Symmetric Encryption

Stephen Haunts

@stephenhaunts | www.stephenhaunts.com

What We Have Covered so Far?

Secure Random Number Generation

Hashing of Data

Secure Password Storage

Overview

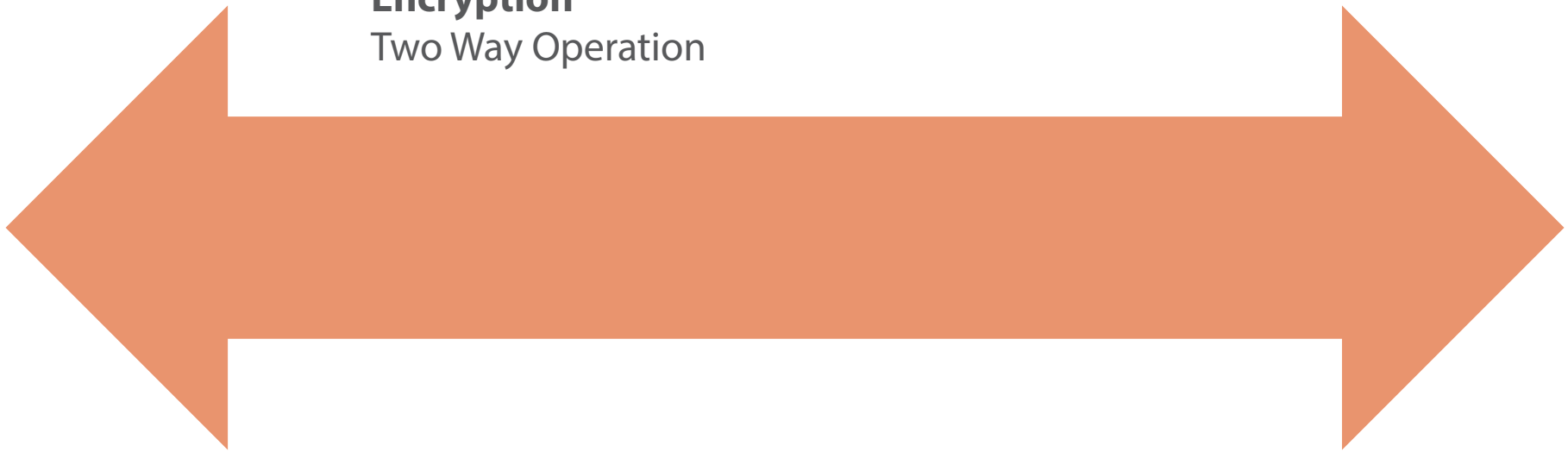
- What is symmetric encryption?
- The history of DES and Triple DES
- How does DES and Triple DES work?
- The history of AES
- How does AES work?

Overview

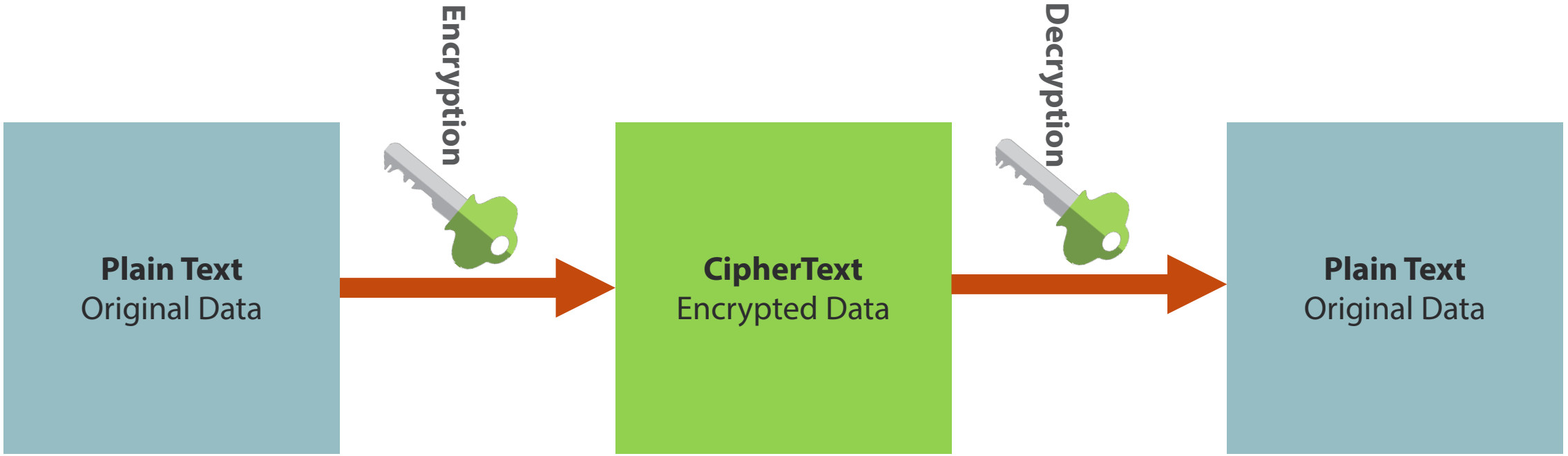
- How secure is AES against brute force attacks?
- Using the .NET Framework Libraries
- Code demonstration for DES, Triple DES and AES

What Is Symmetric Encryption?

Encryption
Two Way Operation



What Is Symmetric Encryption?



Symmetric Encryption Advantages

- Extremely secure
- Relatively fast

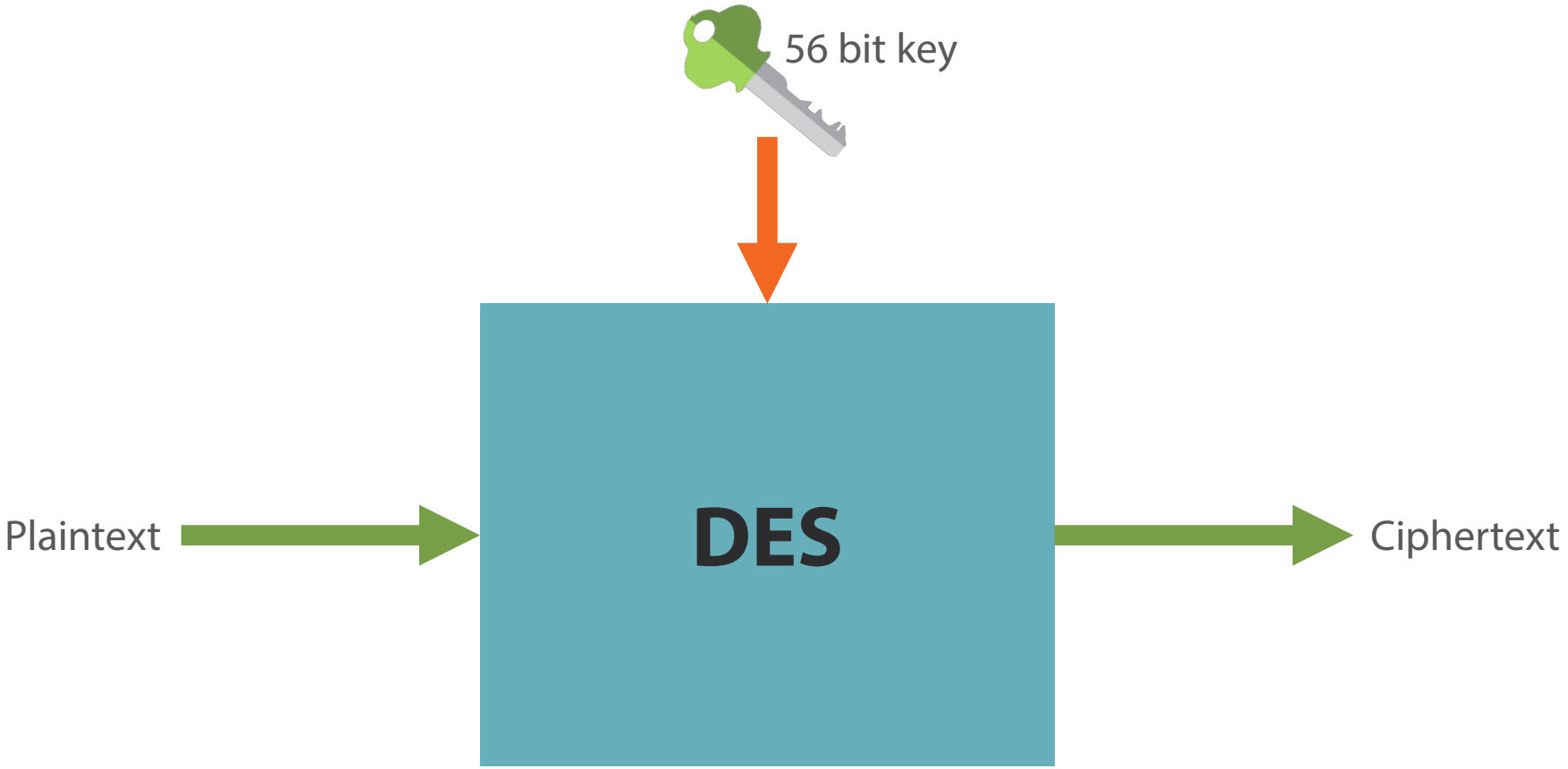
Symmetric Encryption Advantages

- Key sharing
- More damage if compromised

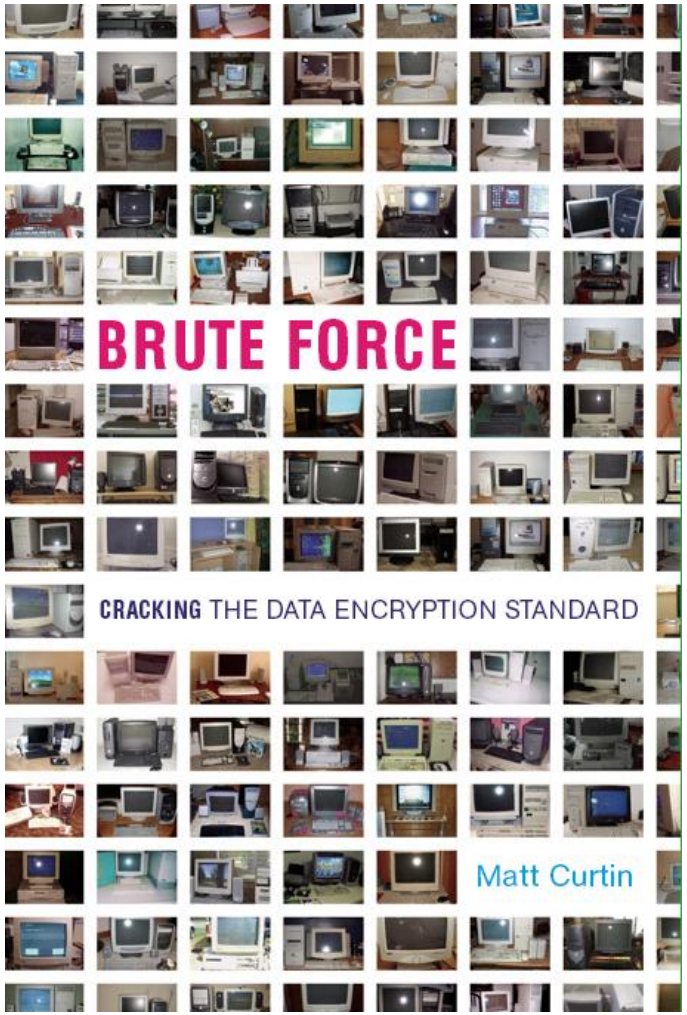
The History of DES and Triple DES?

- Data Encryption Standard (DES) was developed in early 1970's at IBM
- Submitted to the National Bureau of Standards for approval
- Approved at Federal Information Processing Standard 46 (FIPS 46)
- Consultation with the National Security Agency (NSA)
- Provide security for the unclassified electronic data for the US government

The History of DES and Triple DES?



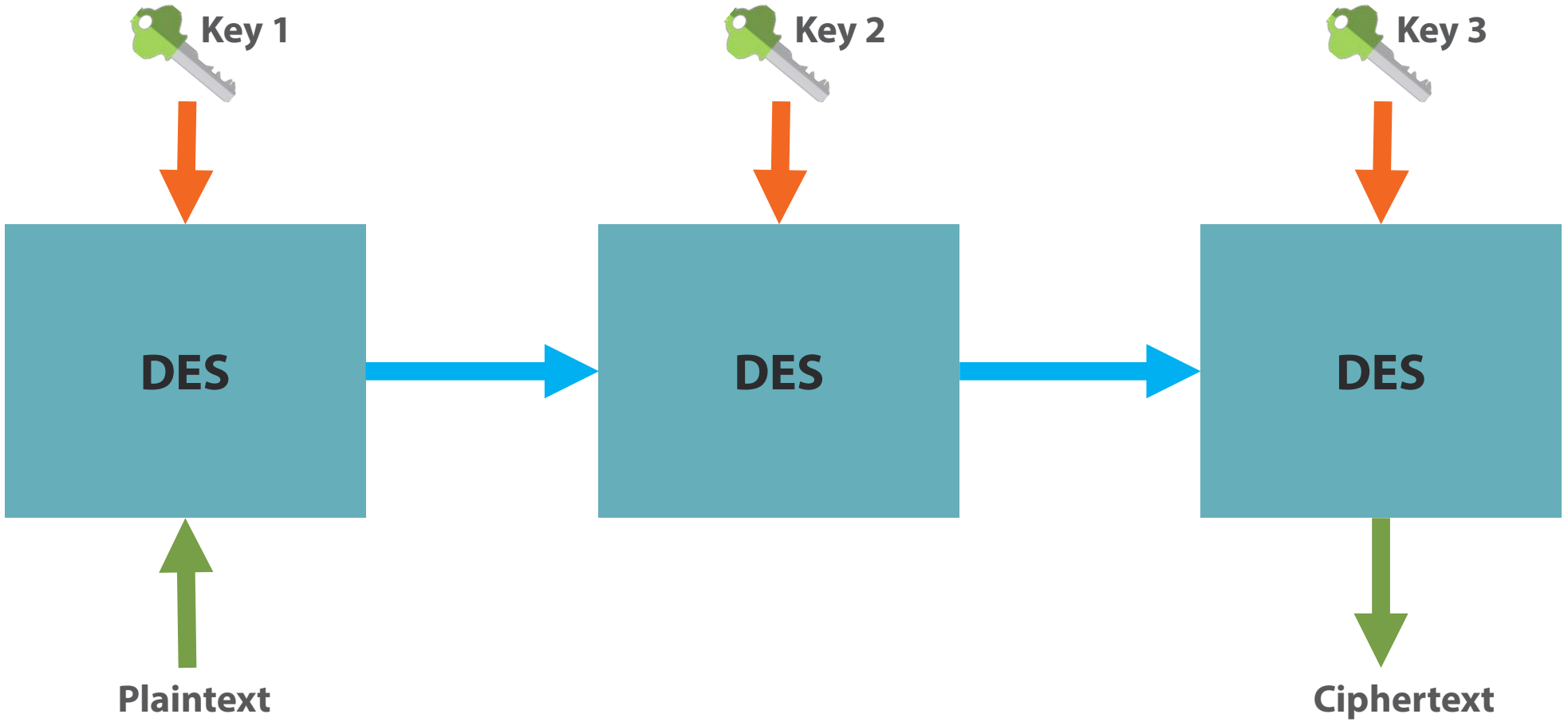
The History of DES and Triple DES?



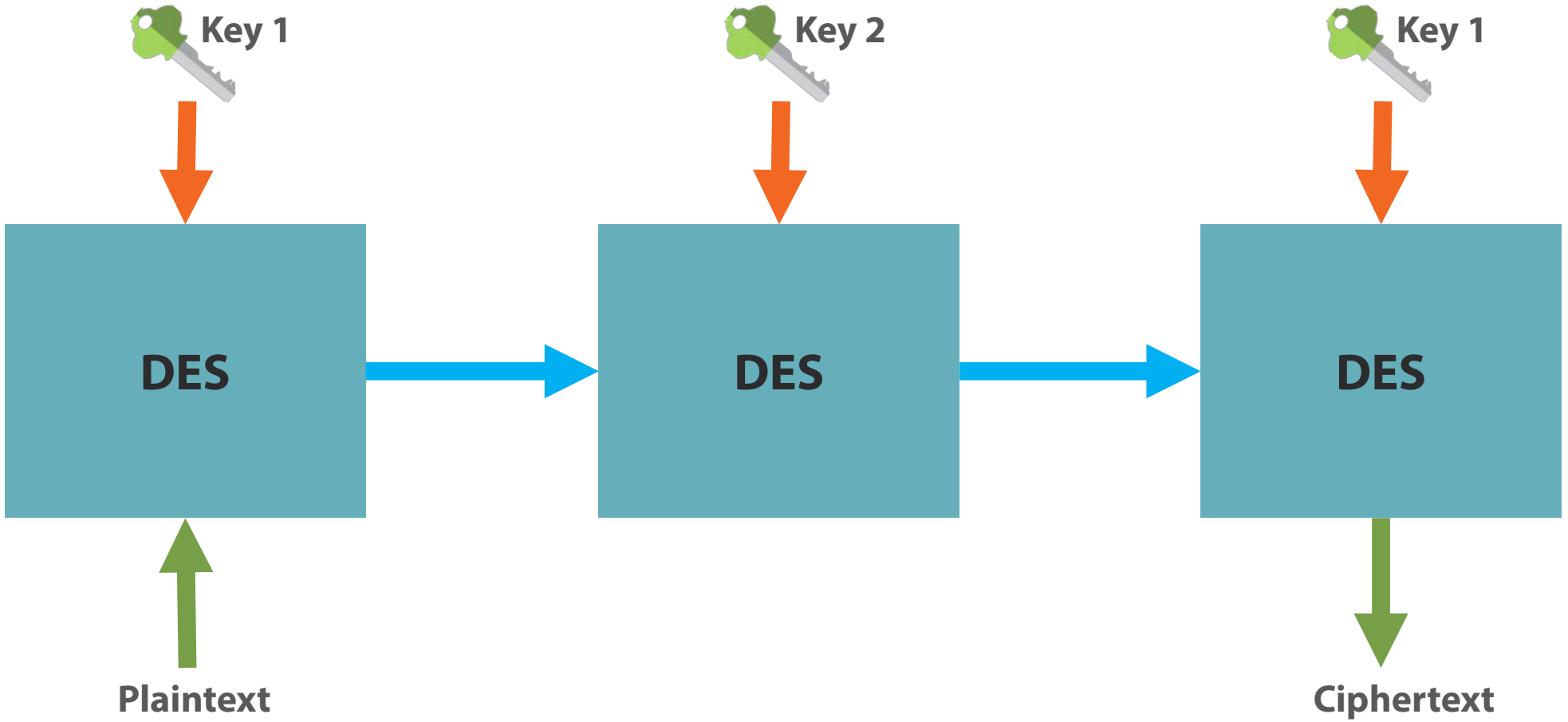
The History of DES and Triple DES?

- A new variant designed called Triple DES
- A simple way to increase key size without redesigning a new cipher
- Many former DES users now use Triple DES
- Triple DES involved applying DES three times with 2 or 3 different keys
- Triple DES was regarded as adequately secure, although it is quite slow

The History of DES and Triple DES?



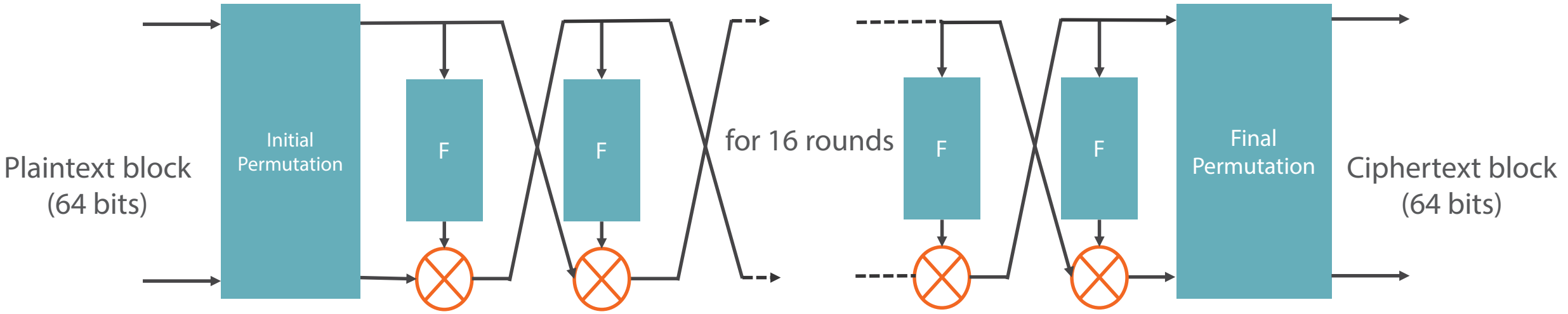
The History of DES and Triple DES?



How Does DES and Triple DES Work?

- DES is a block cipher that transforms plaintext into ciphertext
- DES uses a block size of 64 bits
- Uses a 64 bit key but only 56 bits are used by the algorithm
- Supports different modes of operation

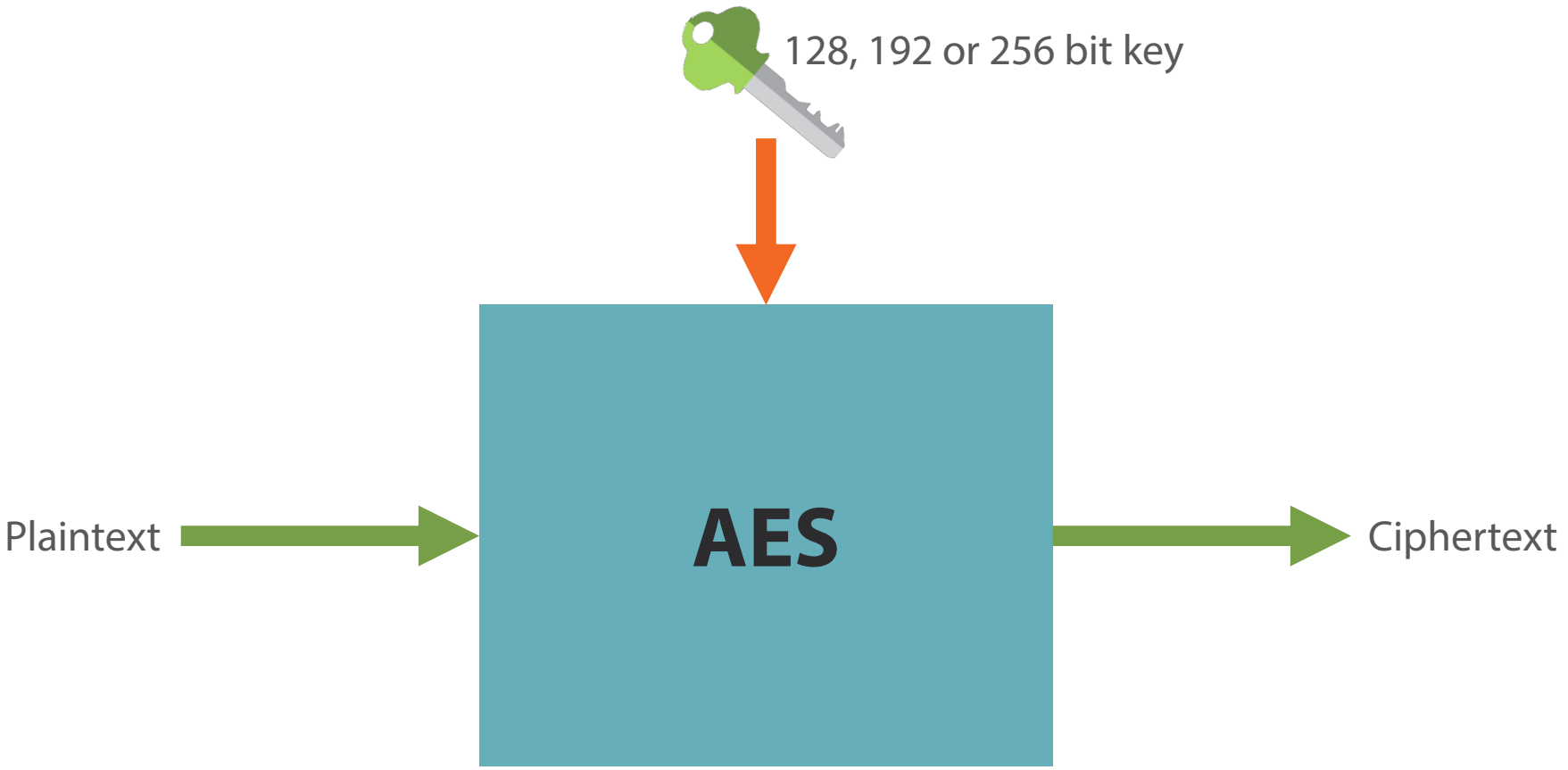
How Does DES and Triple DES Work?



The History of AES

- Advanced Encryption Standard adopted by NIST in 2001
- Selected by a contest to replace the Data Encryption Standard (DES)
- AES is based on the Rijndael cipher
- Rijndael is a family of ciphers with different key and block sizes

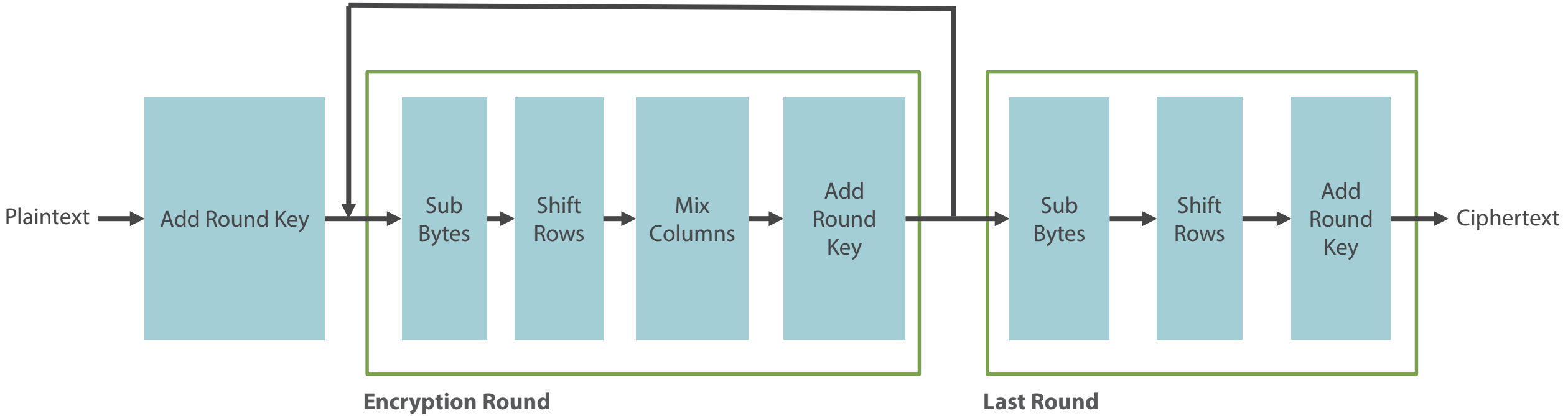
The History of AES



How Does AES Work?

- Unlike DES, AES does not use a Feistel network
- Uses 128 bit block size and 128, 192 or 256 bit keys
- Based on a design known as a substitution – permutation network
  - S-Box performs substitutions
  - P-Box performs bit shuffling to transpose bits across S-Box inputs

How Does AES Work?



How Does AES Work?

- AES key lengths are 128, 192 or 256 bits
- Every key is expanded so a separate sub-key can be utilized for every round
- The Number of rounds of AES generally depends on the length of the key

How Secure Is AES Against Brute Force Attack?

- There is a lot of trust that AES is secure and keys can not be broken
- Longer keys are exponentially more difficult to crack than shorter ones
- Brute force attack involves checking all possible key combinations until the correct key

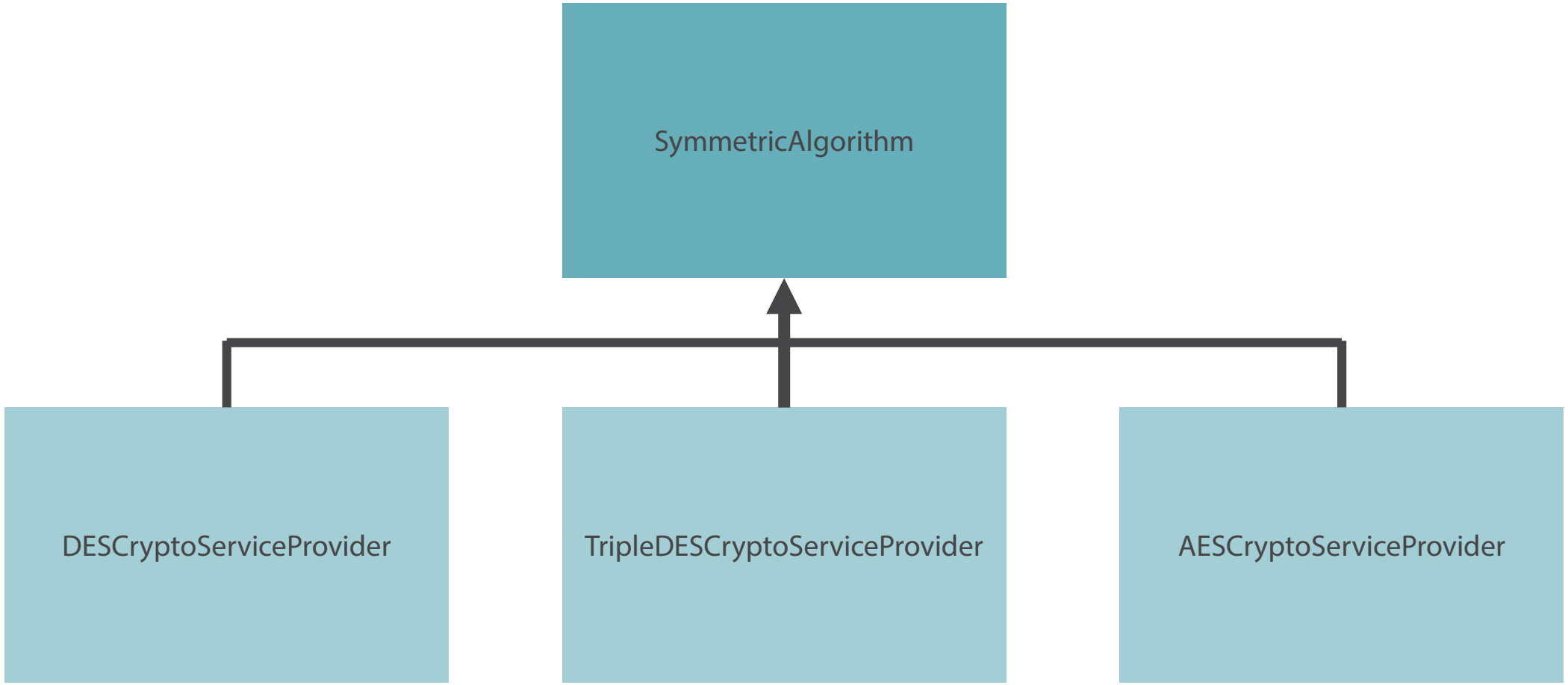
How Secure Is AES Against Brute Force Attack?

Key Size	Possible Combinations
1 bit	2
2 bit	4
4 bit	16
8 bit	256
16 bit	65536
32 bit	4.2×10^{9}
56 bit (DES)	**7.2×10^{16}**
64 bit	1.8×10^{19}
128 bit (AES)	**3.4×10^{38}**
192 bit (AES)	**6.2×10^{57}**
256 bit (AES)	**1.1×10^{77}**

How Secure Is AES Against Brute Force Attack?

Key Size	Time to Crack
56 bit	399 seconds
128 bit	1.02×10^{18} years
192 bit	1.87×10^{37} years
256 bit	3.31×10^{56} years

Using the .NET Framework Libraries



Using the .NET Framework Libraries

Encryption Mode

- Cipher block chaining (CBC)
- Ciphertext feedback (CFB)
- Ciphertext stealing (CTS)
- Electronic codebook (ECB)
- Output feedback (OFB)

SymmetricAlgorithm

CipherMode Mode

PaddingMode Padding

byte[] Key

byte[] IV

Using the .NET Framework Libraries

Padding

- ANSI X923
- ISO 10126
- None
- PKCS7
- Zeros

SymmetricAlgorithm

CipherMode Mode

PaddingMode Padding

byte[] Key

byte[] IV

Using the .NET Framework Libraries

Key

- Byte array to store encryption key
- Generate secure keys
  - RNGCryptoServiceProvider or
  - GenerateKey()

SymmetricAlgorithm

CipherMode Mode

PaddingMode Padding

byte[] Key

byte[] IV

Using the .NET Framework Libraries

IV

- InitializationVector is a byte array
- Also called a nonce or number once
- IV prevents repetition in encryption
- IV does not have to be kept secret

SymmetricAlgorithm

CipherMode Mode

PaddingMode Padding

byte[] Key

byte[] IV

AesManaged or AesCryptoServiceProvider

- .NET provides 2 implementations of AES
  - AesManaged
  - AesCryptoServiceProvider

- AesManaged : .NET specific implementation
- AesCryptoServiceProvider : Uses windows cryptography libraries.
  - FIPS 140-2 certified

CryptoStream

- CLR uses a stream oriented design for cryptography
- Core of this design is CryptoStream

Code Demo

Encryption with DES, TripleDES and AES

Module Summary

- What is symmetric encryption?
- The history of DES and Triple DES
- How does DES and Triple DES work?
- The history of AES
- How does AES work?

Module Summary

- How secure is AES against brute force attacks?
- Using the .NET Framework Libraries
  - Use AESCryptoServiceProvider over AESManaged