题 54 句

security B1

n. 安全

本篇5次 · 真题 31 句

privacy B2

n. 隐私

本篇5次 · 真题 18 句

would A1

aux. (will 的过去式) 将要, 会

本篇4次 · 真题 568 句

expert B1

n. 专家

本篇4次 · 真题 114 句

code B1

n. 代码

本篇4次 · 真题 50 句

battle B1

n. 战斗

本篇4次 · 真题 29 句

attack A2

v. 攻击

本篇4次 · 真题 28 句

united B1

adj. 联合的

本篇3次 · 真题 97 句

limit B1

n. 限度

本篇3次 · 真题 51 句

mass B1

n. 大量

本篇3次 · 真题 44 句

user A2

n. 使用者

本篇3次·真题42句

means A2

n. 方法

本篇3次·真题35句

federal B2

adj. 联邦(制)的

本篇3次·真题29句

technical B2

adj. 技术的

本篇3次·真题23句

investigation B2

n. 调查;侦查

本篇3次·真题8句

precedent C1

n. 先例

本篇3次·真题8句

risk A2

n. 风险

本篇2次·真题167句

issue B1

n. 问题

本篇2次·真题158句

global B2

adj. 全球的

本篇2次·真题140句

argue B1

v. 争论

本篇2次·真题106句

gain B1

v. 获得;赢得

本篇2次·真题96句

belief B1

n. 相信

本篇2次·真题85句

states A1

n. 国家

本篇2次·真题80句

digital B1

adj. 数字的

本篇2次·真题72句

advocate B2

v. 拥护

本篇2次·真题55句

operate B1

v. 运转

本篇2次·真题52句

threat B1

n. 威胁

本篇2次 · 真题 51 句

appeal B2

v. 呼吁

本篇2次 · 真题 48 句

smartphone B1

n. 智能手机

本篇2次 · 真题 44 句

brand B1

n. 品牌, 商标

本篇2次 · 真题 37 句

datum C1

n. 数据 (单数形式, 复数为 data)

本篇2次 · 真题 34 句

emerge B2

v. 出现;浮现

本篇2次 · 真题 32 句

scale B1

n. 规模

本篇2次 · 真题 32 句

content B1

n. 内容

本篇2次 · 真题 31 句

legal B1

adj. 法律的

本篇2次 · 真题 23 句

version B1

n. 版本

本篇2次 · 真题 22 句

crack B1

v. 破裂

本篇2次 · 真题 18 句

assistance B1

n. 帮助

本篇2次 · 真题 16 句

corporate B2

adj. 公司的

本篇2次 · 真题 16 句

compel B2

v. 强迫;迫使

本篇2次 · 真题 15 句

request B1

n. 请求

本篇2次 · 真题 13 句

opposition B2

n. 反对

本篇2次 · 真题 12 句

modify B2

v. 修改, 更改 (使局部变化)

本篇2次 · 真题 11 句

reasonable B1

adj. 合理的

本篇2次 · 真题 10 句

alongside B1

prep. 在...旁边

本篇2次 · 真题 9 句

hack B2

v. 非法侵入 (计算机系统)

本篇2次 · 真题 8 句

system A2

n. 系统

本篇1次 · 真题 176 句

accord C1

n. (国家、团体间的) 协议

本篇1次 · 真题 167 句

view A2

n. 观点, 看法

本篇1次 · 真题 134 句

resource B1

n. 资源

本篇1次 · 真题 119 句

claim B1

v. 声称

本篇1次 · 真题 111 句

measure B1

v. 测量

本篇1次 · 真题 100 句

customer A2

n. 顾客, 客户

本篇1次 · 真题 87 句

involve B1

v. 包含

本篇1次 · 真题 82 句

financial B2

adj. 财政的

本篇1次 · 真题 79 句

further B1

adv. 更远地

本篇1次 · 真题 79 句

specific B2

adj. 具体的

本篇1次 · 真题 59 句

suffer B1

v. 遭受 (痛苦、疾病、损失等)

本篇1次 · 真题 59 句

media B1

n. 大众传播媒介 (报刊、电视、广播、互联...
本篇1次 · 真题 58 句

image A2

n. 形象, 印象
本篇1次 · 真题 57 句

principle B2

n. 原则, 准则
本篇1次 · 真题 54 句

reveal B2

v. 揭示
本篇1次 · 真题 54 句

debate B2

n. 辩论
本篇1次 · 真题 52 句

powerful B1

adj. 强大的
本篇1次 · 真题 50 句

certainly A2

adv. 当然
本篇1次 · 真题 43 句

electronic B1

adj. 电子的
本篇1次 · 真题 43 句

agency B2

n. 代理机构
本篇1次 · 真题 42 句

establish B2

v. 建立, 创立 (组织、机构、关系等)
本篇1次 · 真题 42 句

recognize B1

v. 认出
本篇1次 · 真题 42 句

outcome B2

n. 结果
本篇1次 · 真题 40 句

responsible B1

adj. 负责的
本篇1次 · 真题 40 句

investment B1

n. 投资
本篇1次 · 真题 39 句

official B1

adj. 官方的
本篇1次 · 真题 37 句

opinion A2

n. 观点
本篇1次 · 真题 37 句

relatively B2

adv. 相对地

本篇1次·真题 37 句

worldwide B1

adj. 全世界的

本篇1次·真题 35 句

giant B1

adj. 巨大的

本篇1次·真题 34 句

male A2

adj. 男性的

本篇1次·真题 34 句

preserve B2

v. 保护

本篇1次·真题 34 句

remove A2

v. 移开

本篇1次·真题 34 句

ultimately B2

adv. 最终;终归

本篇1次·真题 34 句

series B1

n. 系列

本篇1次·真题 33 句

enhance B2

v. 提高

本篇1次·真题 32 句

executive B2

n. 主管;经理;管理人员

本篇1次·真题 32 句

valuable B1

adj. 贵重的

本篇1次·真题 32 句

massive B2

adj. 巨大的, 大量的

本篇1次·真题 31 句

reputation B2

n. 名声

本篇1次·真题 30 句

entirely B1

adv. 完全地

本篇1次·真题 29 句

judge B1

v. 判断, 评判

本篇1次·真题 26 句

web A2

n. 网站

本篇1次·真题 26 句

comparison B1

n. 比较

本篇1次 · 真题 25 句

favor B1

n. 帮忙

本篇1次 · 真题 25 句

foundation B2

n. 基础;根基

本篇1次 · 真题 25 句

highlight B2

n. 最精彩的部分

本篇1次 · 真题 25 句

alter B2

v. 改变, 更改 (使某物与之前不同)

本篇1次 · 真题 24 句

software B1

n. 软件 (计算机程序)

本篇1次 · 真题 24 句

chief B1

n. 首领

本篇1次 · 真题 23 句

involved B1

adj. 参与的

本篇1次 · 真题 20 句

stem B2

n. 茎

本篇1次 · 真题 20 句

justify B2

v. 证明...有道理

本篇1次 · 真题 19 句

given B1

prep. 考虑到

本篇1次 · 真题 18 句

collective B2

adj. 集体的

本篇1次 · 真题 17 句

congress B2

n. 国会

本篇1次 · 真题 17 句

enormous B1

adj. 巨大的

本篇1次 · 真题 17 句

essentially B2

adv. 本质上

本篇1次 · 真题 17 句

hacker B2

n. 黑客 (非法入侵计算机系统者)

本篇1次 · 真题 17 句

bureau B2

n. 办事处

本篇1次 · 真题 14 句

underlie C1

v. 是.....的根本原因

本篇1次 · 真题 13 句

former B1

adj. 以前的, 从前的

本篇1次 · 真题 12 句

counter B1

n. 柜台

本篇1次 · 真题 10 句

religion B1

n. 宗教

本篇1次 · 真题 9 句

uncover B2

v. 发现, 揭露 (秘密、真相等)

本篇1次 · 真题 9 句

default B2

n. 违约

本篇1次 · 真题 8 句

defend B1

v. 保护

本篇1次 · 真题 8 句

dynamic B2

adj. 充满活力的

本篇1次 · 真题 8 句

fatal B2

adj. 致命的, 致死的

本篇1次 · 真题 8 句

prevail C1

v. 占上风

本篇1次 · 真题 8 句

profile B2

n. 简介

本篇1次 · 真题 8 句

stake B2

n. 股份

本篇1次 · 真题 8 句

sympathetic B2

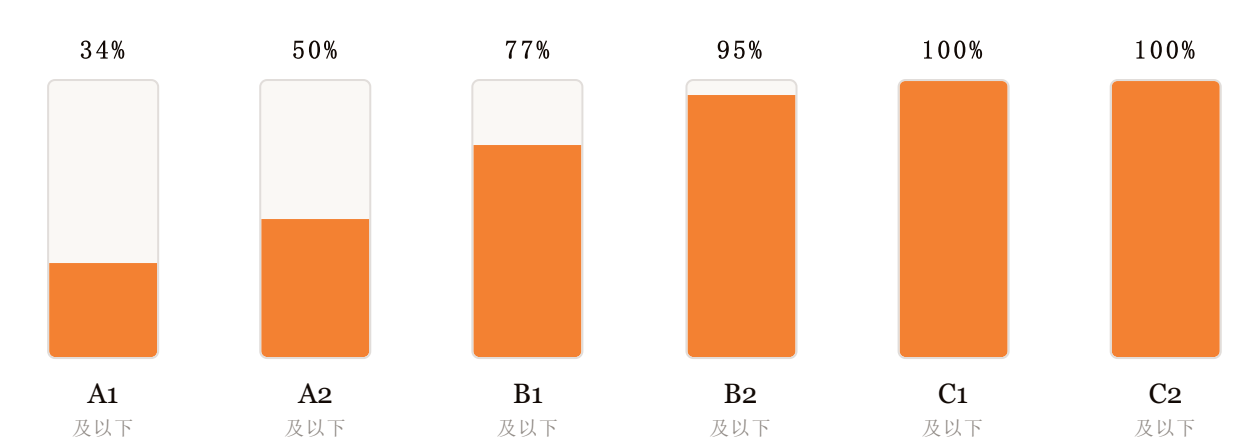
adj. 同情的

本篇1次 · 真题 8 句

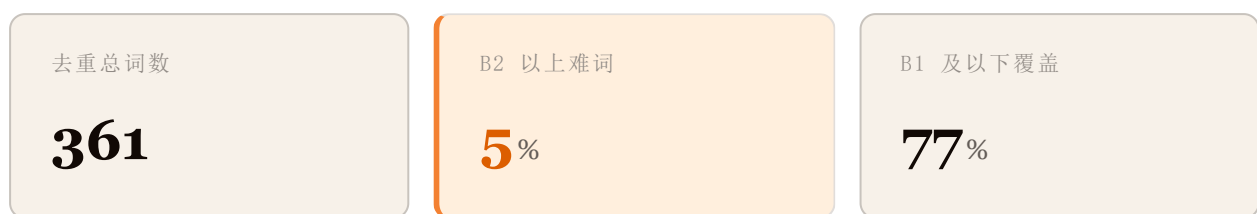
VOCABULARY · 词汇难度分布

全文 361 词按 CEFR 难度累积覆盖

全文去重后共 361 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 17 个 · 约 5%。



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 361 个 · 末柱为 100%



英语六级 2017年12月·第3套 · 全卷构成

Part I	写作	题目解析 →
Part II	听力	与2017年12月第1套共用 · 题目解析 →
Part III Section A	完形填空（选词填空）	题目解析 →
Part III Section B	长篇阅读（信息匹配）	本题
Part III Section C (1)	阅读理解（四选一）	题目解析 →
Part III Section C (2)	阅读理解（四选一）	题目解析 →
Part IV	汉译英（段落翻译）	题目解析 →