공개키암호

국민대학교 정보보안암호수학과 김동찬

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

수업 개요

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

FDL @ KMU 4 / 138

TDES AES	AES LEA SEED ARIA HIGHT PRESENT CLEFIA CM CCM OCB	SHA-1/2/3 MD5 <u>LSH</u>	IMAC- KBKDF CMAC-KBKDF PBKDF2		DH / ECDH CRYSTALS- KYBER SABER	Multi-Party Computation Zero Knowledge
SEED ARIA HIGHT PRESENT		HMAC CMAC CBC-MAC	IFP DLP SVP / CVP LWEP SISP		NTRU Classic McEliece DSA / ECDSA EdDSA RSA-PSS CRYSTALS- DILITHIUM FALCON SPINCS+	(Fully) Homomorphic Encryption Secret Sharing Format-Preserving Encryption ID-based Encryption Tweakable Block Cipher
CLEFIA CAMELLIA		CTR-DRBG HASH-DRBG HMAC-DRBG	SDP RSAES ECIES			

FDL @ KMU 5 / 138

TDES

AES

<u>LEA</u>

SEED

ARIA

HIGHT

PRESENT

CLEFIA

CAMELLIA

SHA-1/2/3

MD5

<u>LSH</u>

IFP

DLP

SVP / CVP

LWEP

SISP

SDP

Primitives

6 / 138

	ECB	SHA-1/2/3		IMAC- KBKDF CMAC-KBKDF			Multi-Party
TDES	CBC	MD5		PBKDF2			Computation
AES		<u>LSH</u>					Zero Knowledge
<u>LEA</u>	OFB CFB CTR			IFP			(Fully)
<u>SEED</u>		HMAC		DLP			Homomorphic Encryption
<u>ARIA</u>	CTS	CMAC		SVP / CVP		٠, ٨	Secret Sharing
<u>HIGHT</u>	CIS	CBC-MAC		LWEP	DSA / ECDS		
PRESENT				SISP	EdDSA	1	Format-Preserving Encryption
CLEFIA	GCM	CTR-DRBG		SDP	RSA-PSS		ID-based
CAMELLIA	CCM	HASH-DRBG					Encryption
	OCB	HMAC-DRBG	RSAES ECIES			Tweakable Block Cipher	

FDL @ KMU 7 / 138

Schemes

ECB

CBC

OFB

CFB

CTR

CTS

GCM

CCM

OCB

HMAC- KBKDF

CMAC-KBKDF

PBKDF2

DH / ECDH

CRYSTALS-

NTRU

Classic McEliece

DSA / ECDSA

EdDSA

RSA-PSS

CRYSTALS-

FALCON

SPINCS+

CTR-DRBG

HMAC

CMAC

CBC-MAC

HASH-DRBG

HMAC-DRBG

RSAES

ECIES

TDES AES ECB CBC	SHA-1/2/3 MD5 <u>LSH</u>	HMAC- KBKDF CMAC-KBKDF PBKDF2		Multi-Party Computation Zero Knowledge
LEA SEED ARIA HIGHT PRESENT CLEFIA CAMELLIA OFB CFB CTR CTR CTS GCM CCM OCB	HMAC CMAC CBC-MAC CTR-DRBG HASH-DRBG HMAC-DRBG	IFP DLP SVP / CVP LWEP SISP SDP RSAES ECIES	NTRU Classic McEliece DSA / ECDSA EdDSA RSA-PSS CRYSTALS- DILITHIUM FALCON	(Fully) Homomorphic Encryption Secret Sharing Format-Preserving Encryption ID-based Encryption Tweakable Block Cipher

FDL @ KMU 9 / 138

CRYSTALS-KYBER
SABER
NTRU
Classic McEliece

Post-Quantum (or Quantum-Safe) Cryptography

CRYSTALS-DILITHIUM
FALCON
SPINCS+

FDL @ KMU 10 / 138