

目录

- IPv6** 3
- 几个特殊地址 3
- 攻击手法和对策 3

IPv6

几个特殊地址

IPv6的Global Unique Address相当于IPv4的单播地址(即Global Address),是以001开头的,所以2001:满足.

LoopBackAddress则类似于IPv4的127.0.0.1,在IPv6中是::1

攻击手法和对策

20240324 SC模拟考试解答讲义笔记

问1:

CRYPTREC推奨暗号方法 (アルゴリズム)

共通鍵暗号方式

- ブロック暗号 AES ブロック長128ビット/鍵長、256と192ビット Camellia
- ストリーム暗号 KCipher-2

認証付き暗号 AEAD TLS1.3で登場する。認証は、改ざんのチェックです。

AEADの例 AES-GCMとAES-CCM

鍵共有アルゴリズム :

From:
<https://www.zhangzt315.com/> - 八百标兵奔北坡

Permanent link:
<https://www.zhangzt315.com/doku.php?id=b.%E7%90%86%E8%AE%BA%E5%82%A8%E5%A4%87%07.%E5%AE%89%E5%85%A8%E4%BB%8E%E4%B8%9A%E8%B5%84%E6%A0%BC:sc&rev=1711344167>

Last update: 2024/03/25 05:22

