国际商务师业务外语辅导：先进加密标准国际商务师考试

For the past three years， the National Institute of Standards and Technology (NIST) has been working to develop a new encryption standard to keep government information secure． The organization is in the final stages of an open process of 0selecting one or more algorithms， or data-scrambling formulas， for the new Advanced Encryption Standard (AES) and plans to make adecision by late summer or early fall． The standard is slated to go into effect next year． AES is intended to be a stronger， more efficient successor to Triple Data Encryption Standard (3DES)， which replaced the aging DES， which was cracked in less than three days in July 1998.
“ Until we have the AES， 3DES will still offer protection for years to come． So there is no need to immediately switch over， ” says Edward Roback， acting chief of the computer security division at NIST and chairman of the AES 0selection committee． “ What AES will offer is a more efficient algorithm． It will be a federal standard ， but it will be widely implemented in the IT community． ”
According to Roback， efficiency of the proposed algorithms is measured by how fast they can encrypt and decrypt information ， how fast they can present an encryption key and how much information they can encrypt． The AES review committee is also looking at how much space the algorithm takes up on a chip and how much memory it requires． Roback says the 0selection of a

more efficient AES will also result in cost savings and better use of resources. “ DES was designed for hardware implementations , and we are now living in a world of much more efficient software , and we have learned an awful lot about the design of algorithms, ”says Roback. “ When you start multiplying this with the billions of implementations done daily, the saving on overhead on the networks will be enormous. ” The process of 0selecting the algorithm for AES has been notable for its openness and transparency. This is a marked departure from the government ’s past inclination toward secrecy in discussing encryption standards , which led to the public cracking of DES after critics questioned the government ’s assertion that the standard was still secure. NIST kicked off the 0selection process in September 1997. Conferences were held in August 1998 and March 1999 ；cryptographers from around the world discussed the algorithm candidates and helped narrow the list to 15 and then to five finalists：IBM ’s MARS ；RSA Laboratories* RC6 ；Joan Daemen and Vincent Rijmen ’s Rijndael；Ross Andersen, Eli Baham and Lars Knudsen ’s Serpent；and Counterpane Labs* Twofish. While most evaluators of the algorithms want to avoid complexity by 0selecting one to serve as a standard, there ’s a minority that wants to 0select more than one. 在过去三年中，（美国）国家标准与技术局（NIST）已在研究开发一种新的加密标准，以确保政府的信息安全。该组织目前正处于为新的先进加 密标准（AES）选择一个或几个算法或数据打乱公式的开放过程的最后阶段，并计划在夏末或秋初作出决定。此标准内定明年实施。 AES预定为比

三层数据加密标准(3DES)更强、更高效的后续标准，3DES替代了老化的DES加密标准，DES在1998年7月在不到三天的时间内就 被破译了。 NIST计算机安全部的代理主管兼AES选择委员会主席Edward Roback说 ：“ 在我们拥有AES之前，3DES还将在今后几年提供保护。所以没有必要马上转换。AES所提供的是一种更有效的算法。它将是一项联邦标准，但它将在IT界 广泛实施。 ”据Roback称，提议中的算法的效率是通过对信息加密和解密有多快、给出加密密钥有多快以及能对多少信息加密等几个方面进行测量的。 AES评价委员会也要看算法占据芯片上多少空间和需要多少内存。Roback说，选择一个更高效的AES也会带来成本的节省和资源的更好利用。 Roback说：“ DES是为硬件实现而设计的，而我们现在处于软件更高效的世界，我们对算法的设计有极多的了解。当我们开始大规模使用此算法，每天实现几十亿次的加密时，（算法带来的）网络开销的节省将是巨大的。 ”为AES选择算法的过程是以其公开性和透明度称著。这标志着政府从以往讨论加密标准时倾向于保密的做法一刀两断，它导致了政府在断言DES 标准仍是安全时被公开破译。 NIST在1997年9月开始这个选择过程。1998年8月和 1999年3月召开了会议，来自全世界的密码专家讨论了候选的算法，帮助把算法缩小到15 个，最后到了5个：IBM的MARS算法，RSA实验室的RC6算法、Joan Daemen和Vincent Rijmen两人的Rijndael算法、Eli Baham和Lars Knudsen两人的Serpent算法以及Counterpane 实验室的Twofish算法。 大多数算法鉴定者都选择一个作标准以避免复杂性，但也有一小部分人要选择多个算法。 把国际商务师站点加入收藏夹 欢迎进入：2010年国际商务师课程免费试