CyBOK

The Cyber Security Body of Knowledge

Cryptography Knowledge Tree

COPYRIGHT

CHANGE LOG

Version date	Version number	Changes made
July 2021	1.0.1	Version updated in line with KA version 1.0.1
October 2019	1.0	

```
schemes ──── AES
        ──── RSA
        ──── DES
        ──── PKCS
        ──── DSA
        ──── Kerberos
        ──── TLS

symmetric primitives ──── block ciphers ──── Feistel networks
                     ──── stream ciphers
                     ──── hash functions ──── Merkel-Damgård construction
                                         ──── sponge constructions

symmetric cryptography ──── symmetric encryption and authentication ──── modes of operation ──── ECB
                                                                                             ──── CBC
                                                                                             ──── OFB
                                                                                             ──── CFB
                                                                                             ──── CTR
                                                                                             ──── AEAD
                                                                    ──── message authentication codes
                                                                    ──── extendable output function
                                                                    ──── key derivation functions

public key cryptography ──── public key encryption ──── key encapsulation mechanisms
                                                   ──── constructions based on RSA ──── RSA-OAEP
                                                                                    ──── RSA-KEM
                                                   ──── data encryption mechanisms
                                                   ──── constructions based on elliptic curves ──── ECIES
                                                   ──── lattice-based constructions
                        ──── public key signatures ──── full domain hash
                                                   ──── probabilistic signature schemes
                                                   ──── Schnorr signatures

cryptographic security models ──── basic security definitions ──── security games ──── random oracle model
                                                              ──── one-way
                                                              ──── passive attack
                                                              ──── indistinguishability
                                                              ──── chosen plaintext attacks
                                                              ──── chosen ciphertext attack
                                                              ──── universal forgery
                                                              ──── chosen message attack
                              ──── hard problems ──── pseudo-random functions
                                                 ──── pseudo-random permutations
                                                 ──── discrete logarithm problem
                                                 ──── Diffie-Hellman problem
                                                 ──── shortest vector problem
                                                 ──── closest vector problem ──── post-quantum cryptography
                              ──── setup assumptions ──── PKI
                                                     ──── common reference strings
                                                     ──── good random number generation
                              ──── simulation of cryptographic operations
                              ──── universal composability

information-theoretically secure constructions ──── one-time pad
                                               ──── secret sharing

standard protocols ──── authentication protocols ──── encryption-based protocols
                                                  ──── message authentication-based protocols
                                                  ──── zero-knowledge-based protocols
                   ──── key agreement protocols ──── key confirmation
                                                ──── forward secrecy
                                                ──── unknown key share security
                                                ──── key transport
                                                ──── Diffie-Hellman key agreement
                                                ──── station-to-station protocol

advanced protocols ──── oblivious transfer
                   ──── zero-knowledge
                   ──── Σ-protocols
                   ──── secure multi-party computation

public-key schemes with special properties ──── group signatures
                                           ──── ring signatures
                                           ──── blind signatures
                                           ──── identity-based encryption
                                           ──── linearly homomorphic encryption
                                           ──── fully homomorphic encryption
```