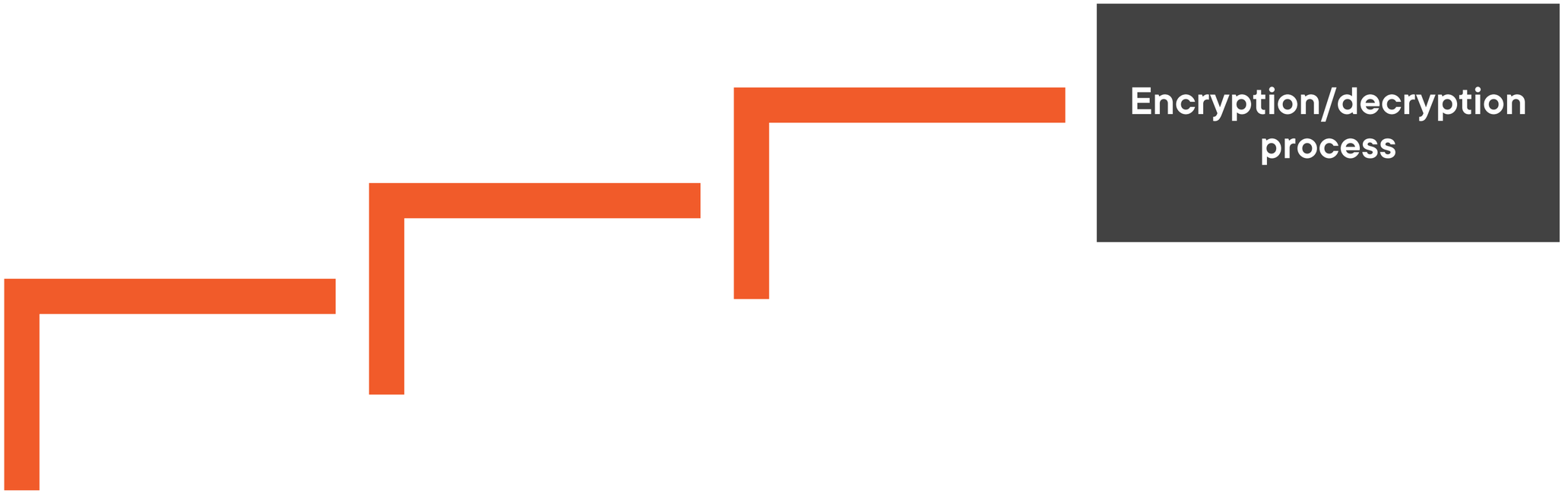
Examining Encryption Algorithms

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Types of Ciphers

Ciphers



Algorithms

A set of rules or instructions used to solve complex problems

add b-roll

maybe this one

Asset ID: SBV-346572537 or pick something better-

Cypher Categories

Classical

Modern

Substitution

Classical

MY VOICE IS MY PASSWORD = DB XGOET OL DB HALLCGKR

M=D, Y=B

Transposition

Classical

MY VOICE IS MY PASSWORD =

Rail fence cipher
Key = 3

M				I				S				A				O		
	Y		O		C		I		M		P		S		W		R	
		V				E				Y				S				D

Route Cipher

Classical

MY VOICE IS MY PASSWORD =

Key = Route

M	O	E	M	A	W	D
Y	I	I	Y	S	O	X
V	C	S	P	S	R	T

Cypher Categories

Classical

Modern

Modern Ciphers

Difficult to crack

Provide authenticity, security, and they protect the integrity of the sender

Are both symmetric and asymmetric

Block cipher: the algorithm operates in groups of bits or a block of a fixed size

Stream cipher: a symmetric key cipher where the plaintext digit is combined with a pseudorandom cipher digit stream

Types of Algorithms

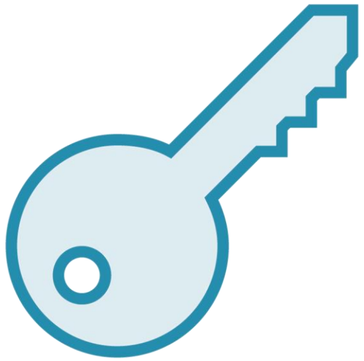
DES	3DES	AES
RC4	RC5	RC6

Algorithms

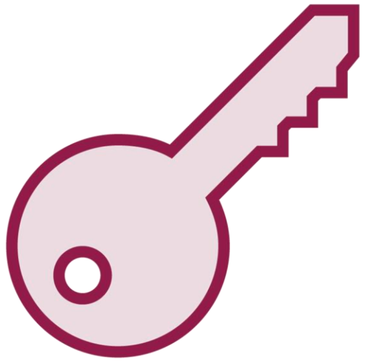
Data Encryption Standard (DES)

DES utilizes a 64-bit block and a 56-bit key for encryption and decryption

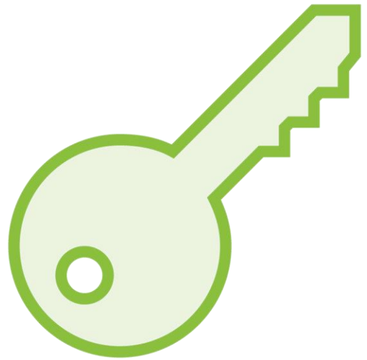
3DES was created to cover DES vulnerabilities



K1



K2



K3

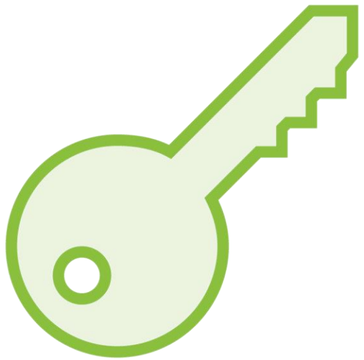
Option 1

All three keys are independent

Data Encryption Standard (DES)

DES utilizes a 64-bit block and a 56-bit key for encryption and decryption

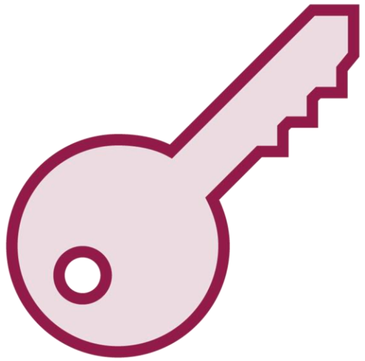
3DES was created to cover DES vulnerabilities



K1

Option 1

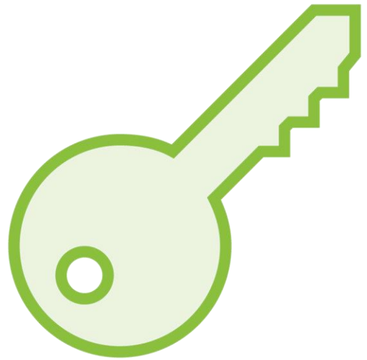
All three keys are independent



K2

Option 2

K1 and K3 are identical

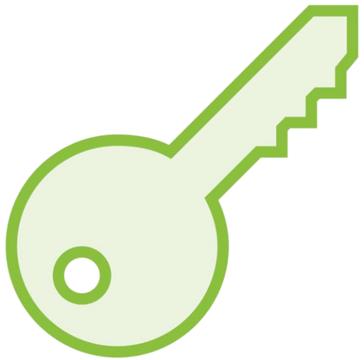


K3

Data Encryption Standard (DES)

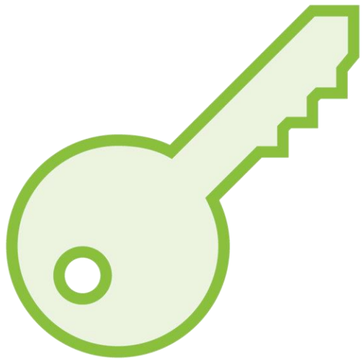
DES utilizes a 64-bit block and a 56-bit key for encryption and decryption

3DES was created to cover DES vulnerabilities



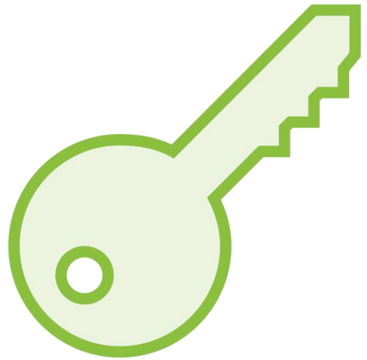
K1

Option 1
All three keys are independent



K2

Option 2
K1 and K3 are identical



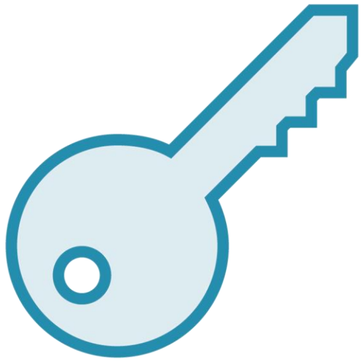
K3

Option 3
All keys are the same

Data Encryption Standard (DES)

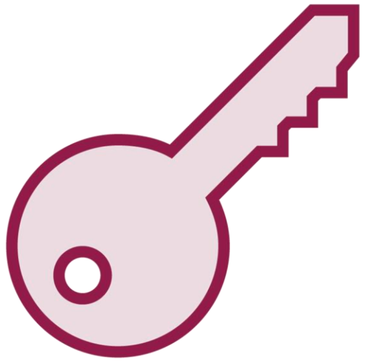
DES utilizes a 64-bit block and a 56-bit key for encryption and decryption

3DES was created to cover DES vulnerabilities



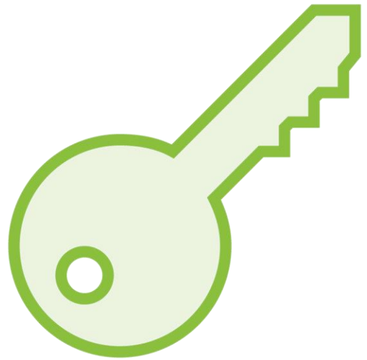
K1

Option 1
All three keys are independent



K2

Option 2
K1 and K3 are identical

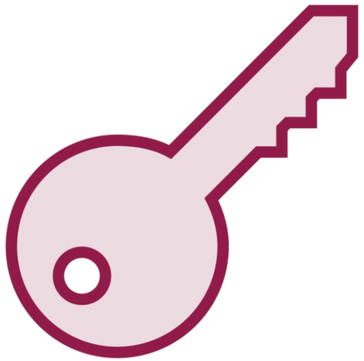


K3

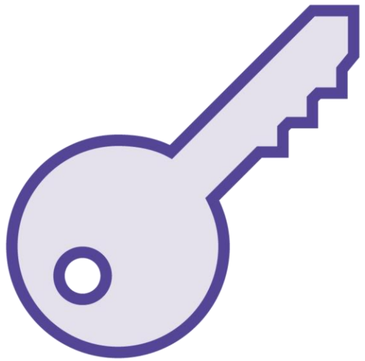
Option 3
All keys are the same

Advanced Encryption Standard (AES)

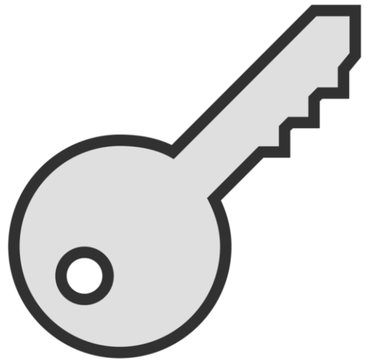
A symmetric-key algorithm created with the help of the National Institute of Standards and Technology (NIST)



AES128



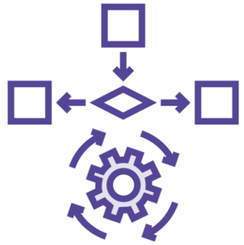
AES192



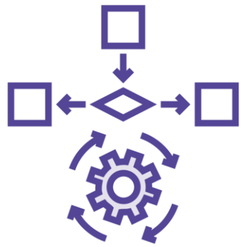
AES256

Works efficiently in both software and hardware and works simultaneously at multiple network layers

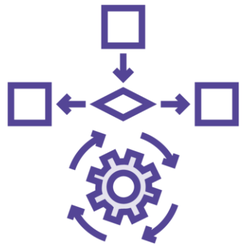
Rivest Ciphers: RC4, RC5, RC6 Algorithms



RC4 is a variable key size symmetric key stream cipher with byte-oriented operations

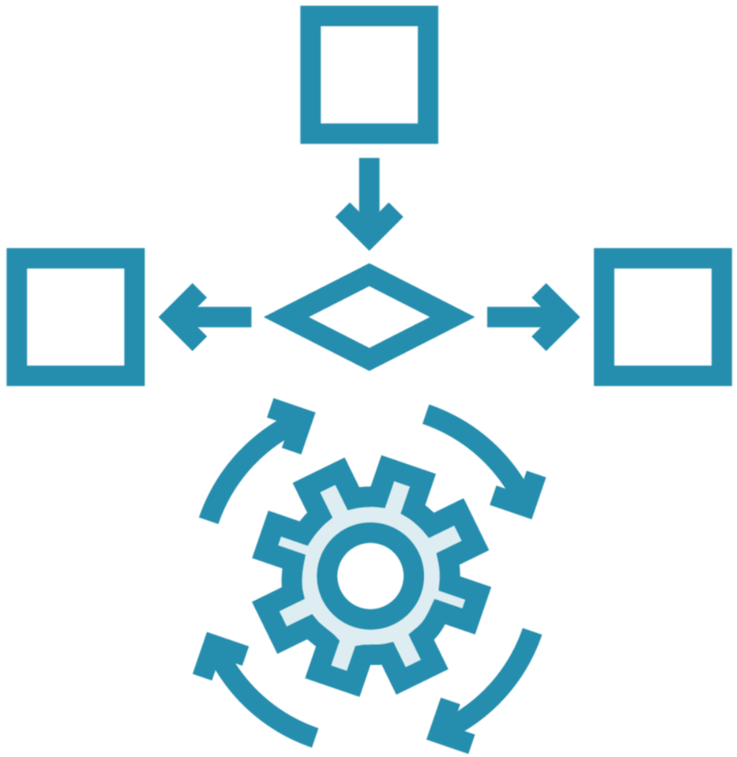


RC5 is parameterized with variable block and key sizes and a variable number of rounds



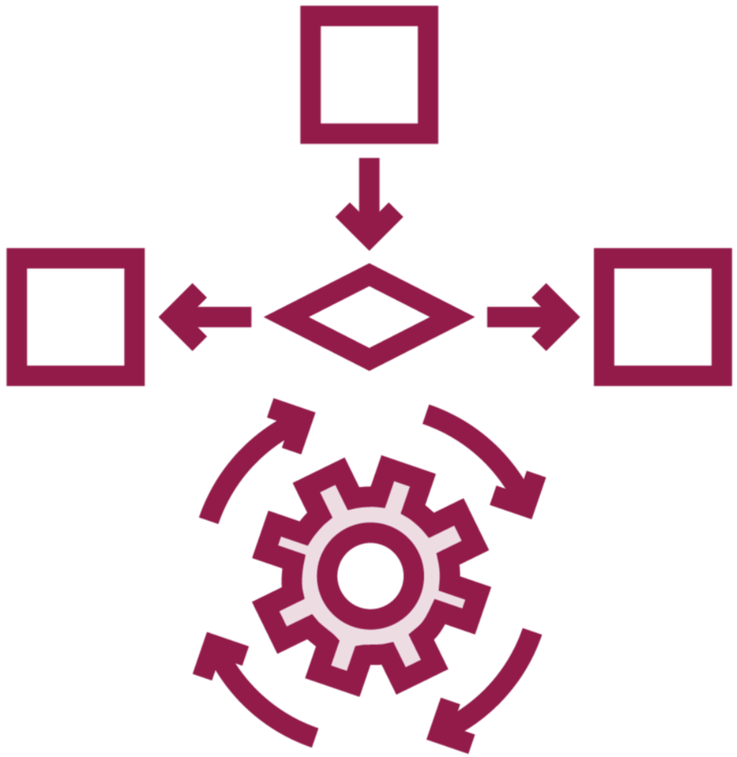
RC6 is a symmetric key block cipher that uses integer multiplication and four 4-bit working registers

Blowfish Algorithm



- Developed in 1993
- Utilizes a 64-bit block and a variable key
- Designed to replace DES and 3DES
- Faster encryption and decryption than AES

Twofish Algorithm

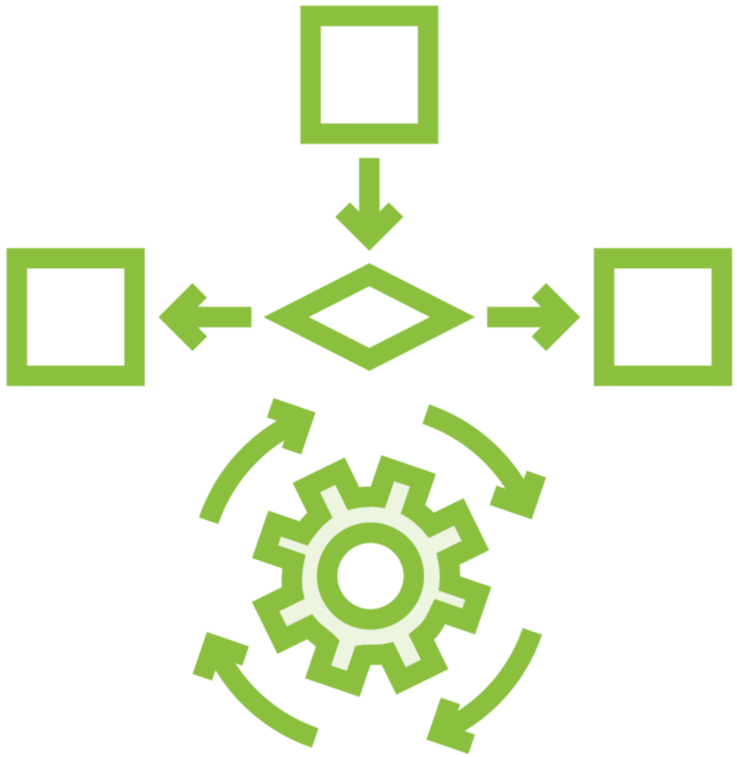


Introduced in 1998

Utilizes a 128-bit block cipher

Uses a single key and supports 256, 192, and 128-bit key sizes

Threefish Algorithm



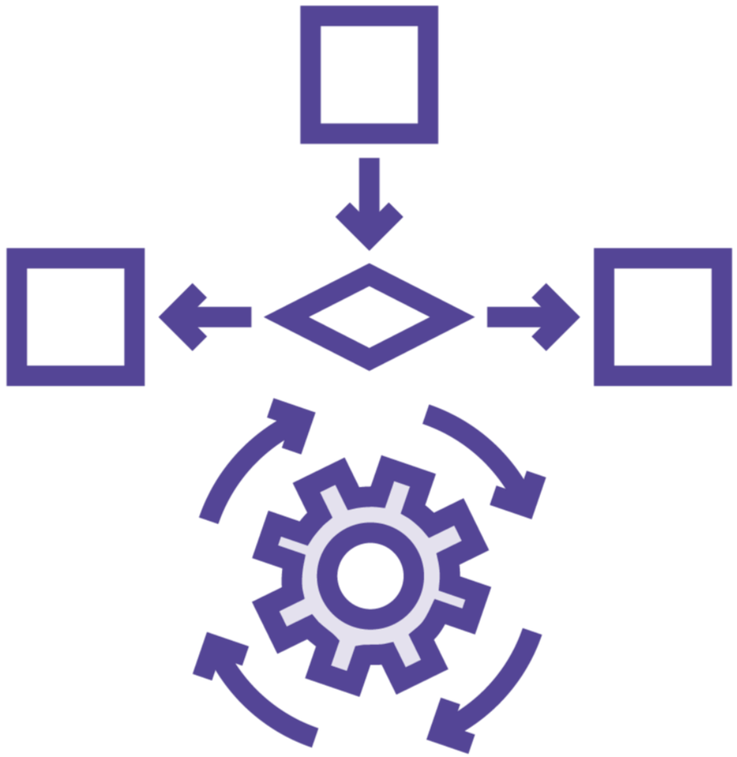
Developed in 2008

12-round Feistel network cipher

Utilizes a block size of 128 bits and a key length of 256 bits

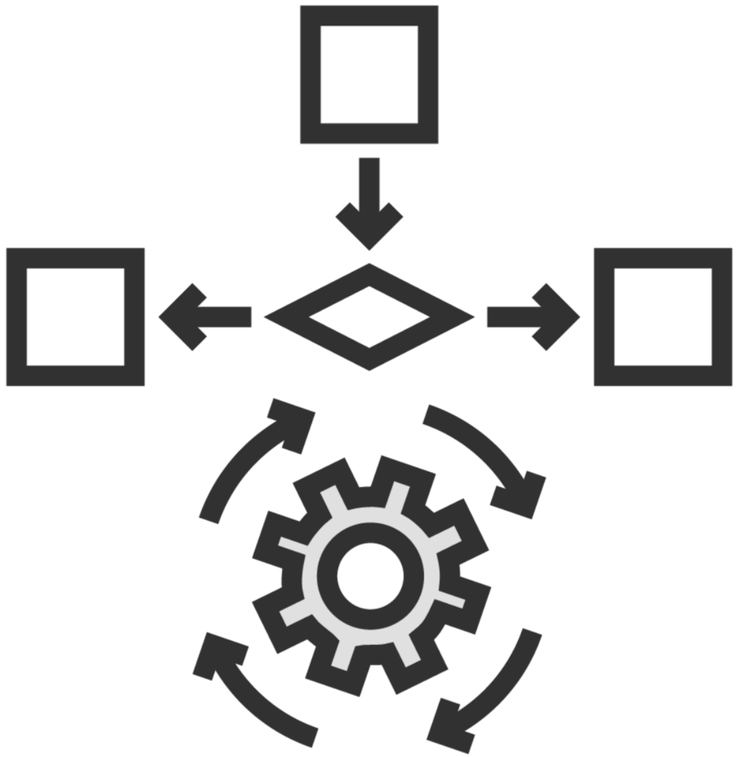
Fast, secure, and has a high resistance to attack

Serpent



- Symmetric-key block cipher
- Utilizes a 128-bit symmetric block cipher
- Used in software and hardware programs
- Involves 32 rounds of computational operations that include substitution and permutation operations

Tiny Encryption Algorithm (TEA)

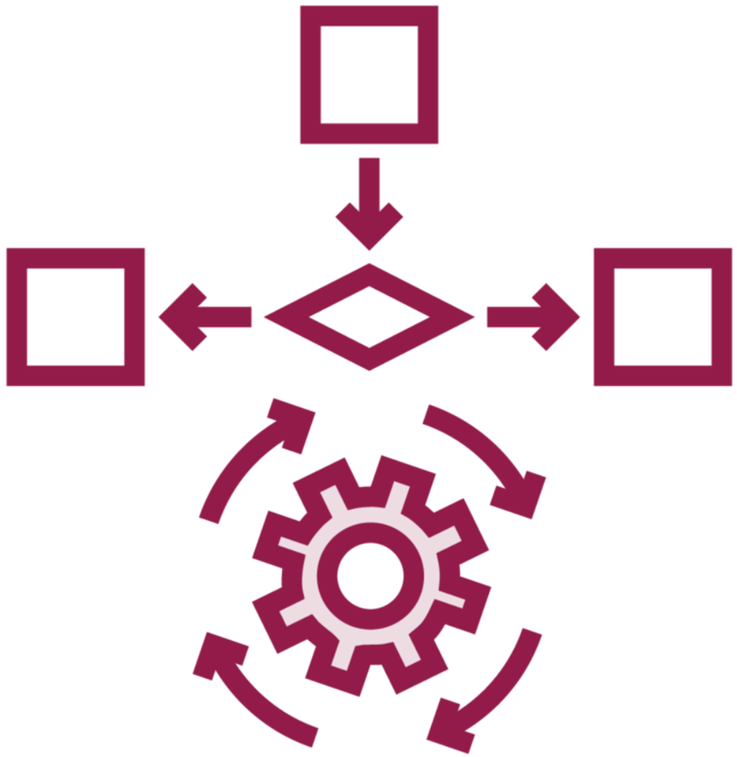


Symmetric block cipher with a block size of 64 bits and a key length of 128 bits

Most widely used encryption algorithms

Uses four tables with 256 entries each

Camellia

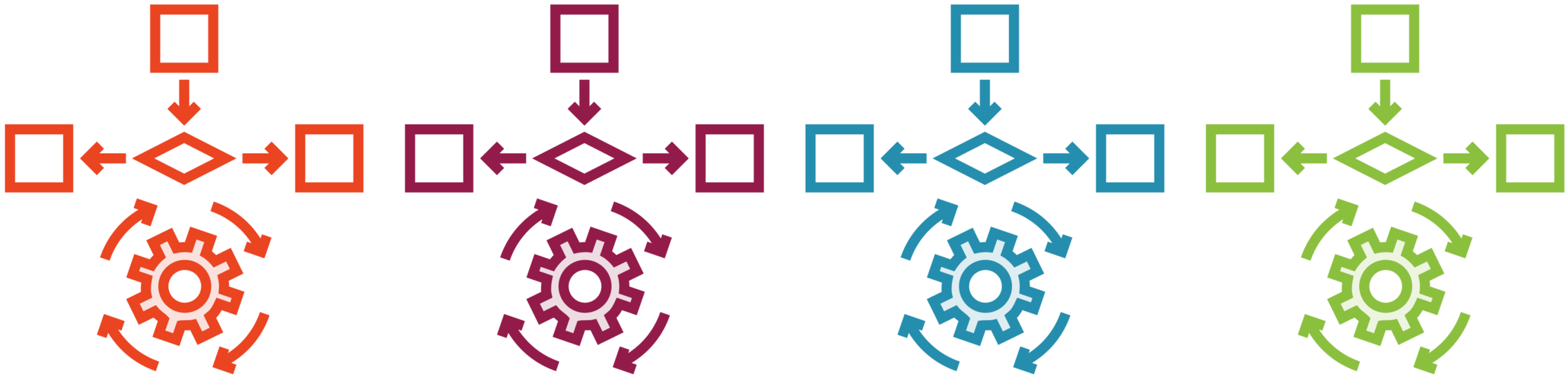


A symmetric-key block cipher

Uses four 8x8-bit S-boxes that perform affine transformations

Associated with the Transport Layer Security (TL5) protocol

Processing skills are equivalent to those of AES



Choose the right one for the job

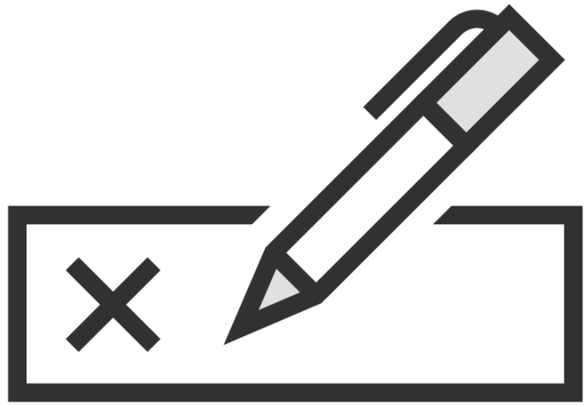
Common Algorithms

Digital Signature Algorithm (DSA)

Creates a 320-bit digital signature with 512-1024-bit security

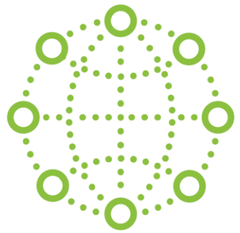
Utilizes both private and public keys

Employs a signature generation and signature verification process



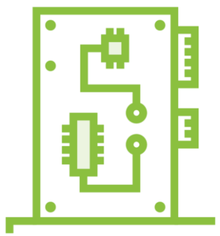
Federal Information Processing Standard for digital signatures

Rivest Shamir Adleman (RSA)



Employed for internet encryption and authentication

Applied in popular operating systems



Utilized in networking cards, smart cards and in hardware-secured phones

Public-key cryptosystem

How RSA Works

Two large prime numbers are taken (a and b), then the product of a and b is determined (c=ab, where c is called the modulus)

RSA chooses e (less than c) and relatively prime to (a-1) (b-1)
e and (a-1) (b-1) have no common factor except 1

RSA chooses f (ef-1) is divisible by (a-1) (b-1)

The values e and f are the public and private exponents

The public key is the pair (c,e) and the private key is the pair (c,f)

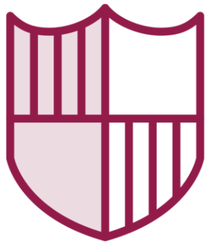
It is difficult to obtain the private key (c,f) from the public key (c,e) unless someone can factor c into a and b, then that person can decipher the private key (c,f)

Diffie-Hellman

Allows two parties to establish a shared secret key over an insecure channel

Does not provide key exchange authentication and is vulnerable to a variety of cryptographic assaults

YAK



Provides mutual authentication and integrity protection

Resistant to man-in-the-middle attacks

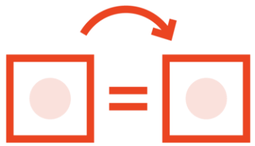
Utilizes public key pairs and requires PKI to distribute authentic public keys

Message Digest Algorithms

Message Digest

Referred to as a hash valued

Produces a unique fingerprint or hash value of the data

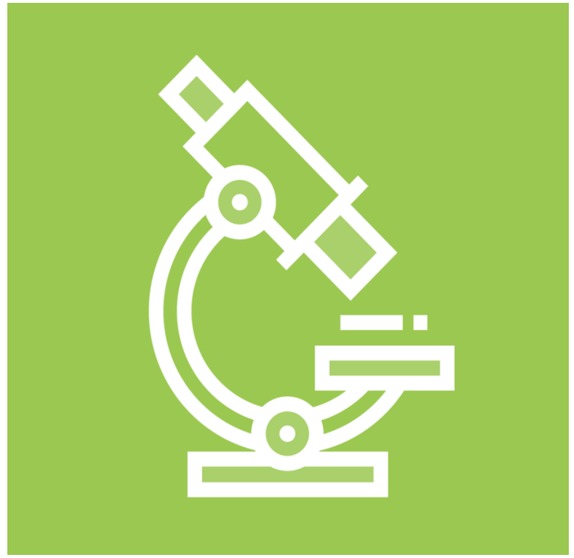


Enables authentication to ensure the data has not been altered

Message Direct Algorithms

MD2

MD4



MD6

Compresses data securely

Resulting message digest always has a size of 128 bits

MD5

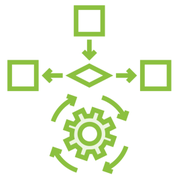
One-way hashing algorithm

Used in digital signature applications

Is not collision resistant

MD6, SHA-2, and SHA-3

SHA-1



Produces a 160-bit hash value that is then turned into hexadecimal

PGP (Pretty Good Privacy)

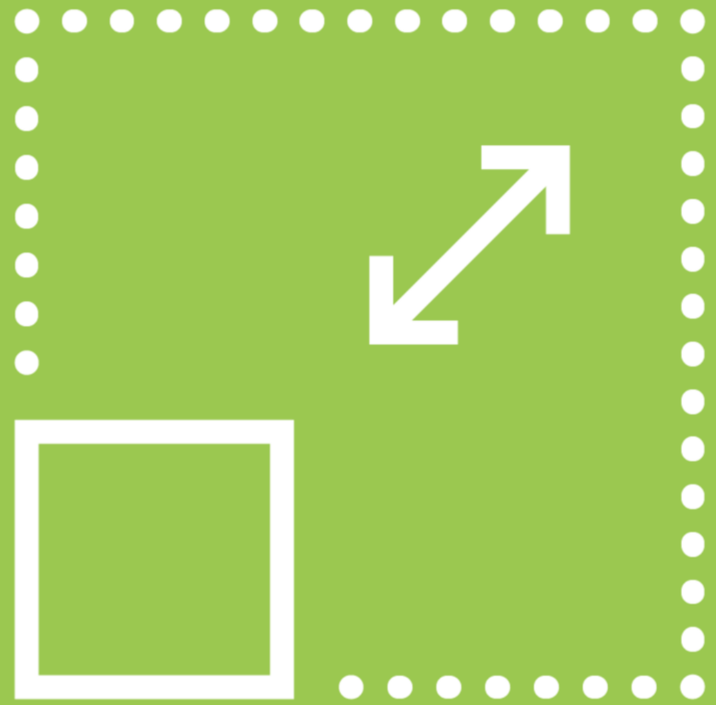
TLS (Transport Layer Security)

SSH (Secure Shell)

SSL (Secure Sockets Layer)

SHA-2

SHA-2



SHA-3

Data is absorbed and the result is squeezed out

Message blocks are XORed into initial bits of state or a subset

That subset is transformed using a permutation function

Challenge Handshake Authentication Protocol (CHAP)

Authentication mechanism used with PPP (Point to Point Protocol) and a three-way handshake

Utilizes a shared key

Extensible Authentication Protocol (EAP)

Designed for point-to-point communications

Supports different authentication mechanisms

Hardware Based Encryption

Hardware Based Encryption

Use computer hardware for assisting or replacing the software when data encryption process is taking place.

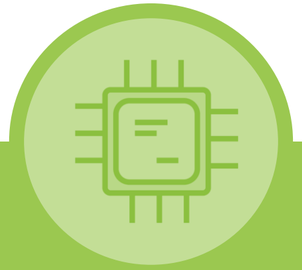
Capable of storing encryption keys and sensitive information in secured areas of RAM or other nonvolatile storage devices.

Hardware Encryption Devices

Trusted Platform Module (TPM)

- **Provides authentication and platform integrity**
- **Provides full disk encryption capabilities**
- **Provides software license protection**

Hardware Encryption Devices



Hardware Security Module (HSM)

- **Manages, generates, and securely stores keys**
- **Offers enhanced encryption computation**
- **Used in SafeNet Luna Network HSM, nSheild, Cloud HSM, and Cryptosec Dekaton**

Hardware Encryption Devices

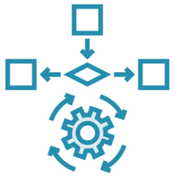
- **A feature for USB storage devices**
- **Protects against malware distribution over USB**
- **Used in Crypto USB, Kingston Ironkey D300S, and diskAshur Pro 500GB**

Hardware Encryption Devices

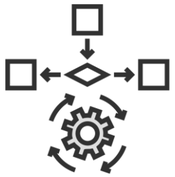
- **Encrypts data stored in hardware**
- **Require TPM or an HSM**
- **Used in Military-grade AES and DiskCypher AES SATA**

Learning Check

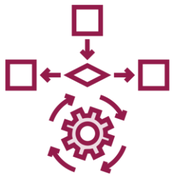
Learning Check



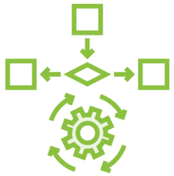
Algorithm



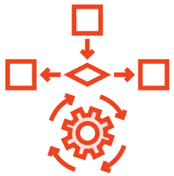
K1



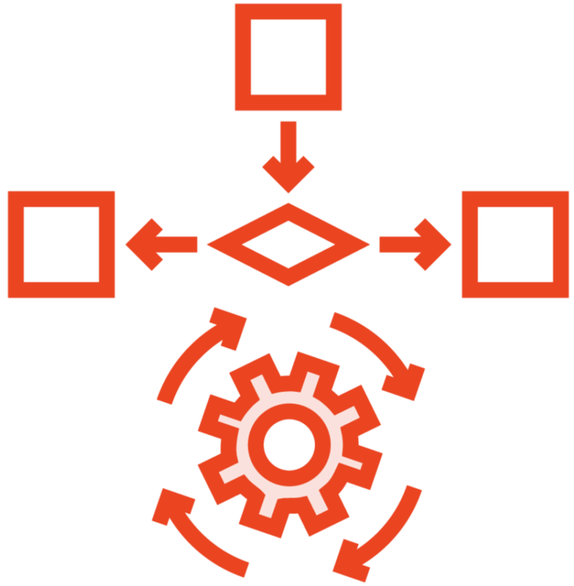
AES



Threefish



MD5



Up Next:
Investigating Cryptography Tools