

密码算法简介

罗鹏

中国科学院信息工程研究所

2017.01.01

大纲

- ▶ 对称密码算法 (私钥密码算法)
 - ▶ 分组密码 (Block Cipher)
 - ▶ 流密码 (Stream Cipher)
 - ▶ 工作模式 (Mode of Operation)
 - ▶ 密码杂凑函数 (Hash Function)
 - ▶ 消息认证码 (Message Authentication Code)
 - ▶ 认证加密 (Authenticated Encryption)
- ▶ 非对称密码算法 (公钥密码算法)
 - ▶ 密钥交换算法 (Key Exchange)
 - ▶ 公钥加密 (Public-Key Encryption)
 - ▶ 数字签名 (Digital Signature Algorithm)

分组密码 (Block Cipher)

经典分组密码

- ▶ **DES**
- ▶ **AES**
- ▶ **Serpent**
- ▶ Twofish
- ▶ **SM4**
- ▶ RC6
- ▶ GOST
- ▶ ...

轻量级分组密码

- ▶ HIGHT
- ▶ **PRESENT**
- ▶ LBlock
- ▶ PRINCE
- ▶ **RECTANGLE**
- ▶ **SIMON**
- ▶ SKINNY
- ▶ ...

流密码 (Stream Cipher)

- ▶ RC4
- ▶ Salsa20
- ▶ ChaCha
- ▶ ...

工作模式 (Mode of Operation)

- ▶ ECB
- ▶ **CBC**
- ▶ CFB
- ▶ OFB
- ▶ **CTR**

密码杂凑函数 (Hash Function)

- ▶ MD5
- ▶ SHA1
- ▶ SHA2
- ▶ SHA3
- ▶ BLAKE2
- ▶ Grøstl
- ▶ JH
- ▶ SM3
- ▶ ...

消息认证码 (Message Authentication Code)

- ▶ CBC-MAC
- ▶ **HMAC**
- ▶ OMAC
- ▶ **Poly1305**
- ▶ DAA
- ▶ ...

认证加密 (Authenticated Encryption)

- ▶ CCM
- ▶ EAX
- ▶ **GCM**
- ▶ OCB
- ▶ ...

Caesar Candidates

- ▶ ACORN
- ▶ Deoxys
- ▶ PRIMATES
- ▶ SHELL
- ▶ ...

密钥交换算法 (Key Exchange)

- ▶ Diffie–Hellman 密钥交换，简称 DH
- ▶ 基于非对称密码算法
 - ▶ Elliptic curve Diffie–Hellman (ECDH 或者 ECDHE)，基于 ECC
- ▶ ...

公钥加密 (Public-Key Encryption)

- ▶ RSA
- ▶ ECC
- ▶ ...

数字签名 (Digital Signature Algorithm)

数字签名都是通过非对称密码算法实现。

- ▶ RSA
- ▶ Elliptic Curve Digital Signature Algorithm (ECDSA)，基于 ECC
- ▶ Edwards-curve Digital Signature Algorithm (EdDSA)
- ▶ ...