第 2 讲 什么是密码？

密码讲堂开讲的第一课必须先讲一讲“什么是密码”，因为日常生活中的“密码”并不是我所说的这个“密码”。日常生活中所说的“密码”，实际上是口令，英文是 password，是登录账户所需的认证凭证。而密码讲堂中所说的密码的英文是 cryptography。建议广大读者以后不要再把口令说成是密码了。

那什么是密码？2020 年 1 月 1 日正式施行的《中华人民共和国密码法》的第二条给出了准确和权威的答案：**本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务**。根据这个定义，我们就能准确地理解什么是密码。

首先就是明确定义了密码的形态。密码是一项技术，称为密码技术；也可以是一种产品，称为密码产品；也可以是一种服务，称为密码服务。密码以三种形态存在，可以是技术、产品和服务，这为密码从业者指明了发展方向，可以从事密码技术研究，可以从事密码产品研发、生产和销售，也可以提供密码服务，以服务形式来提供密码产品，通常指云密码服务或称密码云服务。

第二就是明确定义了密码的用途。密码可用于加密保护和安全认证，准确理解这个用途非常重要，给密码从业者指明了密码到底该用在什么地方。请大家注意：第一个用途是加密保护，这是用途最广泛的应用，如 HTTPS 加密、邮件加密和数字签名、文档加密和数字签名、软件代码数字签名等。CA 机构所签发的 SSL 证书、电子邮件证书、电子文档证书、代码签名证书等就是用于上述加密保护用途的。第二个用途是安全认证，用数字签名技术来实现安全可靠的用户身份认证。这就是国内 CA 机构签发的 USB Key 证书所实现的用途，而国际 CA 机构所做的业务则是提供市场更广泛的加密保护用途的各种数字证书。相信各个国内 CA 机构应该能从这里看到差距和改革的方向，第一个用途更有前途，这也是为何密码的定义是加密保护在前、安全认证在后的根本原因。本密码讲堂将重点讲密码在加密保护方面的技术、产品、服务及其应用。

第三就是明确了技术路线，那就是通过特定变换的方法来实现。这里所指的特定变换的方法就是密码算法，用密码算法来实现特定变换。《密码法》中所指的密码算法是特指国产密码算法，如：SM2、SM3、SM4 和 SM9 等商用密码算法，不包括国外的密码算法，这一点非常重要，一定不能搞错，虽然整个密码法全文都没有明确指出。

第四就是明确了密码的保护对象：信息等，信息需要用密码来实现加密保护，信息同时需

要密码来实现安全认证后才能获取。这里还有一个“等”字非常重要，“信息”这个词范围非常广，包含了人类社会传播的一切内容，如音讯、消息、通讯系统传输和处理的各种对象；但如果还有未包含的，则用“等”字来包含，所有等等都可以用密码来实现加密保护和安全认证，这就不难理解为何其他相关法律如《数据安全法》、《个人信息保护法》等都要求采用密码来保护数据安全和个人信息安全。

大家从上面的解读《密码法》第二条就可以看到，《密码法》虽然不到 5000 字，但内容博大精深，仅仅一条只有 42 个字的第二条就包含了四层含义，每一层又有多个含义。所以，密码从业者或对密码感兴趣的读者一定要仔细解读《密码法》，网上有不少的解读，笔者仅仅是从技术上解读了其中最关键的一条。

密码讲堂所讲的所有内容均属于商用密码范畴，不涉及到核心密码和普通密码范畴。按照《密码法》第八条“商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全”，密码讲堂所讲的所有内容都属于使用商用密码保护网络与信息安全的技术、产品和服务。

《密码法》第二十一条则特别明确了“国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展”，这为密码从业者指明了发展方向，鼓励大家从事商用密码技术的研究和开发，鼓励大家从事商用密码技术的学术交流，鼓励大家把商用密码研究成果进行产业化转化和推广应用到各行各业，并且是要建立一个既开放又要有序竞争的市场体系，从而促进商用密码产业的健康发展。

《密码法》真的是一个博大精深的国家大法，笔者会在后续的讲座中的相关内容中继续解读《密码法》的内容。 有了《密码法》，就可以让密码技术、密码产品和密码服务在法律的保护下健康蓬勃发展，让《密码法》能真正为保障我国万物互联安全提供法律保障。

最后需要特别说明的是，密码讲堂中提到的很多名词名称如：国密算法、国密 SSL 证书、国密证书透明、国密证书自动化管理等等，可以同时对应地理解为：商用密码算法(商密算法)、商用密码 SSL 证书(商密 SSL 证书)、商用密码证书透明(商密证书透明)、商用密码证书自动化管理(商密证书自动化管理)等等，笔者喜欢用前一组名称，因为这组名称有一种自豪感，一种用我国自己的密码技术来保障我国万物互联安全的自豪感和责任感。

-----下一讲内容预告-----

第 3 讲 什么是 PKI/CA？什么是数字证书？

本讲将讲解密码的最重要的应用之一--数字证书，这是密码讲堂的核心内容，后续的讲座都是讲数字证书相关的知识和应用。

王高华

2023 年 2 月 13 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。