Unit 1
Mathematics

Lead In

In this unit, the latest application of modern mathematics is introduced into two fields. One is Game Theory which received special attention with the awarding of the Nobel Prize in economics to John Nash. Now it has been broadened theoretically and applied to many social problems. It has driven a revolution in economic theory. It has also found applications in sociology and psychology, and established links with evolution and biology. The other field is Digital Signature, which is the focus of cryptography studies. In text B, current applications of the Digital Signature technique are illustrated. From the article, readers can understand the basic concepts and principles of Digital Signature and may have an interest in continued study of cryptography.

Text A

Warm-up Questions:

1. What are the basic elements of games and what is the goal of the participants in the game?
2. In order to win in a game, what kind of approach or strategy should be applied?
3. What do you know about the applications of Game Theory in economics and other fields?
4. Have you ever watched the movie *A Beautiful Mind* or *The Da Vinci Code*? How did you like them and why?

Game Theory

by Avinash Dixit and Barry Nalebuff

1 Game theory is the science of strategy. It attempts to determine mathematically and logically the actions that "players" should take to secure the best **outcomes** for themselves in a wide **array** of "games". The games it studies range from chess to child rearing and from tennis to takeovers. But the games all share the common feature of **interdependence**. That is, the outcome for each participant depends upon the choices (strategies) of all. In so-called zero-sum games the interests of the players conflict totally, so that one person's gain always is another's loss. More typical are games with the potential for either mutual gain (positive sum) or mutual harm (negative sum), as well as some conflict.

2 Game theory was pioneered by Princeton mathematician John von Neumann. In the early years the emphasis was on games of pure conflict (zero-sum games). Other games were considered in a cooperative form. That is, the participants were supposed to choose and **implement** their actions **jointly**. Recent research has focused on games that are neither zero-sum nor purely cooperative. In these games the players choose their actions separately, but their links to others involve elements of both competition and cooperation.

3 Games are fundamentally different from decisions made in a **neutral** environment.

To illustrate the point, think of the difference between the decisions of a **lumberjack** and those of a general. When the lumberjack decides how to chop wood, he does not expect the wood to **fight back**; his environment is neutral. But when the general tries to **cut down** the enemy's army, he must anticipate and overcome resistance to his plans. Like the general, a game player must recognize his interaction with other intelligent and purposive people. His own choice must allow for both conflict and for possibilities for cooperation.

4 The essence of a game is the interdependence of player strategies. There are two distinct types of strategic interdependence: **sequential** and **simultaneous**. In the former the players move in sequence, each aware of the others' previous actions. In the latter the players act at the same time, each ignorant of the others' actions.

5 A general principle for a player in a sequential-move game is to look ahead and reason back. Each player should figure out how the other players will respond to his current move, how he will respond in turn, and so on. The player anticipates where his initial decisions will ultimately lead, and uses this information to calculate his current best choice. When thinking about how others will respond, one must **put oneself in their shoes** and think as they would; one should not impose one's own reasoning on them.

6 In principle, any sequential game that ends after a finite sequence of moves can be "solved" completely. We determine each player's best strategy by looking ahead to every possible outcome. Simple games, such as tic-tac-toe, can be solved in this way and are therefore not challenging. For many other games, such as chess, the calculations are too complex to perform in practice—even with computers. Therefore, the players look a few moves ahead and try to evaluate the resulting positions on the basis of experience.

7 **In contrast to** the **linear** chain of reasoning for sequential games, a game with simultaneous moves involves a logical circle. Although the players act at the same time, in ignorance of the others' current actions, each must be aware that there are other players who, in turn, are similarly aware, and so on. The thinking goes: "I think that he thinks that I think...." Therefore, each must **figuratively** put himself in the shoes of all and try to calculate the outcome. His own best action is an **integral** part of this overall calculation.

8 This logical circle is **squared** (the circular reasoning is brought to a conclusion)

using a concept of **equilibrium** developed by the Princeton mathematician John Nash. We look for a set of choices, one for each player, such that each person's strategy is best for him when all others are playing their **stipulated** best strategies. In other words, each picks his best response to what the others do.

9 Sometimes one person's best choice is the same no matter what the others do. This is called a dominant strategy for that player. At other times, one player has a uniformly bad choice—a dominated strategy—in the sense that some other choice is better for him no matter what the others do. The search for an equilibrium should begin by looking for dominant strategies and eliminating dominated ones.

10 When we say that an outcome is an equilibrium, there is no presumption that each person's privately best choice will lead to a **collectively optimal** result. Indeed, there are **notorious** examples, such as the prisoners' **dilemma** (see below), where the players are drawn into a bad outcome by each following his best private interests.

11 Nash's notion of equilibrium remains an incomplete solution to the problem of circular reasoning in simultaneous-move games. Some games have many such equilibria while others have none. And the dynamic process that can lead to an equilibrium is left unspecified. But in spite of these flaws, the concept has proved extremely useful in analyzing many strategic interactions.

12 The following examples of strategic interaction illustrate some of the fundamentals of game theory:

13 **The Prisoners' Dilemma.** Two suspects are questioned separately, and each can **confess** or keep silent. If suspect A keeps silent, then suspect B can get a better deal by confessing. If A confesses, B had better confess to avoid especially harsh treatment. Confession is B's dominant strategy. The same is true for A. Therefore, in equilibrium both confess. Both would fare better if they both stayed silent. Such cooperative behavior can be achieved in repeated plays of the game because the temporary gain from cheating (confession) can be outweighed by the long-run loss due to the breakdown of cooperation. Strategies such as **tit-for-tat** are suggested in this context.

14 **Mixing Moves.** In some situations of conflict, any systematic action will be discovered and exploited by the rival. Therefore, it is important to keep the rival guessing by mixing one's moves. Typical examples arise in sports—whether to run or

to pass in a particular situation in football, or whether to hit a passing shot cross-court or down the line in tennis. Game theory quantifies this insight and details the right proportions of such mixtures.

15 **Strategic Moves.** A player can use threats and promises to alter other players' expectations of his future actions, and thereby induce them to take actions favorable to him or **deter** them from making moves that harm him. To succeed, the threats and promises must be credible. This is problematic because when the time comes, it is generally costly to carry out a threat or make good on a promise. Game theory studies several ways to enhance credibility. The general principle is that it can be in a player's interest to reduce his own freedom of future action. By so doing, he removes his own temptation to **renege** on a promise or to forgive others' **transgressions**.

16 For example, Cortés burned his own ships upon his arrival in Mexico. He purposefully eliminated retreat as an option. Without ships to sail home, Cortés would either succeed in his conquest or **perish**. Although his soldiers were vastly outnumbered, this threat to fight to the death demoralized the opposition; it chose to retreat rather than fight such a determined opponent. Polaroid Corporation used a similar strategy when it purposefully refused to diversify out of the instant photography market. It was committed to a **life-or-death** battle against any intruder in the market. When Kodak entered the instant photography market, Polaroid put all its resources into the fight; fourteen years later, Polaroid won a nearly billion-dollar lawsuit against Kodak and regained its **monopoly** market.

17 Another way to make threats credible is to employ the adventuresome strategy of **brinkmanship**—deliberately creating a risk that if other players fail to act as one would like them to, the outcome will be bad for everyone. Introduced by Thomas Schelling in *The Strategy of Conflict*, brinkmanship "is the tactic of deliberately letting the situation get somewhat **out of hand**, just because its being out of hand may be intolerable to the other party and force his accommodation."

18 **Bargaining.** Two players decide how to split a pie. Each wants a larger share, and both prefer to achieve agreement sooner rather than later. When the two take turns making offers, the principle of looking ahead and reasoning back determines the equilibrium shares. Agreement is reached at once, but the cost of delay governs the shares. The player more impatient to reach agreement gets a smaller share.

19 **Concealing and Revealing Information.** When one player knows something that others do not, sometimes he is anxious to conceal this information (one’s hand in poker), and at other times he wants to reveal it credibly (a company’s commitment to quality). In both cases the general principle is that **actions speak louder than words**. To conceal information, mix your moves. **Bluffing** in poker, for example, must not be systematic. Recall Winston Churchill’s **dictum** of hiding the truth in a “bodyguard of lies”. To convey information, use an action that is a credible “signal”, something that would not be desirable if the circumstances were otherwise. For example, an extended **warranty** is a credible signal to the consumer that the firm believes it is producing a high-quality product.

20 Recent advances in game theory have succeeded in describing and prescribing appropriate strategies in several situations of conflict and cooperation. But the theory is far from complete, and in many ways the design of successful strategy remains an art.

(1, 654 words)

New Words

1. outcome /'aʊtkʌm/	*n.*	结果，成果
2. array /ə'reɪ/	*n.*	排列，编队
	v.	部署，排列
3. interdependence /ˌɪntədɪ'pendəns/	*n.*	互相依赖
4. implement /'ɪmplɪmənt/	*v.*	执行，贯彻
5. jointly /'dʒɔɪntlɪ/	*adv.*	共同地，连带地
6. neutral /'njuːtrəl/	*adj.*	中立的，中性的
7. lumberjack /'lʌmbədʒæk/	*n.*	伐木工人
8. sequential /sɪ'kwenʃəl/	*adj.*	连续的，有顺序的
9. simultaneous /ˌsɪməl'teɪnɪəs/	*adj.*	同时的，同时发生的
10. linear /'lɪnɪə(r)/	*adj.*	线性的，直线的
11. figuratively /'fɪgjʊrətɪvlɪ/	*adv.*	比喻地，象征性地
12. integral /'ɪntɪgrəl/	*adj.*	完整的，整体的

13. square /skweə(r)/	*v.*	使成方形；与……一致，符合
14. equilibrium /ˌiːkwɪ'lɪbrɪəm/	*n.*	平衡，均衡，均势 (*pl.* equilibria)
15. stipulate /'stɪpjʊleɪt/	*v.*	规定，保证
16. collectively /kə'lektɪvlɪ/	*adv.*	全体地，共同地
17. optimal /'ɒptɪməl/	*adj.*	最佳的，最理想的
18. notorious /nəʊ'tɔːrɪəs/	*adj.*	众所周知的；声名狼藉的
19. dilemma /dɪ'lemə/	*n.*	困境，进退两难的局面
20. confess /kən'fes/	*v.*	承认，坦白
21. tit-for-tat /ˌtɪtfɔː(r)'tæt/	*n.*	针锋相对
22. deter /dɪ'tɜː(r)/	*v.*	阻止
23. renege /rɪ'niːg/	*v.*	否认，食言
24. transgression /træns'greʃən/	*n.*	违反，犯罪
25. perish /'perɪʃ/	*v.*	毁灭，死亡
26. monopoly /mə'nɒpəlɪ/	*n.*	垄断，垄断者
27. brinkmanship /'brɪŋkmənˌʃɪp/	*n.*	边缘政策，边缘化
28. bluff /blʌf/	*v.*	诈骗，欺诈
29. dictum /'dɪktəm/	*n.*	格言
30. warranty /'wɒrəntɪ/	*n.*	保证，担保

Phrases and Expressions

1. fight back	抵抗，回击
2. cut down	砍倒；击败，战胜；削减，删节
3. put sb. in one's shoes	以……的立场(角度)出发，设身处地
4. in contrast to	与……形成对比(对照)
5. life-or-death	生死攸关的，重大的
6. out of hand	无法控制；脱手
7. actions speak louder than words	事实胜于雄辩，行胜于言

Notes

1. Game Theory: 博弈论，对策论
2. zero-sum game (Para. 1): 零和博弈。一人或一方得益必然引起另一人或另一方损失的局面。
3. Princeton (Para. 2): 普林斯顿。位于美国新泽西州。
4. John von Neumann (Para. 2): 约翰• 冯 • 诺依曼（1903−1957）。匈牙利裔美国数学家，致力于研究博弈论和控制论，并有相当贡献。
5. John Nash (Para. 8): 约翰 • 纳什。普林斯顿大学数学系教授，美国科学院院士，1994 年诺贝尔经济学奖得主，国际公认的博弈论创始人之一。他提出了“纳什均衡”（Nash equilibrium），对于两人以上的非合作对策，可能出现什么样的结果，给出了分析方法。
6. prisoners’ dilemma (Para. 10): 囚徒困境。博弈论的经典案例。
7. Cortés (Para. 16): 赫尔南多 • 科尔蒂斯。16 世纪殖民时代活跃在中南美洲的西班牙殖民者，以摧毁阿兹特克（Aztec）古文明，并在墨西哥建立西班牙殖民地而闻名。
8. Polaroid Corporation (Para. 16): （美国）宝丽来公司。以即时成像技术闻名。
9. Kodak (Para. 16): （美国）柯达公司

Language Points

1. The games it studies range from chess to child rearing and from tennis to takeovers. (Para. 1)

   Paraphrase: The “games” that game theory studies range from chess to child bring-up and from tennis to corporate takeovers.
2. The essence of a game is the interdependence of player strategies. (Para. 4)

   Paraphrase: The key principal of a game is that player strategies are dependent on each other.
3. A general principle for a player in a sequential-move game is to look ahead and reason back. (Para. 5)

   Paraphrase: A commonly-applied rule for a participant in a sequential game is to anticipate and think logically in turn.

4. The logical circle is squared ... (Para. 8)

   square the circle: to attempt sth. impossible 做(似乎是)不可能的事

5. When we say that an outcome is an equilibrium, there is no presumption that each person's privately best choice will lead to a collectively optimal result. (Para. 10)

   Paraphrase: When we mention that game result is an equilibrium, there is no assurance that each player's best choice will lead to the best effect for all the players.

   此句是一个复合句，when 引导时间状语从句，主句 there is no presumption 中又包含一个同位语从句 that each person's privately best choice will lead to a collectively optimal result，修饰 presumption。

6. Such cooperative behavior can be achieved in repeated plays of the game because the temporary gain from cheating (confession) can be outweighed by the long-run loss due to the breakdown of cooperation. (Para. 13)

   Paraphrase: Since the long-term loss brings more harmful effects than the temporary gain from cheating (confession) once cooperation breaks down, cooperative behavior can be achieved in repeated plays of the game.

Exercises

I. Content Questions

Directions: *Work in pairs and answer the following questions according to Text A.*

1. What kind of games did early game theory mathematicians emphasize? What is the current research focus?
2. Are game strategies different from decisions made in a neutral environment? Why or why not?
3. How many types of strategic interdependence are there in games? What are they?
4. What are the general principles for players in each game?
5. Describe the concept of Nash equilibrium. How is it used in circular reasoning of games?
6. In tennis why is it crucial for players to mix their moves?

7. What is brinkmanship strategy in games of conflict?
8. What is the process of bargaining for players? What agreement can be reached?

II. Questions for Discussion

Directions: *Work in groups and discuss the following questions.*

1. In your opinion, what is the interdependence between competition and cooperation?
2. Do you think Nash's concept of equilibrium is a complete solution to problems in strategic interactions? Why or why not?
3. Can you predict the future of game theory studies? What will be the new applications of it?

III. Text Organization

Directions: *Work in groups and discuss the organization of the text and fill in the chart.*

Parts	Paragraphs	Main Ideas
Part One	Paras. 1-3	Game theory can be defined as ___________________ which studies both ___________ and ____________.
Part Two	Paras. 4-11	There are ___________ distinct types of strategic interdependence: ____________________ and ___________.
Part Three	Paras. 12-19	The typical examples of game theory are given as the basic principles such as ____________________.
Part Four	Para. 20	The research of game theory has succeeded in illustrating strategies in ____________________ and it will focus on ____________________ in future.

IV. Multiple Choice

Directions: *Choose the best answer for each item.*

1. The term "games" in game theory all shares the characteristic of ________.

A. integrity　　B. interference

C. interaction　　D. interdependence

2. According to the passage, recent research of game theory lays its emphasis on ________.

   A. zero-sum games B. pure conflict

   C. pure cooperation D. competition and cooperation

3. In simultaneous-move games, the player should ________.

   A. watch how the other players respond and then respond in turn

   B. be conscious of the other players' current actions

   C. be thinking in a linear chain of reasoning and calculate the possible outcome

   D. try to select his best response to what the others do

4. In the sentence "Other games were considered in a cooperative form. That is, the participants were supposed to choose and implement their actions jointly", the underlined word "implement" means ________.

   A. select B. fulfill C. diversify D. quantify

5. We can infer from "The Prisoners' Dilemma" of game theory that ________.

   A. it belongs to the so-called zero-sum games because the interests of the prisoners conflict totally

   B. an equilibrium can be reached in repeated plays of the game in order to avoid mutual loss

   C. the prisoners are ignorant about whether their partner cooperates with them or confesses to the authorities

   D. a precondition has been set that each prisoner's personal best option will turn to a jointly optimal outcome

6. According to the authors, which of the following statements is true?

   A. Nash's concept of equilibrium addresses the issues of both sequential-move and simultaneous-move games.

   B. The pursuit of an equilibrium should end up looking for dominant strategies or eliminating dominated players.

   C. Nash's concept of equilibrium doesn't specify the dynamic process which can result in an equilibrium.

   D. An equilibrium will ultimately be arrived at in simultaneous-move games.

7. To keep the rival guessing or losing, the use of mixing moves can be found in ________.

   A. lumberjack chopping wood

   B. Cortés conquering Mexico in 16th century

   C. Polaroid securing a monopoly market

   D. a tennis player hitting a passing shot

8. In the sentence "When we say that an outcome is an equilibrium, there is no presumption that each person's privately best choice will lead to a collectively optimal result", the underlined word "presumption" means ________.

   A. hypothesis B. conclusion C. meditation D. anticipation

9. Which of the following ways can enhance the credibility of threats and promise to affect the opponent in a strategic interaction?

   A. Keeping the rival guessing.

   B. Using the strategy of brinkmanship.

   C. Bargaining to have a better outcome.

   D. Concealing and revealing information.

10. In the sentence "A player can use threats and promises to alter other players' expectations of his future actions, and thereby induce them to take actions favorable to him or deter them from making moves that harm him", the underlined word "deter" means ________.

   A. alter B. remind C. stimulate D. prevent

V. Blank Filling

Directions: *Fill in the blanks with words given below.*

methodology	constructing	journal	preferences	prime
modeling	interactive	purchasing	enhances	abuse

The internal consistency and mathematical foundations of game theory make it a(n) ___1___ tool for modeling and designing automated decision-making processes in ___2___ environments. For example, one might like to have efficient bidding rules for an auction website, or tamper-proof automated negotiations for ___3___ communication bandwidth. Research in these applications of game theory is the topic of recent conference and ___4___ papers, but is still in a nascent stage. The automation of strategic choices ___5___ the need for these choices to be made efficiently, and to be robust against ___6___. Game theory addresses these requirements. As a mathematical tool for the decision-maker the strength of game theory is the ___7___ it provides for structuring and analyzing problems of strategic choice. The process of formally ___8___ a situation as a game requires the decision-maker to enumerate explicitly the players and their strategic options, and to consider their ___9___ and reactions. The discipline involved in ___10___ such a model already has the potential of providing the decision-maker with a clearer and broader view of the situation. This is a "prescriptive" application of game theory, with the goal of improved strategic decision-making.

VI. Cloze

Directions: *Choose the best answer for each blank of the following passage.*

Few social situations can be modeled accurately by a single interaction. ___1___, most situations result from a series of interactions over a long period of time. An ___2___ version of the Prisoner's Dilemma scenario includes repeated interaction, which ___3___ the probability of cooperative behavior.

The ___4___ of this version of Prisoner's Dilemma suggests that a player's strategy (___5___ or cooperate) depends on his or her experience in ___6___ interactions, and that that strategy will also affect the future behavior of one's ___7___. The result is a relationship of mutual reciprocity (互惠); a player is likely to cooperate ___8___ his or her opponent previously ___9___ willingness to cooperate, and is unlikely to cooperate if the opponent previously did not. The ___10___ that the game will be played again leads players to ___11___ the consequences of their actions; one's opponent may ___12___ or be unwilling to cooperate in the future, if one's strategy always seeks ___13___ payoffs at the expense of ___14___ player.

In a ___15___ experiment, Robert Axelrod demonstrated that the "winning" strategy in a repeated prisoner's dilemma is one that he ___16___ "tit-for-tat". This strategy ___17___ cooperation on the first move, and in each subsequent move, one chooses the behavior demonstrated by one's opponent in the previous round. ___18___ , there is no "right" or best solution to the ___19___ presented by Prisoner's Dilemma. One lost round in a two-player game can be devastating for a player, and the ___20___ to defect always exists.

1.	A. Even	B. Rather	C. Though	D. Thus
2.	A. extended	B. expanded	C. excluded	D. expected
3.	A. broadens	B. narrows	C. increases	D. decreases
4.	A. truth	B. regulation	C. reasoning	D. logic
5.	A. defect	B. compete	C. violate	D. assist
6.	A. potential	B. subsequent	C. previous	D. sequential
7.	A. partner	B. colleague	C. enemy	D. opponent
8.	A. once	B. if	C. unless	D. whether
9.	A. demonstrated	B. eliminated	C. illustrated	D. anticipated
10.	A. principle	B. presumption	C. knowledge	D. calculation
11.	A. ignore	B. stipulate	C. discover	D. consider
12.	A. regret	B. retaliate	C. retreat	D. renege
13.	A. maximum	B. majority	C. minimum	D. minority
14.	A. another	B. other	C the other	D. one another
15.	A. computer-analyzed		B. computer-assisted	
	C. computer-instructed		D. computer-simulated	
16.	A. defines	B. terms	C. induces	D. decides
17.	A. calls off	B. calls up	C. calls out	D. calls for
18.	A. Still	B. Yet	C. Instead	D. However
19.	A. obstacle	B. difficulty	C. conflict	D. paradox
20.	A. interaction	B. competition	C. willingness	D. temptation

VII. Writing

Directions: *Game theory is widely applied in the fields of politics, economics, sociology, biology, law and sports. Please write a brief report about the latest development of game theory in one field which you are interested in (within 600 words). Use the resources available, library or Internet etc. for your references. Make an outline of your report in Powerpoint format and give a presentation in class.*

科技英语阅读方法（一）

名词化结构

大量使用名词化结构是科技英语最突出的特点之一。科技文体要求行文简洁、表达客观、内容确切、信息量大、强调存在的事实。而使用名词化结构的优点正是叙述客观，强调动作的客体而非动作本身，并能够用来代替同位语从句等较长的句子结构，从而使得文章简洁紧凑。

要准确理解一篇文章，就必须正确把握句子的结构和中心信息，因此准确阅读和理解名词化结构尤为重要。名词化结构主要分为以下三类：

1. 单纯名词化结构

单纯名词化结构指由一个或多个名词修饰一个中心名词构成的名词化结构。理解这类名词化结构的重点是确定中心名词，然后确定其他的修饰名词与中心名词的关系。

water purification system

这个名词化结构的中心名词是 system，purification 修饰 water，因此该结构相当于 a system for the purification of water。

laser noise amplitude modulation

该结构的中心名词是 modulation，laser 作为方式修饰 noise amplitude，该结构相当于 modulation of noise amplitude by means of a laser。

2. 复合名词化结构

复合名词化结构由一个中心名词和形容词、名词、副词、分词及介词短语等多个前置或后置修饰语构成。理解这类结构首先要确定中心名词，然后判断修饰语之间以及与中心名词之间的逻辑关系。意义越具体、物质性越强、与中心名词的关系越密切的修饰词离中心名词越近，如 acute bacterial peritonitis（急性细菌性腹膜炎）。

3. 由动词派生的名词化结构

这类名词化结构通常是由实义动词派生的名词搭配介词短语构成，在句中充当主语、宾语或介词宾语。

Archimeds first discovered the principle of displacement *of water by solid bodies.*

句中的名词化结构 displacement of water by solid bodies 由 displace 的名词加上两个介词短语构成，用来补充说明 the principle。一方面简化了同位语从句，另一方面强调 displacement 这一事实。此句译为：阿基米德最先发现了固体排水的原理。

The building of these giant iron and steel works will greatly accelerate the development of the iron and steel industry of our country.

句中的名词化结构 the building of these giant iron and steel works 由 build 的动名词加上介词短语构成，充当句子的主语，其逻辑结构为动宾结构。

Dr. Almaraz had assisted in *the removal of a lymph node* from a patient infected with AIDS.

句中用名词 removal 来代替动词 remove，从而使得文章用词更为正式，而且表达客观发生的事实。此句译为：阿尔马拉兹医生曾协助给一位艾滋病人切除淋巴结的手术。

科技英语翻译技巧（一）

名词化结构

科技文章涵盖大量概念性、原理性词汇及表达，因而与普通英语相比，名词化结构在科技英语中更为普遍。在科技英语中名词化结构通常作句子的主语、宾语或定语，在翻译时应根据中文的行文习惯将名词化结构转化为不同的成分。

1. 将名词化结构译为动词。许多名词化结构是由实义动词派生的名词作为中心名词并搭配介词短语构成，在翻译时根据汉语习惯可以还原成动词来译。如：

All substances will permit *the passage of some electric current*, provided the potential difference is high enough.

这里名词 passage 在翻译时要译为动词“通过”。此句可翻译为：只要有足够的电位差，电流便可通过任何物体。

Television is *the transmission and reception* of images of moving objects by radio waves.

句中名词化结构 the transmission and reception 应翻译为动词“发射和接收”。此句译为：电视通过无线电波发射和接收活动物体的图像。

2. 将名词化结构译为动宾关系。大多数复合名词性词组可以使用这种翻译方法。

As a small-scale illustration of *the artificial modification of physical weather processes*, take the frost prevention in an orchard.

句中的名词化结构 the artificial modification of physical weather processes 中，physical weather processes 是中心名词 the artificial modification 的修饰语，根据中文的特点，将这个名词化结构译为动宾结构“对天气的物理过程进行人工影响”。此句译为：我们可举果园中防霜作为说明对天气的物理过程进行小尺度人工影响的例子。

3. 将名词化结构译为独立的从句。这种译法通常出现在名词化结构较长而且较为复杂的情况下。

The slightly porous nature of the surface of the oxide film allows it to be colored with either organic or inorganic dyes.

句中的主语 the slightly porous nature of the surface of the oxide film 是一个较为复杂的名词化结构，译为一个的独立从句“氧化膜表面具有轻微的渗透性”，且与主句形成因果关系。此句译为：氧化膜表面具有轻微的渗透性，因此可以用有机或无机染料着色。

This position was completely reversed by *Haber's development of the utilization of nitrogen from the air*.

句中的名词化结构 Haber's development of the utilization of nitrogen from the air 放到句首作为原因状语从句，译为“由于哈勃发明了利用空气中的氮气的方法”。此句译为：由于哈勃发明了利用空气中的氮气的方法，这种局面就完全改观了。

Translation Practice

I. Exercises for Practicing the Skills (Pay attention to the underlined part)

1. The first application is in community access networks, such as the Cerritos, Calif., <u>rollout with equipment from Tropos Networks or the Garland, Texas, deployment by NexGen City</u> with ASICs from MeshNetworks.
2. The transformer is a device of very great practical importance which makes use of <u>the principle of mutual induction</u>.

3. During the 19th century, the theories of tidal and acoustic gravity oscillations were subjects of great interest.
4. Incentives for cost minimization are increased, and costs become more transparent.
5. The deployment of 911 across cellular networks is being addressed in three steps.
6. Because of the wide range of nanoproducts in use or under development, it is important to establish which materials should be tested first and how to perform this testing.
7. But all the games share the common feature of interdependence.
8. Technology for development will allow construction of larger projects, artificial intelligence (intelligent agents, knowledge based systems, data mining and intelligent filtering, and so on) will be increasingly feasible as costs decrease, performance improves and widespread networking are available.

II. Word and Phrase Translation

A. **Directions:** *Translate the following expressions into Chinese.*

1. mutual gain game and mutual harm game
2. sequential-move game
3. simultaneous-move game
4. linear reasoning
5. circular reasoning
6. Nash equilibrium
7. dominant strategy
8. optimal result
9. breakdown of cooperation
10. strategy of brinkmanship

B. **Directions:** *Translate the following expressions into English.*

1. 完全博弈
2. 竞争与合作
3. 策略性相互作用
4. 囚徒困境
5. 长远性损失
6. 针锋相对策略
7. 策略混合
8. 打斜线球或底线球（网球）
9. 垄断性市场
10. 均衡份额

III. Sentence Translation

Directions: *Translate the following English sentences into Chinese. (Pay attention to the underlined part)*

1. The essence of a game is the interdependence of player strategies. There are two distinct types of strategic interdependence: sequential and simultaneous.
2. When we say that an outcome is an equilibrium, there is no presumption that each person's privately best choice will lead to a collectively optimal result.
3. In some situations of conflict, any systematic action will be discovered and exploited by the rival. Therefore, it is important to keep the rival guessing by mixing one's moves. Typical examples arise in sports—whether to run or to pass in a particular situation in football, or whether to hit a passing shot cross-court or down the line in tennis.
4. Brinkmanship "is the tactic of deliberately letting the situation get somewhat out of hand, just because its being out of hand may be intolerable to the other party and force his accommodation."
5. When one player knows something that others do not, sometimes he is anxious to conceal this information (one's hand in poker), and at other times he wants to reveal it credibly (a company's commitment to quality). In both cases the general principle is that actions speak louder than words.

Text B

Digital Signature in Applied Cryptography

1 **Cryptography** literally means "the art of secret writing". It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an **eavesdropper**, referred to as Eve, will not be able to listen in on their communication. Cryptography also enables Bob to check that the message sent by Alice was not modified by Eve and that the message he receives was really sent by Alice.

2 Public key cryptography is not only used to protect messages. An important application is the creation and checking of so-called digital signatures. Digital signatures are coupled to the electronic document to which they apply. This coupling is established using public-key cryptography and so-called cryptographic **hash** functions.

The basic principle of digital signature

3 In public key cryptography, anything Alice **encrypts** with Bob's public key can be **decrypted** by Bob with the corresponding private key. Alice can also encrypt a message with her private key, which means that Bob can decrypt it with Alice's public key. Since the public key is, as the name suggests, publicly available, this is not a very good idea if Alice wants to keep that message a secret. Eve can also simply obtain a copy of Alice's public key and thus also decrypt the message.

4 But because Alice keeps her private key to herself, Bob knows that only Alice could have encrypted this message. Bob can now be sure that this message was written by Alice. A signature on a paper message serves as proof that this message was written by the person who signed it. Encrypting with a private key thus can be regarded as an **equivalent** to placing one's signature on the message. This is why this is called creating a digital signature for the message.

5 If Alice wants to keep the message a secret that only Bob is allowed to learn, she of course then simply encrypts the digitally signed message with Bob's public key. Bob first decrypts the message with his own private key and then decrypts the result with Alice's public key. He now knows that no one else could have read the message (because it was encrypted using his public key) and that no one but Alice could have written this message (because it was encrypted using her private key).

How digital signatures work

6 Digitally signing large messages takes a long time, just like encrypting large messages with someone's public key. Just like with public key encryption, placing digital signature therefore involves an extra step. First a summary of the message is computed, and then this summary is signed.

Cryptographic hash functions

7 The summary is generated using so-called cryptographic hash functions. A

cryptographic hash function can **transform** input of an arbitrary length **to** an output of a certain number of **bits**, typically 128 or 160 bits. The output is called the hash value. Well-known hash functions are MD5 and SHA-1, although many more exist.

8 A very simple example of a hash function is to simply **add up** the position in the alphabet of all the characters in the message. For example, the message "ape" would give as output 22 (1 plus 16 plus 5). Since the hash value is usually shorter than the message itself, this makes it easier and faster to compare two messages or to find a particular message in a table. For example, it is common in database management systems to compute the hash value of all the names in a database with information on people. To determine whether a particular person occurs in the database, the hash value of his name is computed against the hash values of all the names. This is much faster than comparing the name itself against all the names in the database, because the hash value is a number of a fixed length. Names can be many characters long and each character has many more possibilities than just 0-9. Hash functions should have two **properties**:

a. Given a particular output, it should be difficult to find a message that has that particular output (for cryptographers this means the hash function is "one-way").

b. Given two messages, the chance that they have the same hash value should be small (cryptographers refer to this as "collision-free").

9 If a particular hash function has these properties, it is called a cryptographic hash function. It is now possible to use the hash value of a message instead of the message itself.

10 The simple example given above does not have these properties. There are many messages that have the hash value 22. And furthermore, it is quite easy to find another message that also has this hash value.

Cryptographic hash functions and digital signatures

11 Hash functions can be used to determine whether a message has been modified. Alice computes the hash value of the message she wants to send to Bob and sends the hash value of the message together with the message to Bob. Bob computes the hash value of the message he receives, and compares it against the hash value he received from Alice. If these two hash values are the same, Bob knows that the message was

not modified. **After all**, the second property of the hash function says that the chance that the modified message has the same hash value as the original message is very small.

12 Eve can now no longer just modify the message without Bob noticing this. However, Eve can modify the message and compute the hash value of the modified message. She can then replace the hash value that Alice sent with the hash value she computed. Bob will then think that the message was not modified, because the message he received has the same hash value as the one he got from Alice. But Bob has no way to know that he did not get that hash value from Alice.

13 Of course this is where digital signatures come in. After computing the hash value of the message she wants to send, Alice digitally signs this hash value and sends the result (the digital signature of the message) to Bob. Bob then decrypts the digital signature using Alice's public key. He compares the result with the hash value he computed for the message he received and so determines whether the message was modified. If everything **checks out**, Bob knows that this message really came from Alice and it was not modified.

14 Because Eve does not have Alice's private key, she is no longer able to replace the hash value that Alice signed with the hash value of the modified message. And it is next to impossible for Eve to modify the message in such a way that the hash value remains the same. Because of the first property of the hash function, it is difficult for Eve to find another message that has the same hash value. And even if she manages to find one, the chance that this other message is even remotely the same as the original message from Alice is extremely small.

15 An important reason for using a cryptographic hash function is that the message remains in unencrypted form. Furthermore, the (digitally signed) hash value can now be **transmitted** and stored **invisible** to the user, for example as part of the headers of an e-mail message or **encapsulated** using the well-known MIME standard. The digital signature can also be transmitted over an entirely separate channel. Alice could publish the digital signature of a message in a newspaper. This way, she could later prove that she had a copy of this message on the date of publication of this newspaper without having to reveal the message. This can be useful for example if Alice had to

prove that she wrote a particular message and did not **infringe** on somebody else's copyright.

Applications of digital signatures

16 Digital signatures offer many applications other than signing messages such as e-mail. A digital signature can be created for any kind of file. The digital signature then can be used as proof that the file was not modified after the digital signature was created. It can also be used to make the file unique, for example by **appending** a serial number to the file and signing the result.

Authenticating Web servers

17 Using public key cryptography a Web browser and server can communicate with each other securely. The browser can encrypt a session key using the public key of the server and send it to the server.

18 In this application the Web browser typically obtains a copy of the public key of the server by requesting a certificate containing this public key from the server. This certificate has been signed by some trusted third party. The public key of this trusted third party has been programmed into the Web browser beforehand. Using this public key the browser can determine that the certificate is authentic. The browser then knows it has the right public key.

Electronic money (digital cash)

19 Making files unique with digital signatures is the basis of digital cash (electronic money). Alice the banker creates electronic banknotes of various **denominations** and puts a unique number on every banknote. She signs the result. Bob the client now makes a withdrawal from his account with Alice and receives some of the signed banknotes. The banknotes can be **anonymous** or include Bob's name. Bob then goes to Charlie's electronic hardware store and purchases a digital camera using these banknotes as payment. Charlie verifies that the banknotes bear Alice's signature and so knows that they are not **counterfeit**.

20 Bob could of course make as many copies of the signed banknotes as he wants, since the banknotes are in electronic form. Charlie therefore now has to go to Alice and report to her the unique number on the banknote he received. Alice will then record that number as "spent" and indicate to Charlie that the transaction is okay. If

the number was already recorded as “spent”, Alice will reject the transaction. If the transaction is okay, the amount indicated on the banknotes **is credited to** Charlie’s account.

21 This system has many advantages over traditional payment techniques. Alice can create banknotes of any denomination, including for example millicents (0.001 cents). This way for example an electronic **archive** could charge one millicent for every document Bob requests, and Bob could pay that without having to take a subscription or make a deposit in advance.

22 One disadvantage of this system is that it requires Charlie to immediately check with Alice whether the banknote is still valid. If Charlie waits even a few minutes, Bob can spend the banknote again at Dave’s. Then either Charlie or Dave is not going to get his money.

23 This principle is currently used for electronic **coupons**. As a coupon is less valuable than a banknote, the risk of double spending a coupon appears to be acceptable. Furthermore, coupons are usually only valid at one particular store.

Signed computer programs

24 Digital signatures can also be used to authenticate software applications. The manufacturer of a computer program can generate a digital signature for the **executable**. When a user downloads the program, he can verify that the digital signature is correct. He then knows that this program was really made by that particular manufacturer. If he trusts that manufacturer, he can safely install the application. The manufacturer of course promises that the application will not do anything **malicious**.

25 The source code of many open source software programs is distributed together with the digital signature of the author(s). This way the recipients can check that they have not been modified by anyone else. For instance everyone can verify the authenticity of the Linux kernel by checking whether it was properly signed by Linus Torvalds.

26 ActiveX controls (more or less comparable to Java applets, but based on a Microsoft standard) are digitally signed. Microsoft’s Internet Explorer checks the digital signature using a Microsoft public key installed in the browser. The control is

only executed if the digital signature is authentic. If the signature does not check out, or the browser security level is set to high, the user will be asked to confirm execution.

27 Unfortunately it appears to be difficult to properly sign ActiveX controls so that all users can verify that the signature is authentic. This has led to the practice of telling users in the installation **manual** or on the web page containing the control to simply press “Yes” whenever Internet Explorer says anything about the digital signature. This makes it of course very easy for a hacker to replace the ActiveX control with anything he desires. Although the digital signature will not check out, the user will simply follow the manual and click “Yes” anyway.

28 More recently suggestions have been made to extend this application to hardware as well. The CPU in a PC would check the digital signature on the operating system or on applications to be executed. If the digital signature does not check out, or it was not created by an authorized manufacturer, the CPU refuses to execute the operating system or program. It is unclear at the time of writing whether the owner of the PC in question will be able to indicate who are authorized manufacturers.

(2, 200 words)

New Words

1.	cryptography /krɪp'tɒgrəfɪ/	*n.*	密码学，密码系统
2.	eavesdropper /'iː vzˌdrɒpə(r)/	*n.*	偷听者
3.	hash /hæʃ/	*n.*	哈西值；无用信息，杂乱信号
4.	encrypt /ɪn'krɪpt/	*v.*	加密，将……译成密码
5.	decrypt /diː 'krɪpt/	*v.*	解密，破译（电文）
6.	equivalent /ɪ'kwɪvələnt/	*n.*	等同的事物，相等物
7.	bit /bɪt/	*n.*	位，比特
8.	property /'prɒpətɪ/	*n.*	性质，特性
9.	transmit /trænz'mɪt/	*v.*	传输，传送，传导
10.	invisible /ɪn'vɪzəbl/	*adj.*	看不见的，无形的
11.	encapsulate /ɪn'kæpsəleɪt/	*v.*	装入胶囊，压缩
12.	infringe /ɪn'frɪndʒ/	*v.*	破坏，侵犯，违反

13. append /ə'pend/	*v.*	附加，添加
14. authenticate /ɔː'θentɪkeɪt/	*v.*	鉴别
15. denomination /dɪˌnɒmɪ'neɪʃən/	*n.*	命名
16. anonymous /ə'nɒnɪməs/	*adj.*	匿名的
17. counterfeit /'kaʊntəfɪt/	*n.*	赝品，伪造品
	adj.	伪造的，假冒的
	v.	伪造，假冒
18. archive /'ɑːkaɪv/	*v.*	存档
	n.	档案文件
19. coupon /'kuːpɒn/	*n.*	商家的优待券，优惠券
20. executable /'eksɪkjuːtəbl/	*adj.*	可执行的，实行的
21. malicious /mə'lɪʃəs/	*adj.*	怀有恶意的，恶毒的
22. manual /'mænjʊəl/	*n.*	手册，指南

Phrases and Expressions

1. transform to	转换，变换，把……变成
2. add up	合计，计算总数
3. after all	毕竟，终究
4. check out	检验；合格，及格
5. be credited to	被记入账户的贷方，被划入账户

Notes

1. cryptographic hash function (Para. 2): 加密哈西函数
2. hash value (Para. 7): 哈西值
3. MD5 (Para. 7): 单向加密的加密算法。MD5 的全称是 Message-Digest Algorithm 5，在 20 世纪 90 年代初由 MIT 的计算机科学实验室和 RSA Data Security Inc 发明，经 MD2、MD3 和 MD4 发展而来。MD5 按 512 位数据块为单位来处理输入，产生 128 位的消息摘要。
4. SHA-1 (Para. 7): SHA（Secure Hash Algorithm）算法由 NIST 开发，并在 1993 年作为联邦信息处理标准公布。在 1995 年公布了其改进版本 SHA-1。SHA

与 MD5 的设计原理类似，同样也按 512 位数据块为单位来处理输入，但它产生 160 位的消息摘要，具有比 MD5 更强的安全性。

5. MIME standard (Para. 15): 多用途的网际邮件扩充协议标准。MIME 指的是 Multipurpose Internet Mail Extension protocol，多用途的网际邮件扩充协议。
6. source code (Para. 25): 源代码
7. Linux (Para. 25): 一种可免费使用的 UNIX 操作系统，运行于一般的 PC 机上，是开放源代码的操作系统。
8. Linus Torvalds (Para. 25): 李纳斯·托沃兹。Linux 内核的发明人和 Linux 系统的创始人，1969 年 12 月 28 日出生于芬兰赫尔辛基市，毕业于赫尔辛基大学计算机系。
9. ActiveX control (Para. 26): ActiveX 控件。以前也叫做 OLE 控件或 OCX 控件，它是一些软件组件或对象，可以将其插入到 WEB 网页或其他应用程序中。ActiveX 插件技术是国际上通用的基于 Windows 平台的软件技术，除了在线杀毒插件之外，许多软件均采用此种方式开发，例如 Flash 动画播放插件、Microsoft MediaPlayer 插件、CNNIC 通用网址插件、网络实名插件等。
10. Java (Para. 26): 一种编程语言。Java 编程语言可被用来创建任何常规编程语言所能创建的应用程序。

Language Points

1. Cryptography also enables Bob to check that the message sent by Alice was not modified by Eve and that the message he receives was really sent by Alice. (Para. 1)

   此句中宾语从句的主语 message 由分词 sent 作后置定语修饰，这也是科技文章的特点之一。

   译文：密码学知识可以帮助鲍勃核查由艾丽斯发出的信息未经夏娃修改，并且他所获取的信息确实由艾丽斯发出。
2. A signature on a paper message serves as proof that this message was written by the person who signed it. (Para. 4)

   译文：书面文件上的签名的作用在于证明这一文件确实由签名的人所书写。
3. Encrypting with a private key thus can be regarded as an equivalent to placing one’s signature on the message. (Para. 4)

   译文：因此用密钥解码可以看作是一个与文件签名相等同的过程。

4. Just like with public key encryption, placing digital signature therefore involves an extra step. (Para. 6)

   Paraphrase: Placing digital signature needs an additional step, just as with public encryption.

   译文：就像使用公钥加密一样，加装数字签名也还需要一个额外的步骤。

5. Furthermore, the (digitally signed) hash value can now be transmitted and stored invisible to the user, for example as part of the headers of an e-mail message or encapsulated using the well-known MIME standard. (Para. 15)

   Paraphrase: Moreover, the (digitally signed) hash value can now be sent and stored though users cannot see it. For instance, it can be used as part of the header of an e-mail or enclosed using the MIME standard.

   译文：而且，（经过数字签名的）哈西值现在可以以不向用户公开的方式进行传输和保存，例如作为电子邮件的部分标题，或者运用著名的多用途的网际邮件扩充协议标准压缩哈西值。

6. The public key of this trusted third party has been programmed into the Web browser beforehand. (Para.18)

   译文：具有公信力的第三方公钥之前已经被安装在网络浏览器上。

7. Making files unique with digital signatures is the basis of digital cash (electronic money). (Para. 19)

   译文：用数字签名标识文档是数字货币（电子货币）的基础。

8. The source code of many open source software programs is distributed together with the digital signature of the author(s). (Para. 25)

   译文：许多开放性的软件程序的源代码和程序作者的数字签名一起被公布出来。

9. For instance everyone can verify the authenticity of the Linux kernel by checking whether it was properly signed by Linus Torvalds. (Para. 25)

   Paraphrase: For example, every user can confirm the credit of the Linux kernel by checking whether it was properly signed by Linus Torvalds.

   译文：例如每个用户可以通过检查利纽克斯内核是否由李纳斯·托沃兹签署来确定它的真实性。

Exercises

I. Content Questions

Directions: *Work in pairs and answer the following questions according to Text B.*

1. In the communication of Alice and Bob, how can they avoid being overheard by Eve?
2. What is the basic principle of digital signature in public key cryptography?
3. What is the extra step before placing digital signature on large messages?
4. By using cryptographic hash functions, how can we transform input of an arbitrary length to an output of a certain number of bits?
5. What are the basic properties of hash functions?
6. Describe the MIME standard.
7. How can a Web browser determine that his/her Web server is authentic?
8. What are the advantages of electronic money over traditional payment? What is the possible defect?
9. How can we use digital signature to authenticate software applications?
10. What are the recent digital signature applications to hardware?

II. Questions for Discussion

Directions: *Work in groups and discuss the following questions.*

1. Which is more appealing for you, traditional payment or electronic money? Why?
2. What do you feel will be the future development of the digital signature technique?

III. Word Processing

Directions: *Fill in the blanks with appropriate words or phrases, using the information obtained from the text.*

1. Digital signatures are coupled to the ________ document to which they apply. This coupling is established using ________ and so-called cryptographic hash functions.
2. A cryptographic hash function can transform input of a(n) ________ length to an output of a certain number of bits, typically 128 or 160 bits.

3. Hash functions should have two properties: the hash function is ________ and ________.
4. An important reason for using a cryptographic hash function is that the message remains in ________ form. Furthermore, the (digitally signed) hash value can now be transmitted and stored ________ to the user.
5. The digital signature then can be used as ________ that the file was not modified after the digital signature was created. It can also be used to make the file unique, for example by appending a(n) ________ to the file and signing the result.
6. Using public key cryptography a Web ________ and ________ can communicate with each other securely.
7. As a coupon is less valuable than a banknote, the risk of ________ spending a coupon appears to be acceptable. Furthermore, coupons are usually only ________ at one particular store.
8. The ________ of many open source software programs is distributed together with the digital signature of the author(s).
9. Microsoft's Internet Explorer checks the digital signature using a Microsoft public key installed in the browser. The control is only executed if the digital signature is ________.
10. If the digital signature does not check out, or it was not created by a(n) ________ manufacturer, the CPU refuses to execute the ________ system or program.

IV. True or False

Directions: *Read each of the following statements carefully and decide whether it is true or false according to the text.*

1. The use of public key cryptography is only to protect messages.
2. Encrypting electronic messages with private keys is just similar to a written signature on paper.
3. The extra step of placing a digital signature means to sign the summary of the message first and then compute the summary.
4. One basic quality of the cryptographic hash function is that two messages are very likely to have identical hash values.

5. The current popular hash functions, MD5 and SHA-1, have replaced other equivalents.
6. With the well-known MIME standard, the digitally signed hash values can be transmitted and stored indiscernible to the user.
7. Though digital signature is proof to confirm the file was not modified after the digital signature is created, it cannot reveal the uniqueness of the original file.
8. The communications between a Web browser and server are less risky with a delivered certificate containing the public key from the browser.
9. In the payment of digital cash, a client should always make sure that the electronic banknotes are signed before withdrawing money from the account.
10. The ActiveX control is executable only if Microsoft's Internet Explorer checks that the digital signature (signed in ActiveX control) is authentic.

V. Translating and Editing

Directions: *Translate and edit Paras. 19-23 from Text B into Chinese with no more than 200 Chinese characters.*