Cryptography

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Introduce basic cryptography concepts

Outline forms of cryptography and common examples that can be leveraged by your organization

Discuss methods of cryptanalytic attacks and how to protect your organization

This is the 9th objective of the Security Engineering domain of the CISSP® Exam

“Cryptography is typically bypassed, not penetrated.”

Adi Shamir (co-inventor of the RSA algorithm (i.e. the S in RSA))

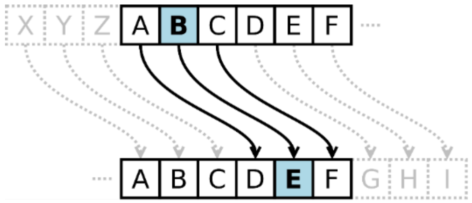
Basic Concept of Cryptography

Key Cryptographic Concepts

Algorithm (i.e. Cipher)	Key	Encryption / Decryption
Transposition	Substitution	Work Factor

Cryptography Isn't New!

Spartan Scytale



Caesar Cipher

Confederate Army's Cipher Disk

German Enigma Machine

Advances in Cryptography

Traditional Cryptography

Exists today and has for quite a while

Uses math as fundamental mechanism

Principle is that strong mathematics is difficult to break, so security of cryptographic output is high

Numerous methods of application possible

Quantum Cryptography

Exists mainly in theory

Uses physics as fundamental mechanism

Principle is a person cannot know a particle's momentum and position with unlimited accuracy at the same time (i.e. law of physics prevents circumvention of protection)

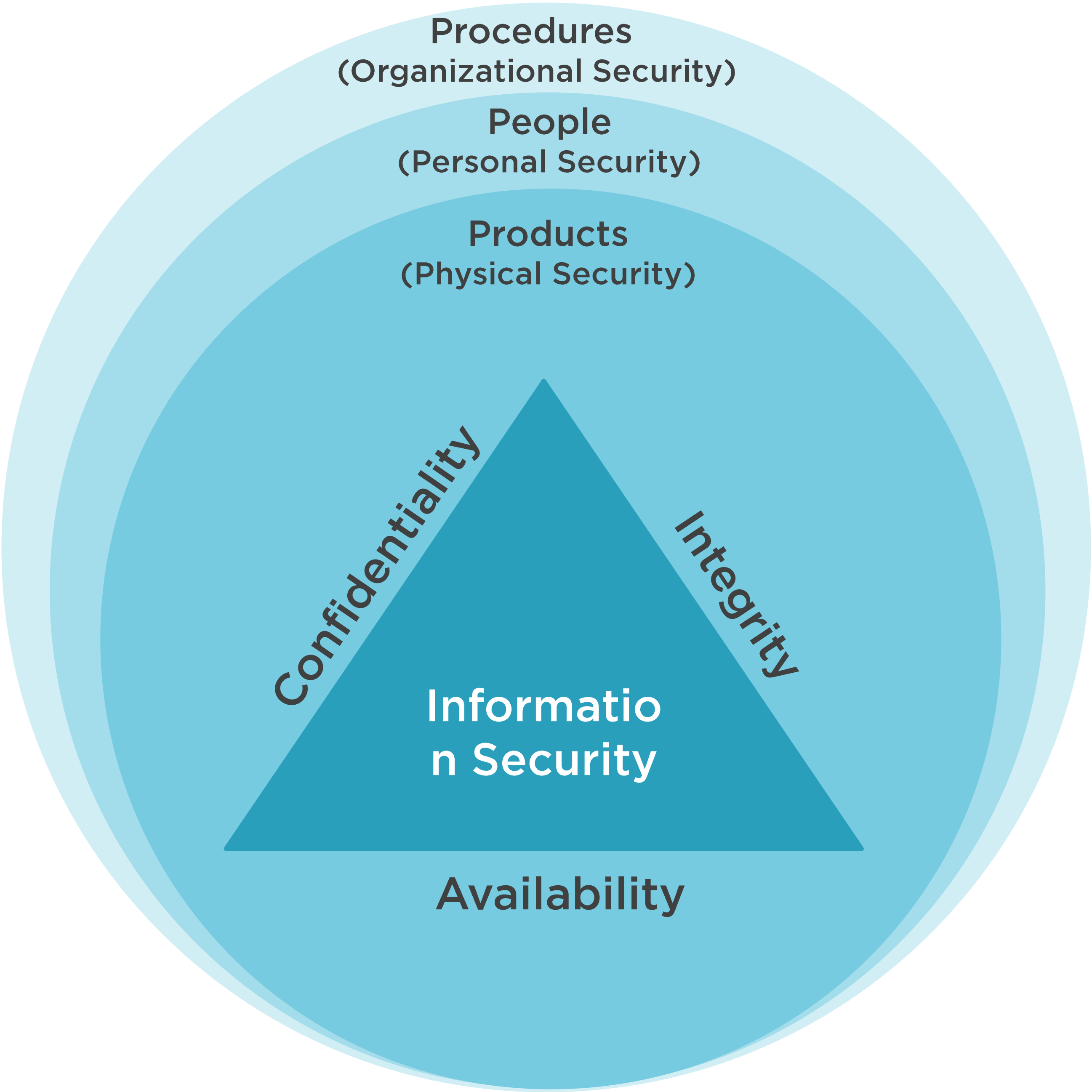
Only used for key creation and distribution, as further uses are passed over to traditional cryptography methods

Cryptography aligns well with the C & I, but not the A, of the CIA Triad

Confidentiality = C

Integrity = I

~~Availability = A~~



The stronger the cryptographic function, the more expensive to break it, and the less likely it will be broken (i.e. economically infeasible)

Cipher Methods

Stream-Based Ciphers

Performs on a bit-by-bit level

Ciphertext is created out of the plaintext with the keystream, typically via an exclusive-or (XOR) operation

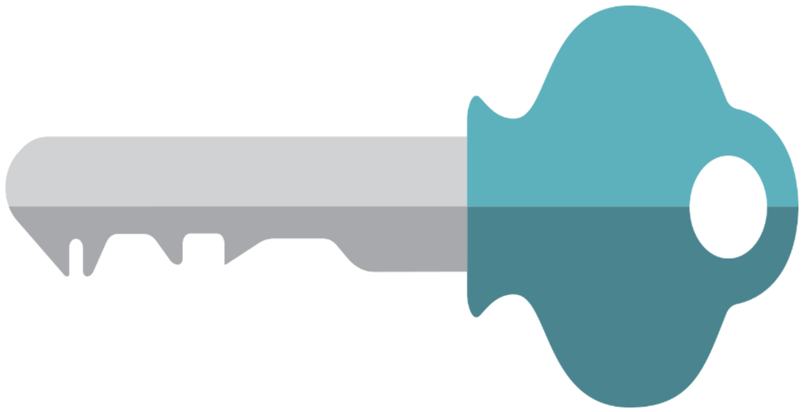
XOR is a simple binary decisions (0+0 = 0, 1+1 = 0, 1+0 = 1, 0+1 = 1)

Block Ciphers

Performs on a preset block size (e.g., 64 bits)

Ciphertext is typically created with substitution and transposition of plaintext

Typically viewed as stronger than stream-based ciphers, due to the more computationally intensive operation, but requires use of Initialization Vector



Key length is the size of the key, which is usually measured in bits or bytes

The level of security provided by the cryptographic function is directly related to the length of the key (i.e. larger keys provide more)

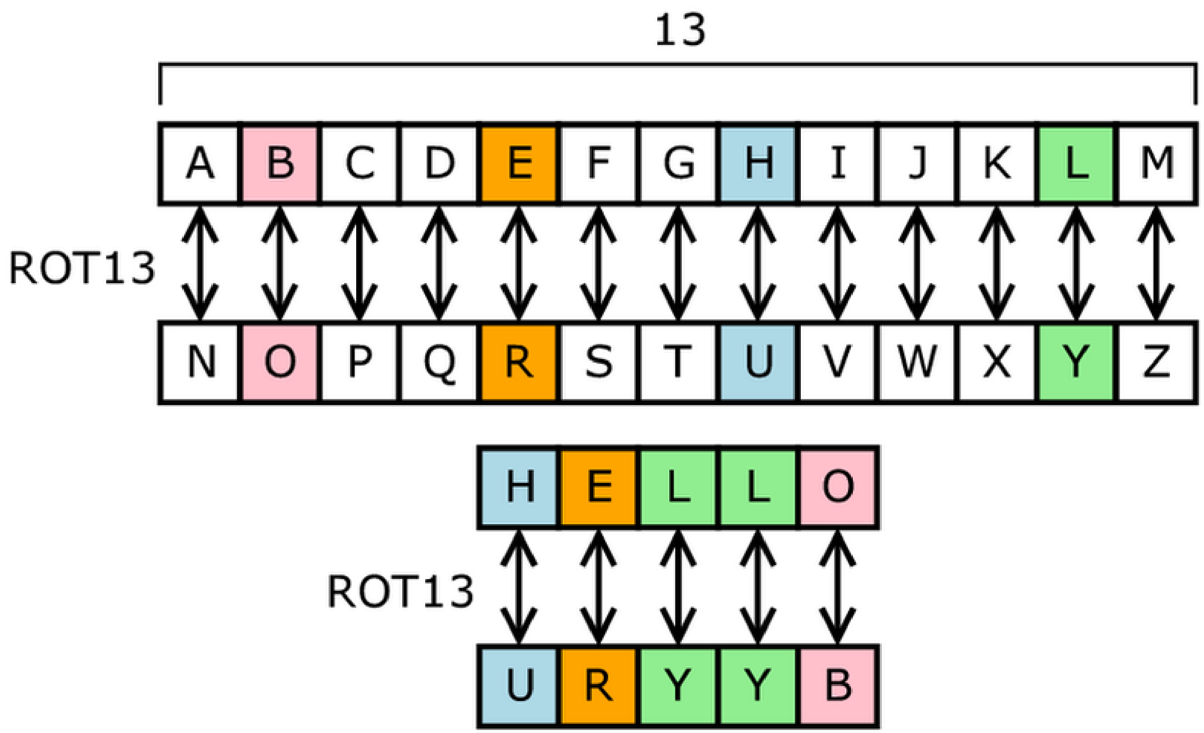
- Some exceptions exist to that, due to the implementation (i.e. Triple DES is really three 56-bit keys providing 112-bit protection, not 168-bit (total key length))

It isn’t best to always use the largest key length possible, as the particular circumstances of usage might not benefit from it

Substitution Ciphers

Each letter is changed to another one (i.e. substituting one for another)

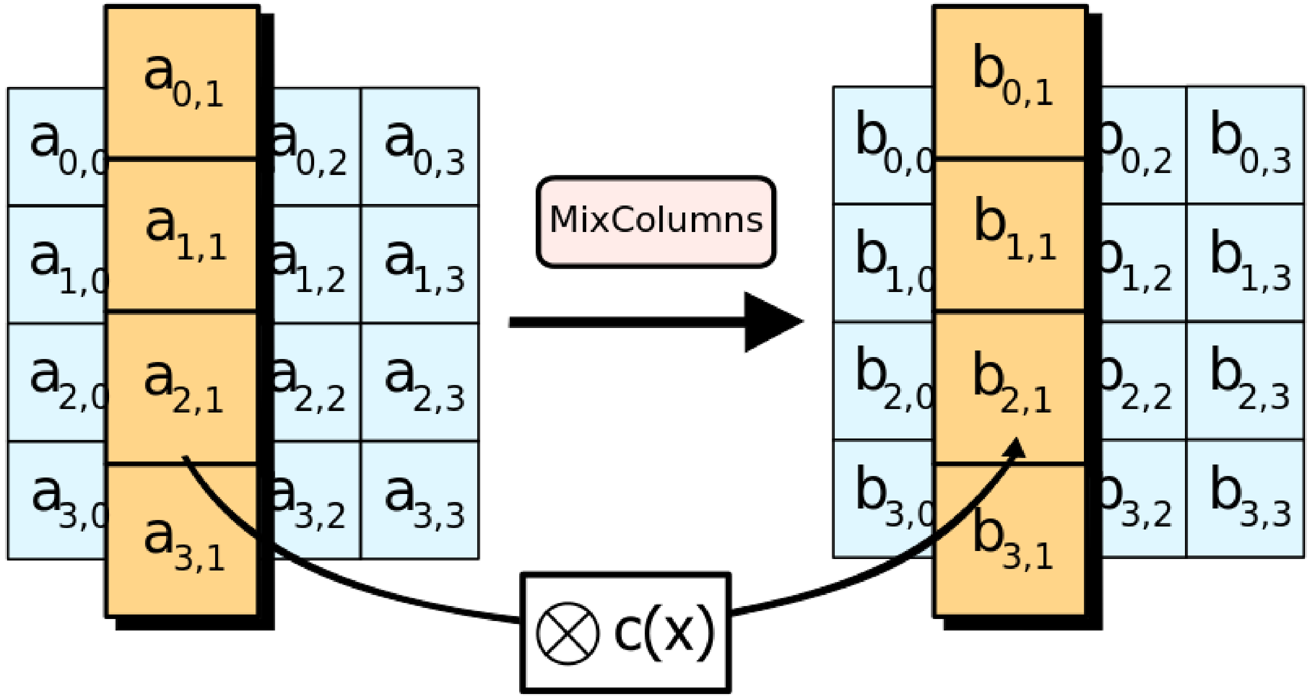
Example provided is ROT13 or Rotate 13 Places, which in an ancient implementation of the Caesar Cipher



Transposition Ciphers

Each letter's order is interchanged with each other via permutation (i.e. transposing of the order of the letters)

Example provided is the MixColumns step of the Advanced Encryption Standard (AES) / Rijndael



Forms of Cryptography

Symmetric

Created thousands of years ago

Single key for encryption and decryption

Send and receiver have to have the key

Faster operation than asymmetric

Key management is difficult

Example: Encrypted file that is emailed from one user to another, where the sender has to contact the recipient separately and tell them the password to decrypt the file

Asymmetric

Created in the 1970s

Separate keys for encryption and decryption

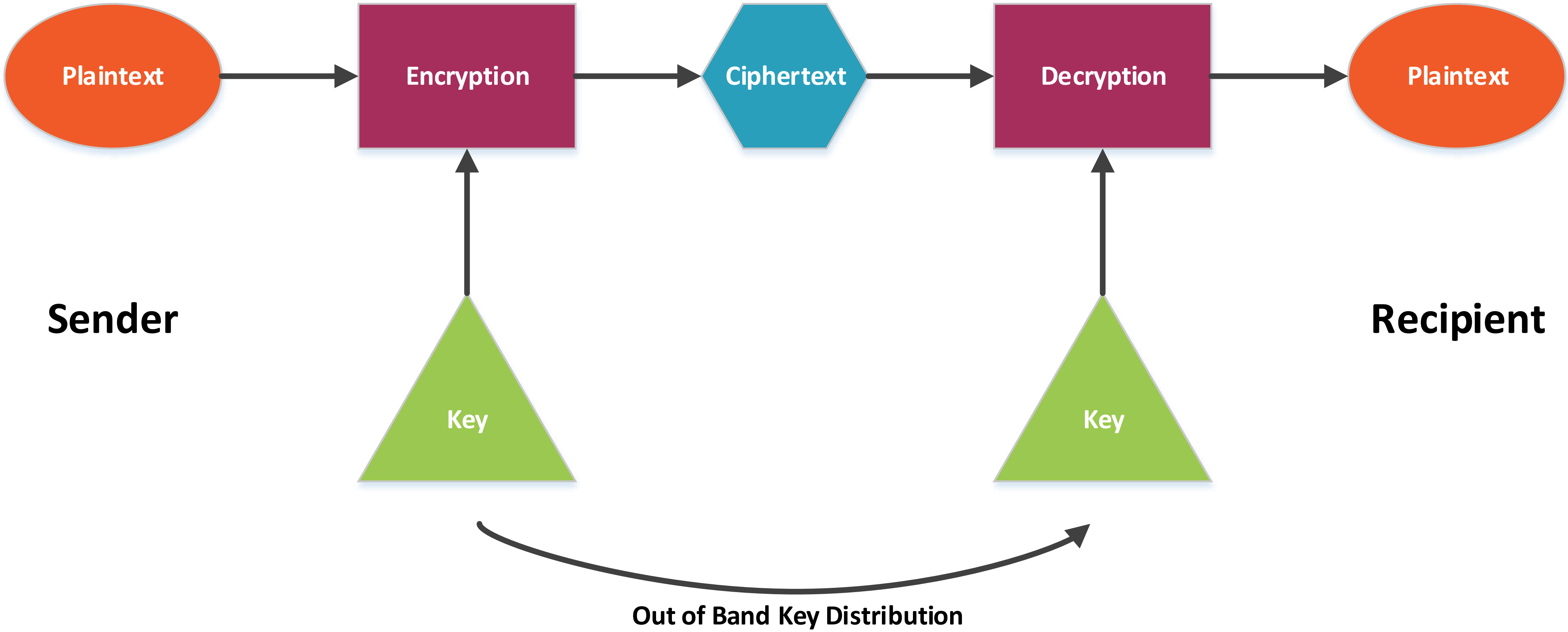
Sender and receivers have their own keys

Slower operation than symmetric

Key management is simpler

Example: User leverages a shared Public Key Infrastructure's certificates to encrypt a file with the recipient's public key, sends it to them, and the recipient decrypts the file with their

Symmetric Encryption Example



Common Symmetric Cryptography Examples

Data Encryption Standard (DES)

Double DES (2DES)

Triple DES (3DES)

Advanced Encryption Standard (AES) / Rijndael

Data Encryption Standard (DES)

Was the standard encryption mechanism in late 1900s until Rijndael replaced it, due to its limitations

Block cipher (also adapted to be a stream cipher)

Uses 56-bit key (64-bit in length, but 8 are parity)

Block modes

- Electronic Cookbook Mode (ECB)
- Cipher Block Chaining Mode (CBC)

Stream modes

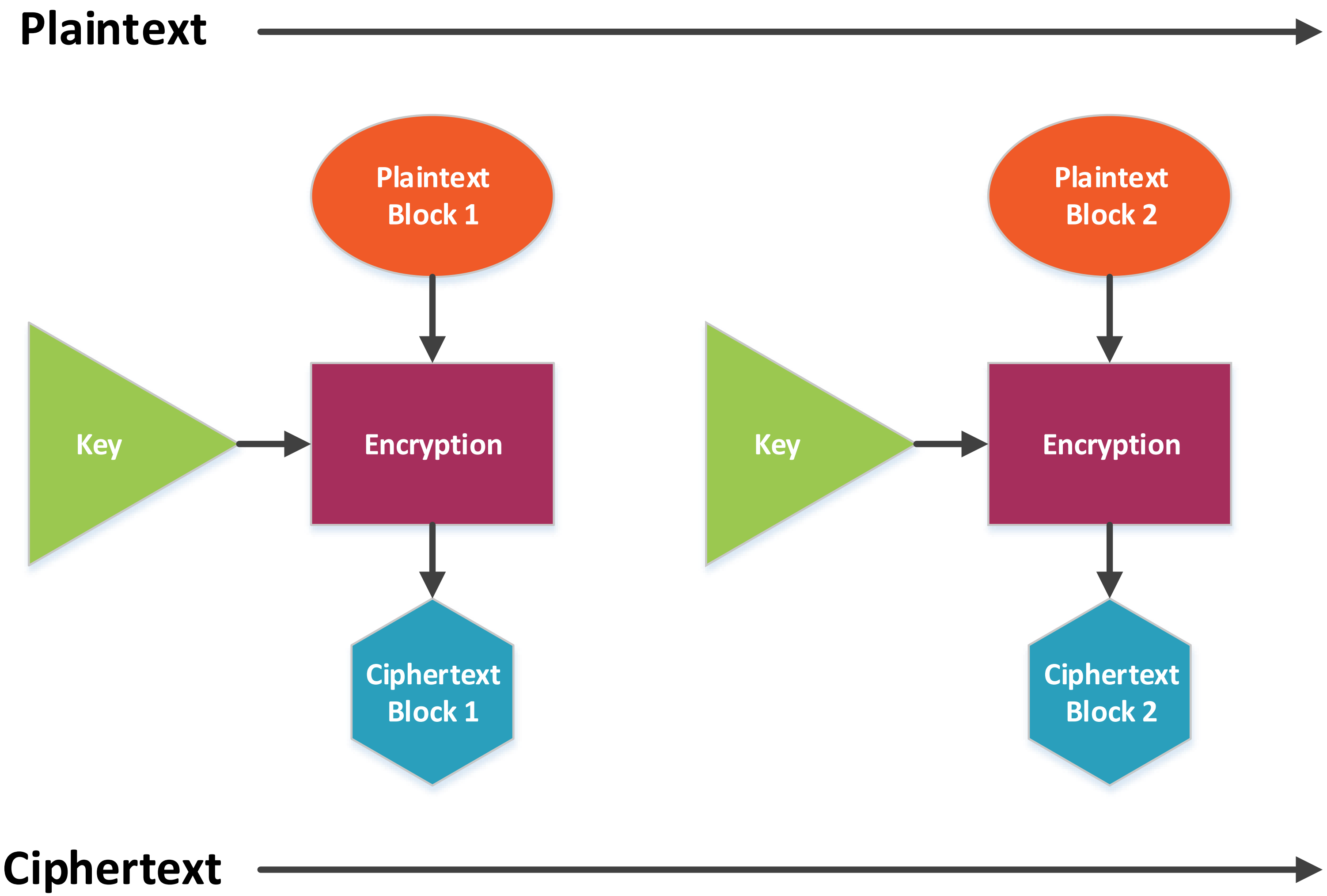
- Cipher Feedback Mode (CFM)
- Output Feedback Mode (OFM)
- Counter Mode (CTR)

DES – Electronic Cookbook Mode (ECB)

Most basic block cipher mode in DES

Blocks are operated on independently of each other, which reduces the protection provided

Decryption is the reverse of the encryption process

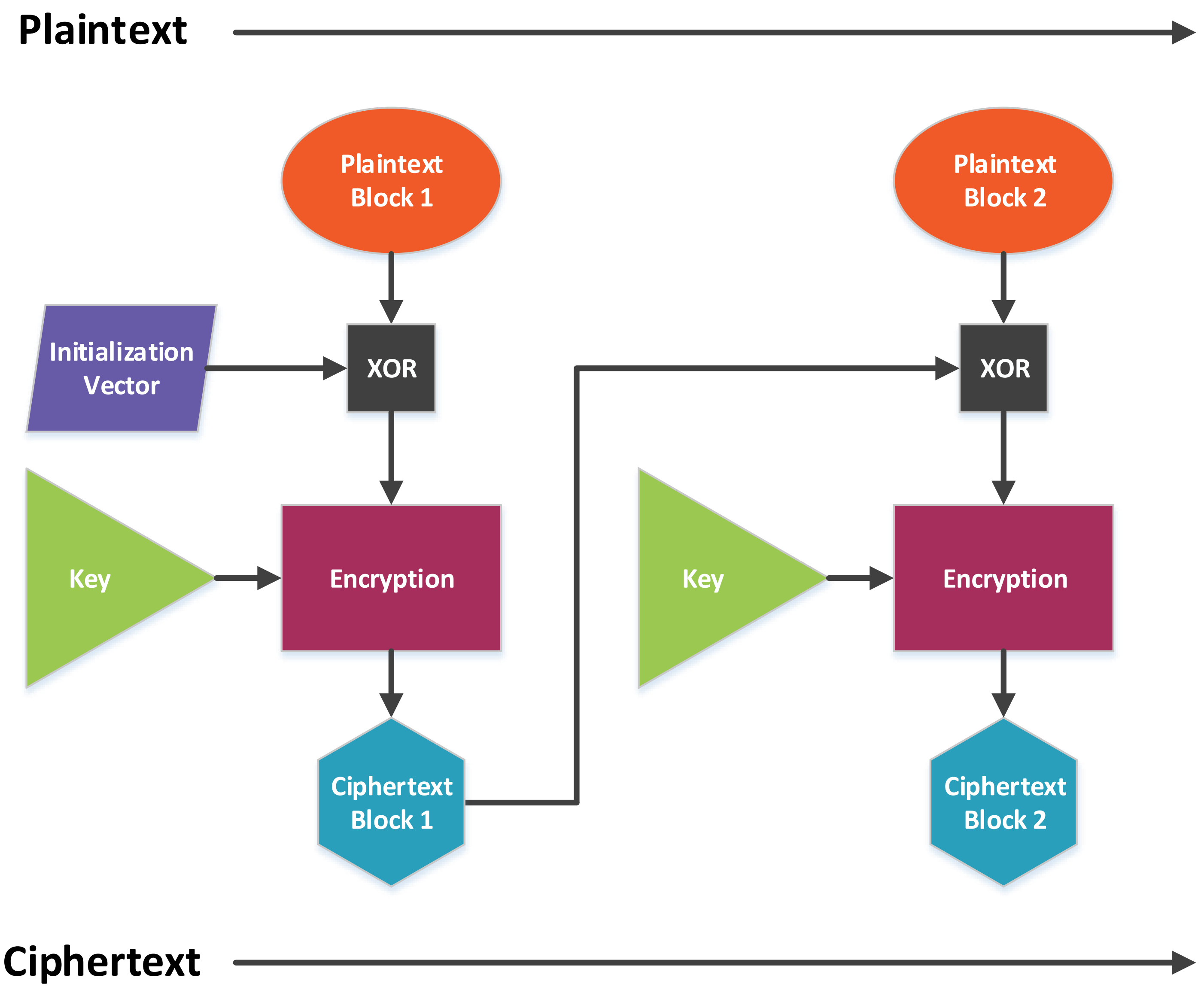


DES – Cipher Block Chaining Mode (CBC)

Stronger than ECB

Chaining function performs XORs on plaintext input with previous ciphertext output

First plaintext is mixed with the Initialization Vector, which is a randomly chosen value



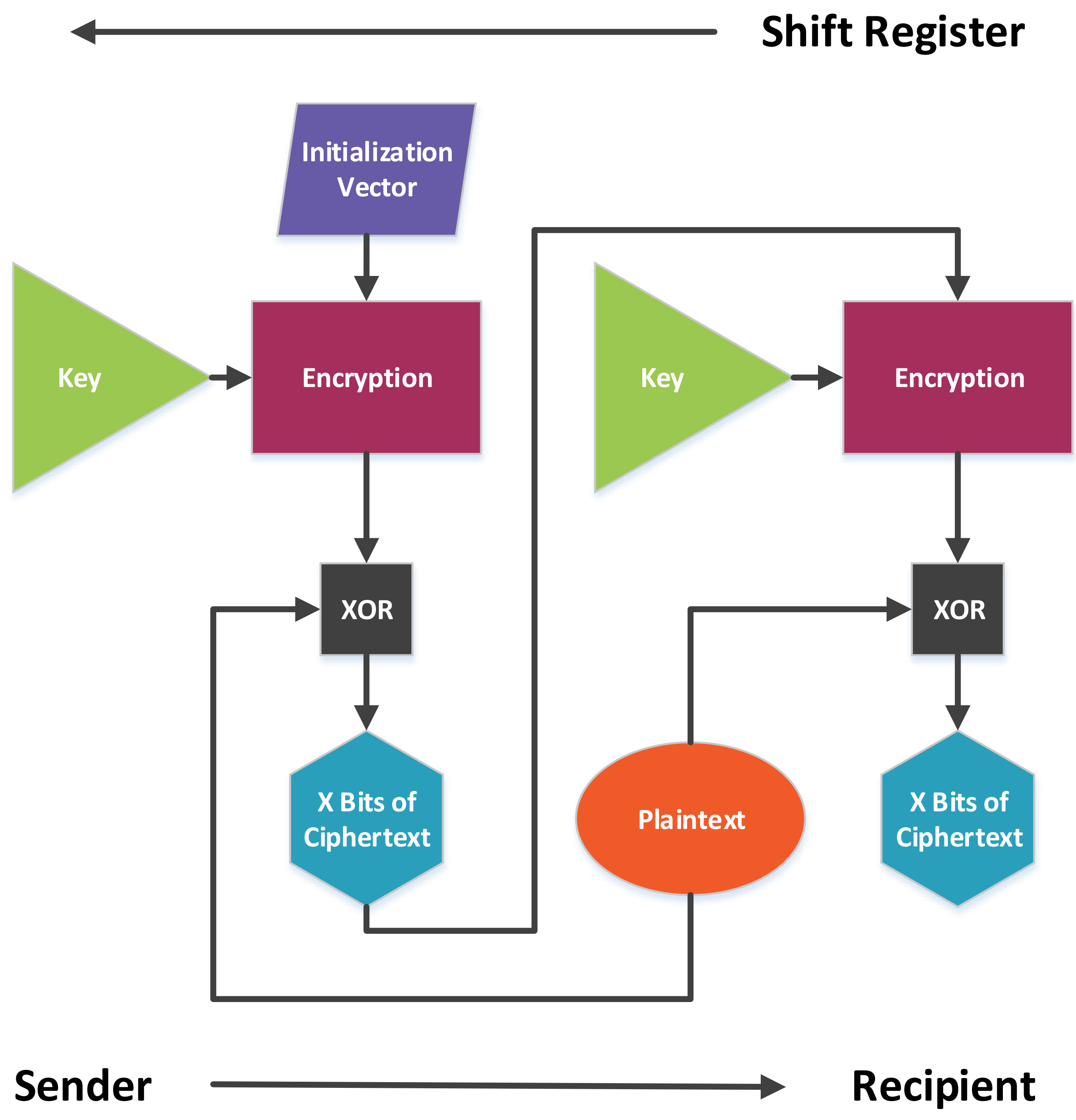
DES – Cipher Feedback Mode (CFB)

Stream-based cipher

Can be 1, 8, 64, or 128-bit sized segments

Segments are transmitted to recipient and then loaded in shift register to continue operation

Operation ends when no more input is provided



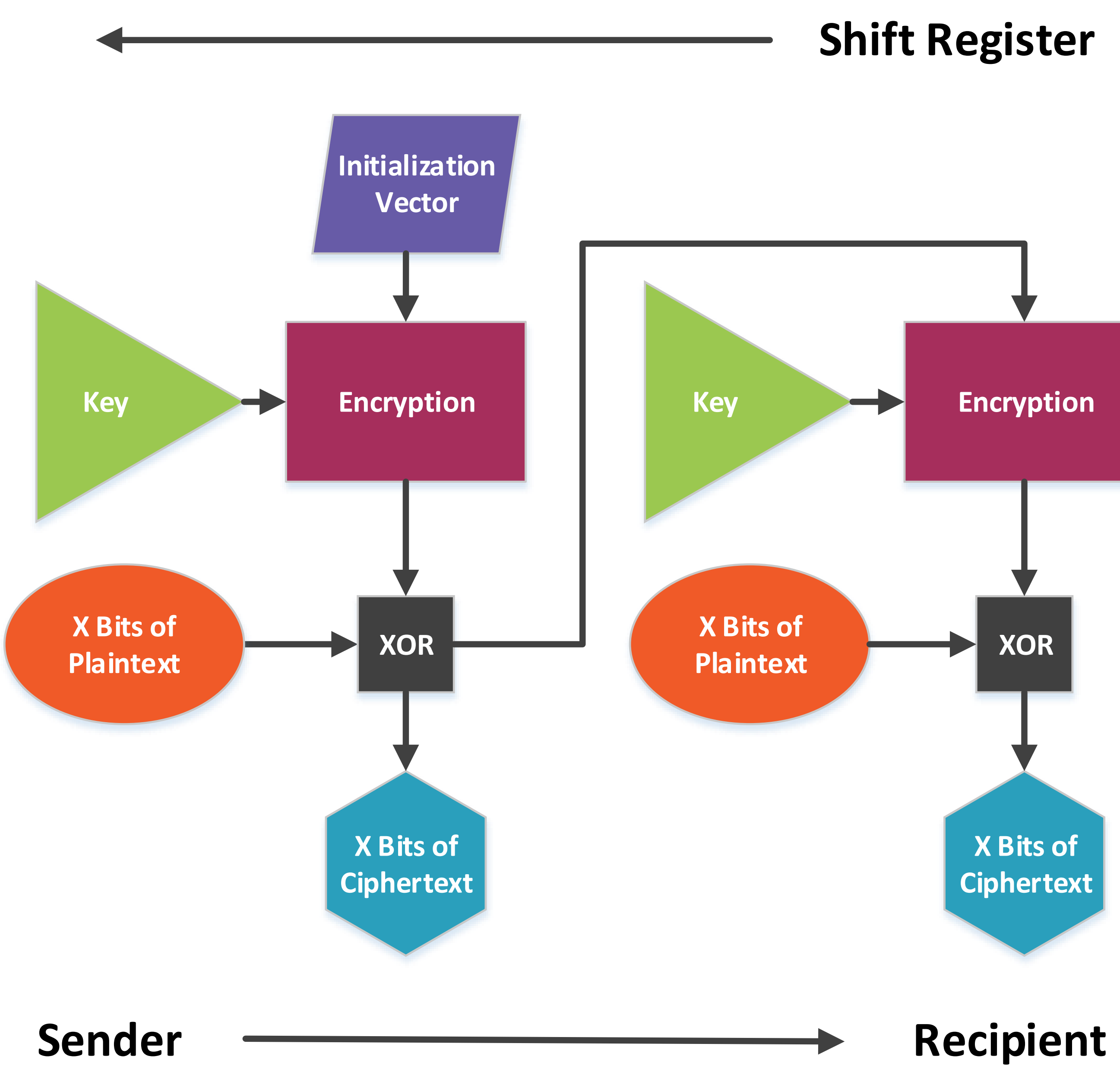
DES – Output Feedback Mode (OFB)

Stream-based cipher

Very similar to CFB

Main difference is key stream and message data are now independent

This is because the ciphertext is not fed back into the shift register, but the keystream is



DES – Counter Mode (CTR)

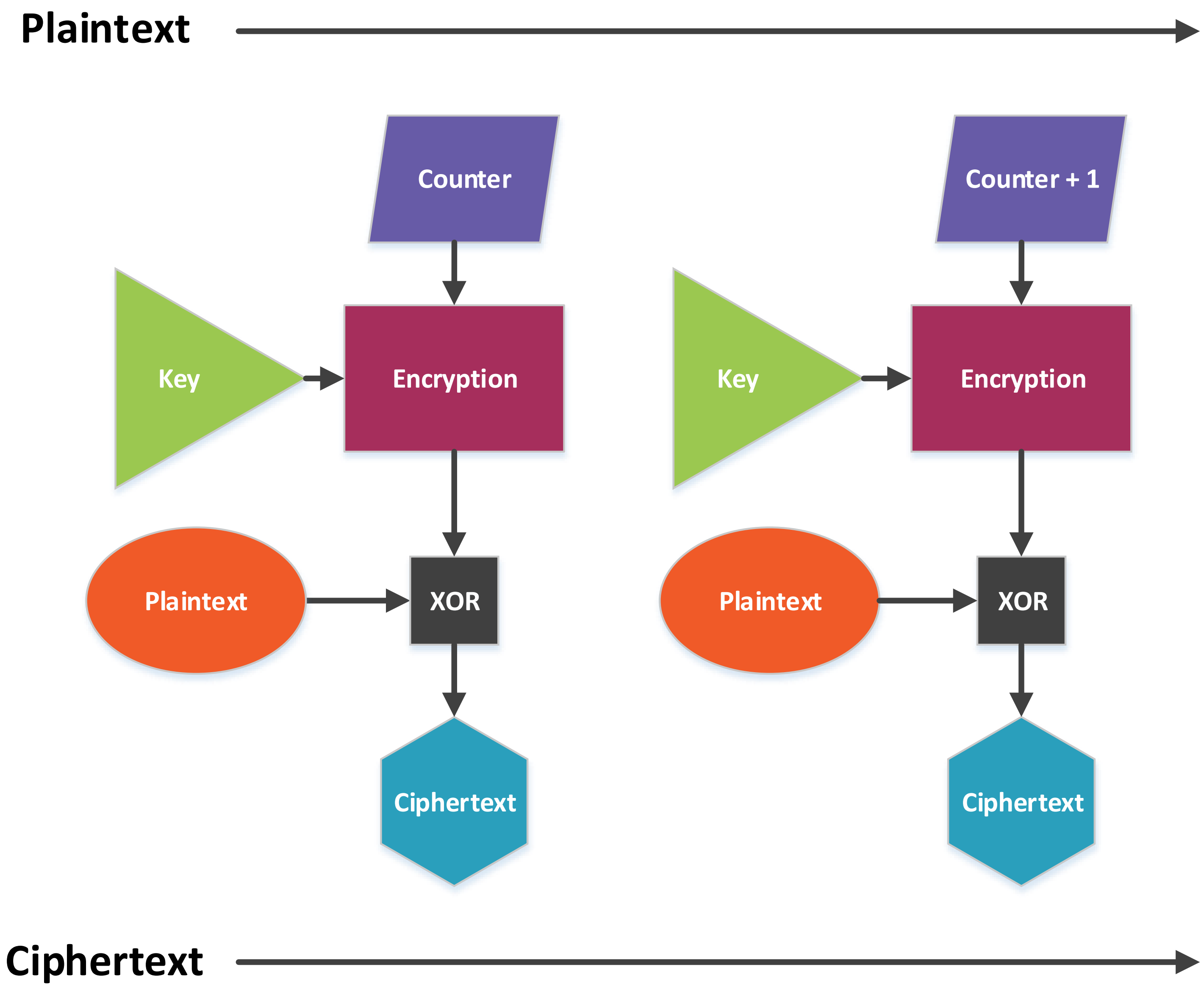
Stream-based cipher

High-speed application uses are common

Counter is a 64-bit Initialization Vector

Each counter is different

Just like OFB, key stream and message are independent from each other

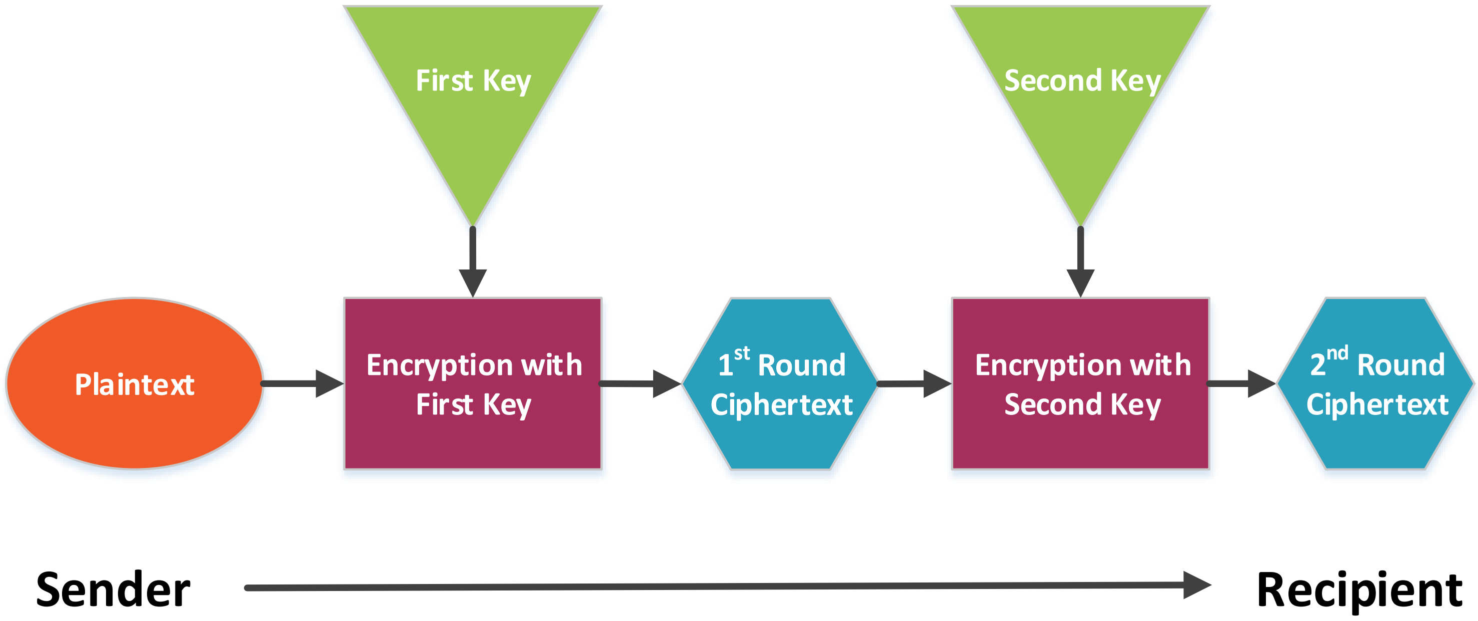


Double DES (2DES)

Created to try to resolve the issues around DES keys being too small

Simple approach of doubling the encryption process for 112- bit strength (two 56-bit keys)

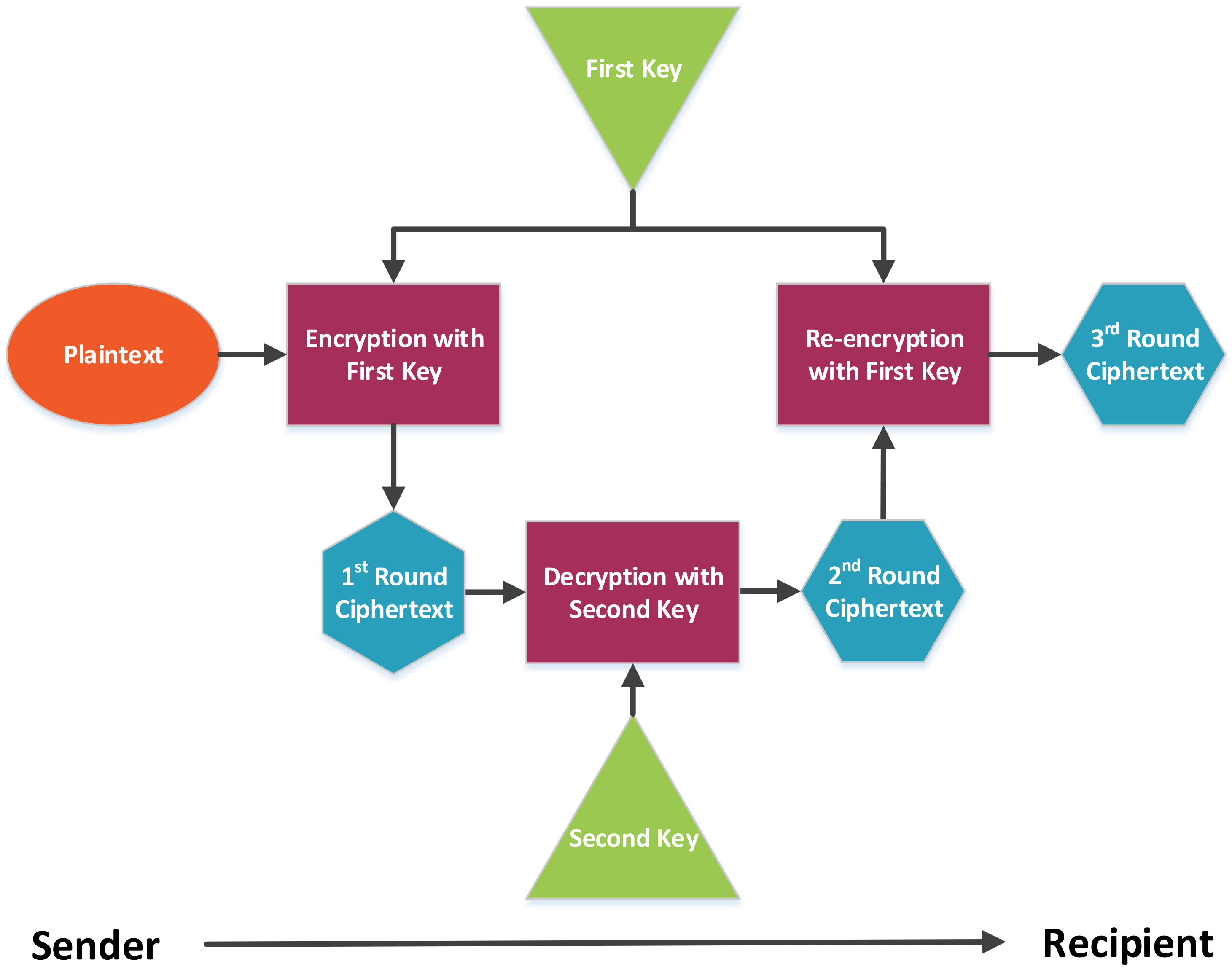
Limited success, due to vulnerabilities in operation, led to 2DES being replaced by 3DES



3DES

Created to attempt to solve the weaknesses of 2DES and DES

Targeted 168-bit key strength, but with only two 56-bit keys, it still only effectively has 112-bit strength

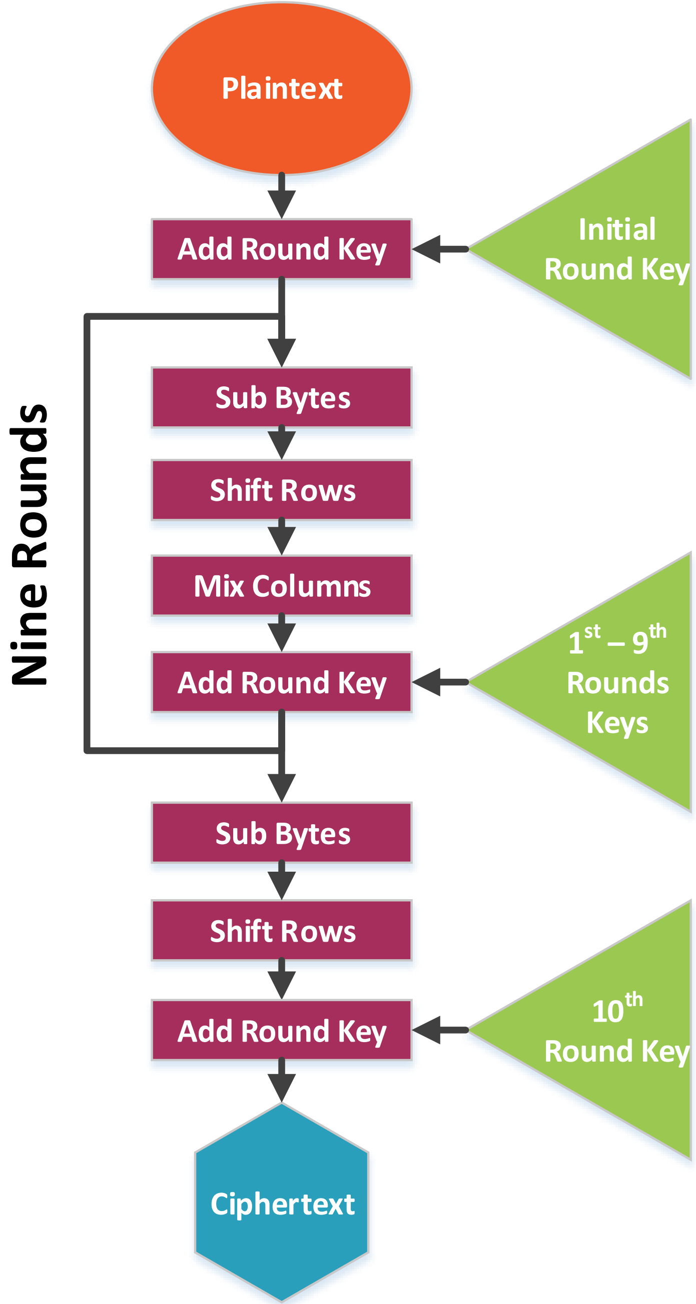


Advanced Encryption Standard (AES) (aka Rijndael)

Block cipher

Block size of 128-bits, with key lengths of 128, 192, and 256-bits

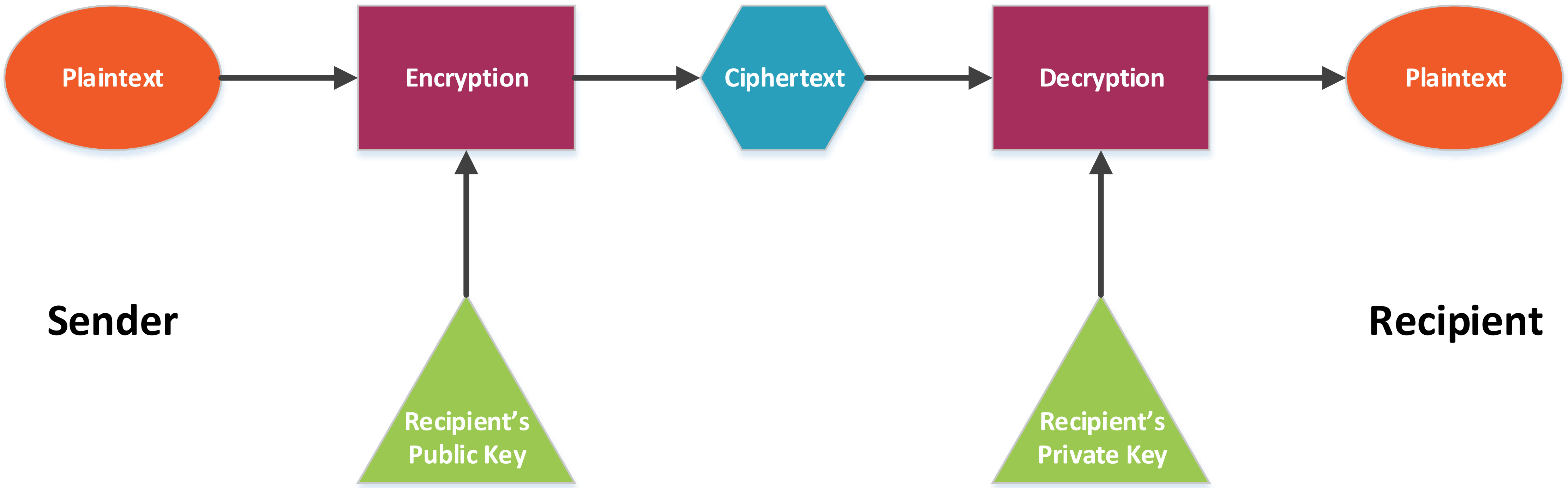
Leverages multiple methods in operation (Sub Bytes, Shift Rows, Mix Columns, and Add Round Key)



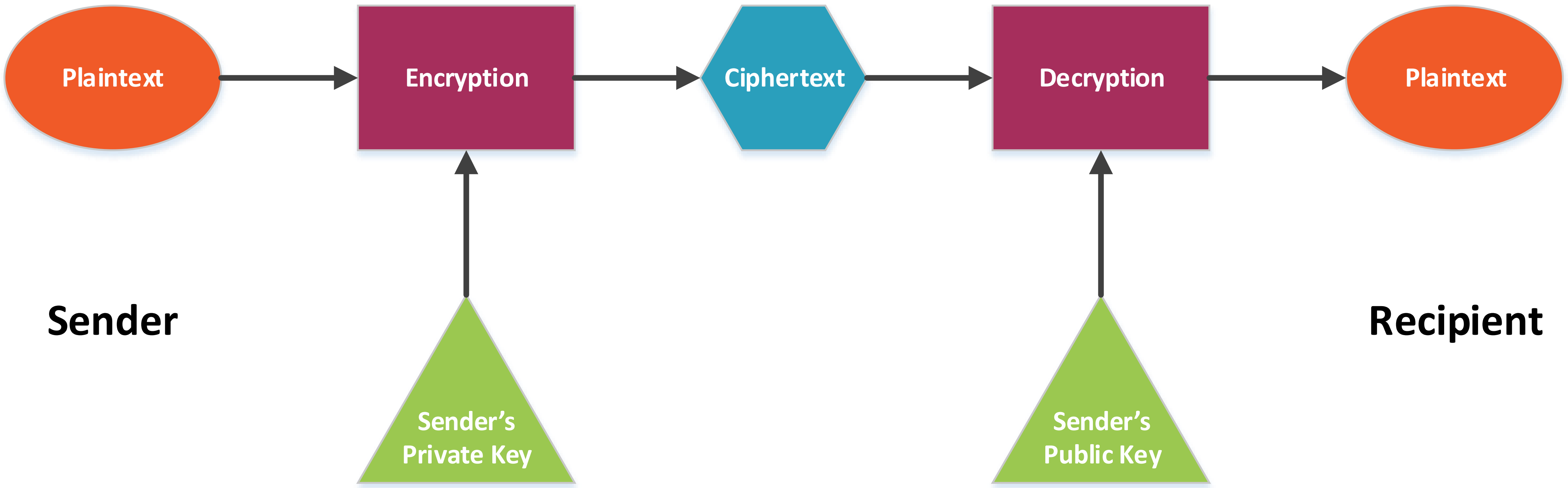
Symmetric Algorithm Pros and Cons

Advantages	Disadvantages
Fast	Key management difficulties
Provides confidentiality and integrity	Lack of true nonrepudiation of origin
	Lack of true access control
	Lack of true digital signatures

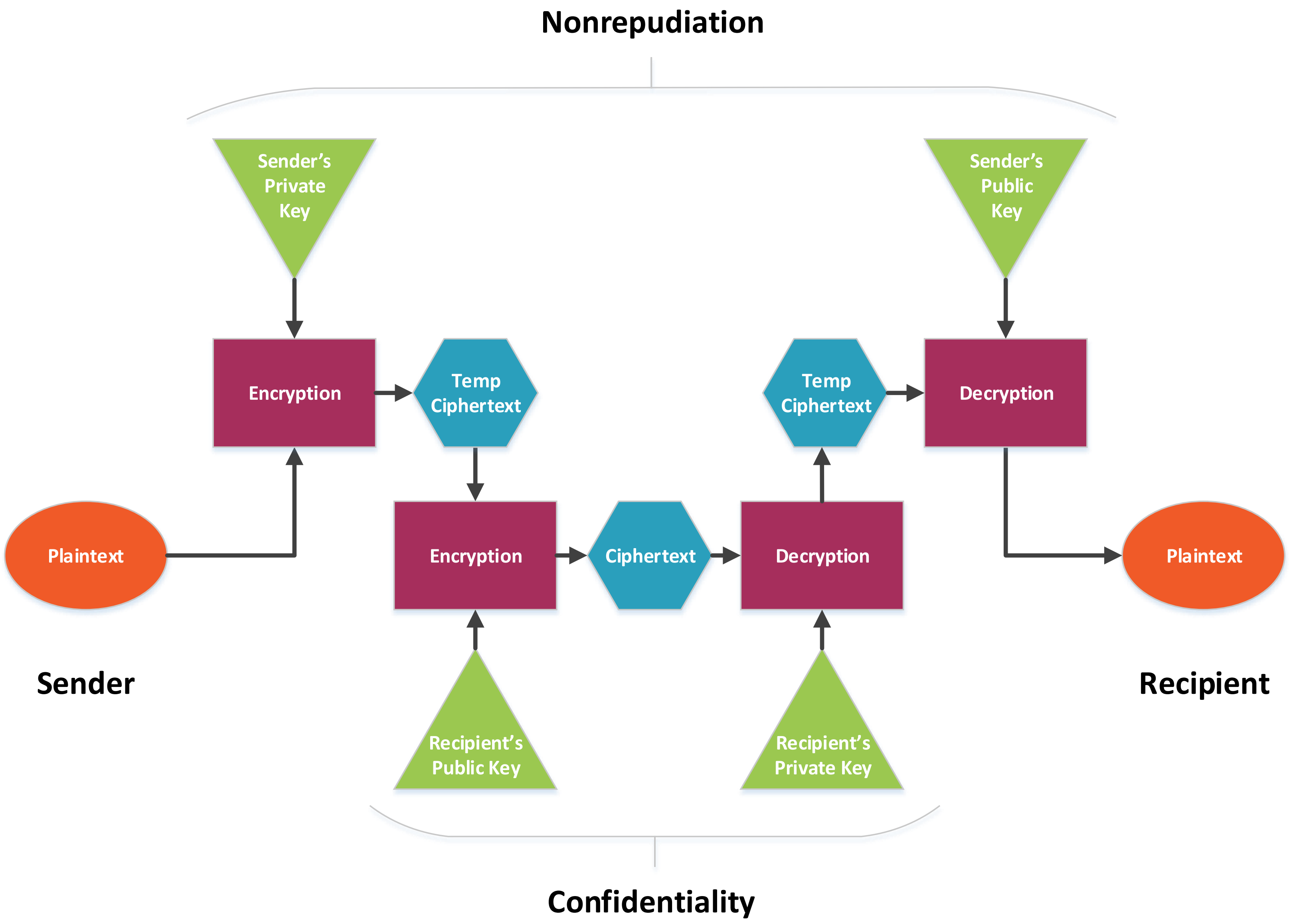
Asymmetric Confidentiality Example



Asymmetric Nonrepudiation Example



Asymmetric Example of Both



Common Asymmetric Cryptography Examples

RSA
(named after inventors’ last names (i.e. Ron Rivest, Adi Shamir, Len Adleman))

Diffie-Hellman

Elliptic Curve Cryptography (ECC)

Asymmetric Algorithm Pros and Cons

Advantages

Provides confidentiality and integrity

Key management difficulties

Nonrepudiation of origin and delivery

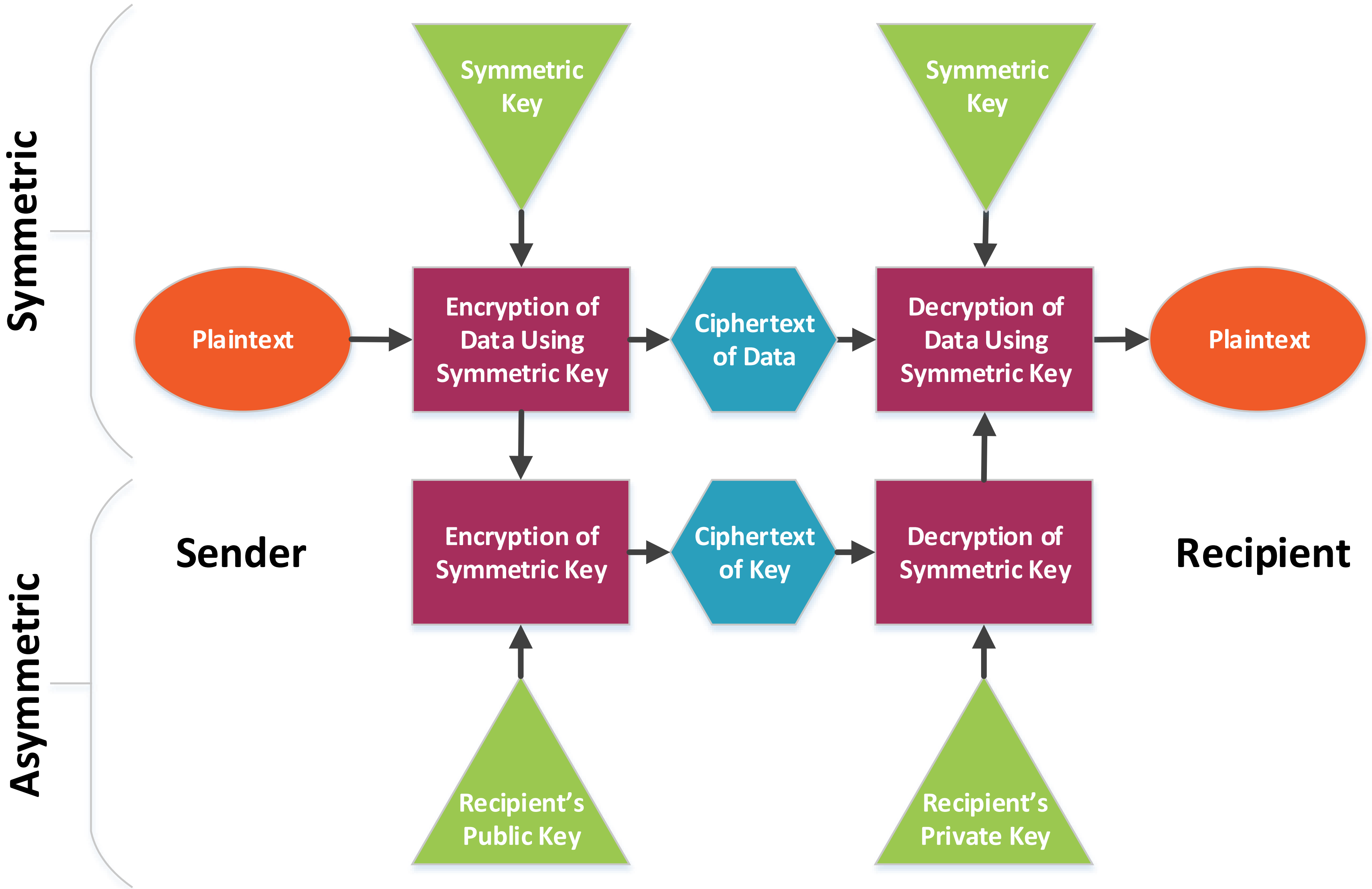
Access control and data integrity

Digital signatures

Disadvantages

Slow compared to symmetric

Hybrid Cryptography



Hashing

Hashes are also called Message Digests

Function that takes any length input and generates a fixed length output

Is a one way operation (can't be reversed)

Provides a way to validate that contents of a file were not changed from when the hash was originally created for a file

Common hashing algorithms are:

- MD5 Message Digest Algorithm
- Secure Hash Algorithm (SHA)
  - Multiple versions
- HAVAL
- RIPEMD-160

Hashing Attacks

Two main ways to attach hash functions:

- Brute force
- Cryptanalysis

Brute forcing a hash function is done so by exploiting a vulnerability in the algorithm

Cryptanalysis against a hash function is done by attacking the implementation of the algorithm, not the algorithm itself (e.g., side-channel attacks)

Rainbow tables are commonly used to defeat hashes, especially password hashes, where large tables are prepopulated with hash results to uncover the password behind the hash

Methods of Cryptanalytic Attacks

- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Implementation

Cryptography's Lifecycle

As computational power increases, while becoming more economical, there will be a definitive lifespan of all cryptographic functions

Governance of the algorithms, key sizes, validity period, protocols, etc. used in your organization is important to prevent attackers from compromising your defenses that rely on cryptographic mechanisms

A cryptographic function is considered broken when the following occurs:

- Decryption without key economically
- Hash can be reproduced economically without original source
- Side channel attack is possible

Cryptography Export Controls and Law Enforcement

Many countries have laws in place to limit the use, import, or export of cryptographic functions

For example, the US government regulates what technology products can vs. cannot be exported, due to the cryptography included within the product

Some technology manufacturers create different versions of the same product, with one that can be sold in the US and another with weakened or no cryptographic functions that can be exported

Privacy concerns by citizens continue to evolve the acceptable use of cryptography within products and by law enforcement (back doors)

Encoding != Encryption

Summary

Introduced basic cryptography concepts

Outlined forms of cryptography and common examples that can be leveraged by your organization

Discussed methods of cryptanalytic attacks and how to protect your organization

This is the 9th objective of the Security Engineering domain of the CISSP® Exam

What’s Next?

Site and Facility Secure Design

What are they?

How do they relate to this module and the other modules?

Why are they important to this course and the CISSP® exam?