공개키 암호

국민대학교 정보보안암호수학과

김동찬

https://sites.google.com/kookmin.ac.kr/dongchankim

수업 개요

- https://sites.google.com/kookmin.ac.kr/dc-2023-pkc

암호 알고리듬

TDES
AES
LEA
SEED
ARIA
HIGHT
PRESENT
CLEFIA
CAMELLIA

ECB
CBC
OFB
CFB
CTR
CTS

GCM
CCM
OCB

SHA-1/2/3
MD5
LSH

HMAC
CMAC
CBC-MAC

CTR-DRBG
HASH-DRBG
HMAC-DRBG

HMAC- KBKDF
CMAC-KBKDF
PBKDF2

IFP
DLP
SVP / CVP
LWEP
SISP
SDP

RSAES
ECIES

DH / ECDH

CRYSTALS-KYBER
SABER
NTRU
Classic McEliece

DSA / ECDSA
EdDSA
RSA-PSS

CRYSTALS-DILITHIUM
FALCON
SPINCS+

Multi-Party Computation

Zero Knowledge

(Fully) Homomorphic Encryption

Secret Sharing

Format-Preserving Encryption

ID-based Encryption

Tweakable Block Cipher

암호 알고리듬

TDES

AES

LEA

SEED

ARIA

HIGHT

PRESENT

CLEFIA

CAMELLIA

SHA-1/2/3

MD5

LSH

IFP

DLP

SVP / CVP

LWEP

SISP

SDP

Primitives

암호 알고리듬

TDES
AES
LEA
SEED
ARIA
HIGHT
PRESENT
CLEFIA
CAMELLIA

ECB
CBC
OFB
CFB
CTR
CTS

GCM
CCM
OCB

SHA-1/2/3
MD5
LSH

HMAC
CMAC
CBC-MAC

CTR-DRBG
HASH-DRBG
HMAC-DRBG

HMAC- KBKDF
CMAC-KBKDF
PBKDF2

IFP
DLP
SVP / CVP
LWEP
SISP
SDP

RSAES
ECIES

DH / ECDH

CRYSTALS-KYBER
SABER
NTRU
Classic McEliece

DSA / ECDSA
EdDSA
RSA-PSS

CRYSTALS-DILITHIUM
FALCON
SPINCS+

Multi-Party Computation

Zero Knowledge

(Fully) Homomorphic Encryption

Secret Sharing

Format-Preserving Encryption

ID-based Encryption

Tweakable Block Cipher

암호 알고리듬

Schemes

ECB

CBC

OFB

CFB

CTR

CTS

GCM

CCM

OCB

HMAC

CMAC

CBC-MAC

CTR-DRBG

HASH-DRBG

HMAC-DRBG

HMAC- KBKDF

CMAC-KBKDF

PBKDF2

RSAES

ECIES

DH / ECDH

CRYSTALS-KYBER

SABER

NTRU

Classic McEliece

DSA / ECDSA

EdDSA

RSA-PSS

CRYSTALS-DILITHIUM

FALCON

SPINCS+

암호 알고리듬

TDES
AES
LEA
SEED
ARIA
HIGHT
PRESENT
CLEFIA
CAMELLIA

ECB
CBC
OFB
CFB
CTR
CTS

GCM
CCM
OCB

SHA-1/2/3
MD5
LSH

HMAC
CMAC
CBC-MAC

CTR-DRBG
HASH-DRBG
HMAC-DRBG

HMAC- KBKDF
CMAC-KBKDF
PBKDF2

IFP
DLP
SVP / CVP
LWEP
SISP
SDP

RSAES
ECIES

DH / ECDH

CRYSTALS-KYBER
SABER
NTRU
Classic McEliece

DSA / ECDSA
EdDSA
RSA-PSS

CRYSTALS-DILITHIUM
FALCON
SPINCS+

Multi-Party Computation

Zero Knowledge

(Fully) Homomorphic Encryption

Secret Sharing

Format-Preserving Encryption

ID-based Encryption

Tweakable Block Cipher

암호 알고리듬

CRYSTALS-KYBER

SABER

NTRU

Classic McEliece

Post-Quantum (or Quantum-Safe) Cryptography

CRYSTALS-DILITHIUM

FALCON

SPINCS+