



2023年1月，国家密码管理局发布《关于开展商用密码应用安全性评估从业人员考核的公告》以来，密评从业人员考核培训需求激增，为更好的满足市场需求，公司精心打造师资团队，推出商用密码理论知识与安全性评估人员知识强化和应考培训，针对性提高学员密评基础知识和应试能力。

商用密码应用与安全性评估知识培训

专家名师授课，专业答疑解惑

培训采取线上直播授课模式，老师线上讲解答疑，采用密评考试平台测验。针对国密局发布的《关于公布商用密码应用安全性评估从业人员考核知识点的通知》，公司专门邀请国内知名的密码研究和应用领域的专家，对密码基础原理、密码应用法规体系、密评工作规范要求等进行详细分析讲解，对问题进行答疑解惑。理论学习结合模拟考试，通过实训助力密评考试能力有效提升。

培训形式

在线直播平台授课

密评考试平台刷题考试

联系方式

拨打公司电话，为您提供全方位的培训咨询和报名事项服务。

联系电话：4000-181-171

培训内容

5天36小时，课程紧凑，干货满满，长期开班。

<p>密评考核形式介绍 摸底测试</p>	<p>帮助学员快速熟悉以往密评考试形式，培训老师了解学员基础情况，有针对性的提供培训方案。</p>
<p>密码基础培训</p>	<p>密码基础培训面向密码基础相对薄弱的学员，帮助其快速熟悉密码基本概念和基础知识、算法及应用，为开展密评工作奠定基础。</p>
<p>密码应用培训</p>	<p>通过培训商用密码相关的政策法规、标准体系及产品实现，助力学员构建科学、完整的密码知识体系，深化对密码基础知识的理解与应用。</p>
<p>密评工作培训</p>	<p>围绕“商用密码应用安全性评估”工作，对密评工作的内容、测评实施、报告编制、结果备案等全生命周期的内容进行培训，帮助学员建立系统完整的密评工作体系架构。</p>
<p>培训效果考核</p>	<p>培训完成后，检验培训效果，巩固培训成果。</p>

加密+MAC→可鉴别的加密模式

- 分组密码算法两大功能
 - 加密
 - MAC
- 研究人员将两种功能合并
 - 即可鉴别的加密模式 (Authenticated encryption)
 - 可同时实现数据的机密性、完整性以及对数据真实性的鉴别。
- 相关国家标准GB/T 36624-2018《信息安全技术 安全技术 可鉴别的加密机制》已经发布
 - CCM (Counter with CBC-MAC)：应用在 802.11协议族
 - GCM (Galois/Counter Mode) 等模式，在 TLS 1.2 以后的算法套件中广泛应用



密码算法安全强度

随着计算机领域的不断发展，密码算法要求的安全强度也在变化

- 80 bit 安全强度的算法和密钥长度已经禁止使用
- 2030年以后，112bit安全强度也不再满足要求，会被禁止或限制使用

密钥长度	DES	ZUC	SM4	AES	SM9	SM7	SM8	SM12
40	DES	ZUC	SM4	AES-40	SM9	SM7	SM8	SM12
56	DES	ZUC	SM4	AES-56	SM9	SM7	SM8	SM12
128	DES	ZUC	SM4	AES-128	SM9	SM7	SM8	SM12
192	DES	ZUC	SM4	AES-192	SM9	SM7	SM8	SM12
256	DES	ZUC	SM4	AES-256	SM9	SM7	SM8	SM12

《量化评估》编制原则

依据GB/T 39786-2021和GM/T 0115-2021，对信息系统的密码应用情况给出定量评估结果。

- 遵循法律法规和相关指导性文件的总体要求
- 遵循GB/T 39786-2021和GM/T 0115-2021
- 引导方向 (安全) 密码技术 (2021版-2023版)
- 特别鼓励使用合规的密码算法/技术/产品/服务
- 优先在网络和数据安全层面、应用和数据安全层面推进密码技术应用 (权重高)

密码算法分类

- 对称密码算法**
 - 以一种在不知道密钥的情况下难以恢复的方式变换数据，其密钥是“对称的”，加密计算及其逆计算 (解密) 都使用“同一”密钥。
 - 对称密码通常由多个实体掌握；但是，密钥不得向未经授权访问该算法和密钥保护的数据的实体公开。
- 公钥密码算法**
 - 通常称为公钥密码算法，使用“两个”相关密钥 (即密钥对) 来执行它们的功能：公钥和私钥。
 - 任何人都可以知道公钥；但私钥应该由“拥有”密钥的实体单独控制。即使密钥对的公钥和私钥是相关的，也不能使用公钥的知识来推算出私钥。
- 密码杂凑算法**
 - 可以为一个相对较长的消息生成一个小的摘要值，而且这种特性是单向的，即难以从一个给定的摘要值反向推算出消息。
 - 密码杂凑函数本身一般不需要密钥参与，但是它是其他算法和密钥管理的重要基础。

国内外典型分组密码算法比较

SM4算法和AES算法安全性和性能比较如下：

密钥长度 (比特)	分组长度 (比特)	加密轮数 (比特)	实现性能
AES 128, 192, 256	128	10/12/14	密钥扩展算法复杂；加解密算法不同；实现起来较为复杂
SM4 128/128	128	32	加解密算法相同，密钥顺序互逆；加解密算法与扩展基本相同；实现起来较为简单

杂凑算法的抗碰撞性

- 抗碰撞性 (单向性, 抗原像攻击)**
 - 即给定杂凑值，找到原像使用 $H^{-1}(M)$ 是困难的。密码杂凑函数是单向的，从消息计算杂凑值很容易，但从杂凑值推出消息是非常困难的。
- 弱碰撞自由 weak collision-free (抗第二原像攻击)**
 - 即对于给定的消息M1，找不到不同的另一个消息M2，使得 $HASH(M1)=HASH(M2)$ 。在计算上是不可行，则HASH函数是弱碰撞自由的。
- 强碰撞自由 strong collision-free**
 - 即如果找到两个不同消息M1和M2，使得 $HASH(M1)=HASH(M2)$ ，在计算上不可行，则HASH函数是强碰撞自由的。

2004年王小云院士宣布成功找到了MD4和MD5等算法的碰撞，之后不久，SHA-1算法也被证明存在碰撞。2017年2月，腾讯和微软研究人员合作找到了世界首例针对SHA-1算法的碰撞实例。

