中 山 大 学

二OO五 年港澳台人士攻读博士学位研究生入学考试试题

科目代码：771

科目名称：计算机网络

考试时间： 4 月 17 日 上 午

考 生 须 知

全部答案一律写在答题纸上，答在试题纸上的不得分！

答题要写清题号，不必抄题。

一、 简单回答下列问题（每小题3分，共30分）

1） 什么是计算机安全？什么是网络安全？什么是信息安全？

2） 什么是 DES？AES？RSA？

3） 身份认证在网络安全中起到举足轻重的地位，它属于保障信息完整性服务的范畴。认证的目的主要有哪两个？

4） 什么是数字签名？

5） 什么是 Hash 函数？

6） 什么是 Kerberos？

7） 什么是 PKI 技术？

8） 什么是 PGP？

9） 什么是 MD5？

10） 什么是 SHA1？

二、在一个 RSA 公钥密码体制中，已知素数 p = 3，q = 11，公钥 e = 7，明文 M = 5，计算私钥 d，并对明文进行加密、解密运算。（10 分）

三、（25 分）

1） 请给出信息理论中一个离散信源 S 及 S 的 Shannon 熵(entropy) H(S)

的详细定义。(10 分)

2) 假设信源字母表 S ={*a*, *b*}, 其对应的概率分布为 P = { $p_1 = 0.9$, $p_2 = 0.1$}试求 H(S)。(5 分)

3) 请用信息论中熵的概念解释：为什么通常的一幅彩色照片所包含的信息量与比它要大很多的一段文本所包含的信息量要大得多？ (10 分)

四、数据压缩与数据加密有何联系？并证明你的结论。(10 分)

五、(25 分)

1) Huffman 编码是 1952 年发表的，现在还有用吗？请用例子简单说明你的结论。(10 分)

2) 请简单地介绍一下 Huffman 编码、LZ 编码、算术编码，这三种编码方法的主要差别及各自的优点。(10 分)

3) 考虑信源(S = {a, b, c, d, 1, 2}, *P* = {0.35, 0.10, 0.19, 0.25, 0.06, 0.05})。构造信源(S, P)的 Huffman 编码。(5 分)