CS 4910: Into to Computer Security

Cryptographic Tools I

Instructor: Xi Tan

Review

- CIA
- Levels of Impact
- Why is computer security hard
- Assets of a computer system

Outline

Cryptographic tools

- Overview
- Symmetric Key Cryptography
- Public Key Cryptography
- Message Integrity and Digital Signatures
- Summary

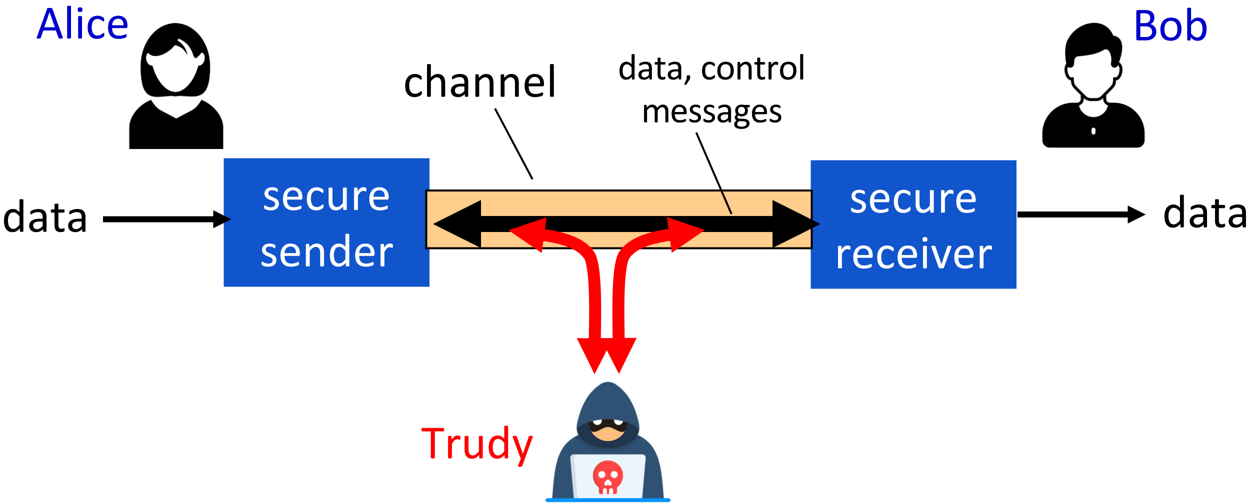
Overview

What is Cryptography

- Greek: “krypto” = hide
- Cryptographic – secret writing.
  - Originally, it is the study of encryption principles and methods
  - The most basic problem of cryptography is to ensure security of communication over insecure media
- Cryptographer

Friends and enemies: Alice, Bob, Trudy

- Well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, *real-life* Bobs and Alice!
  - Web browser/server for electronic transactions (e.g., on-line purchases)
  - On-line banking client/server
  - DNS servers
  - Routers exchanging routing table updates

Cryptography

Can help

- Confidentiality
  - Obscure a message from eavesdroppers
- Integrity
  - Assure recipient that the message was not altered
- Authenticity
  - Verify the identity of the source of a message
- ...

Cryptography & Security

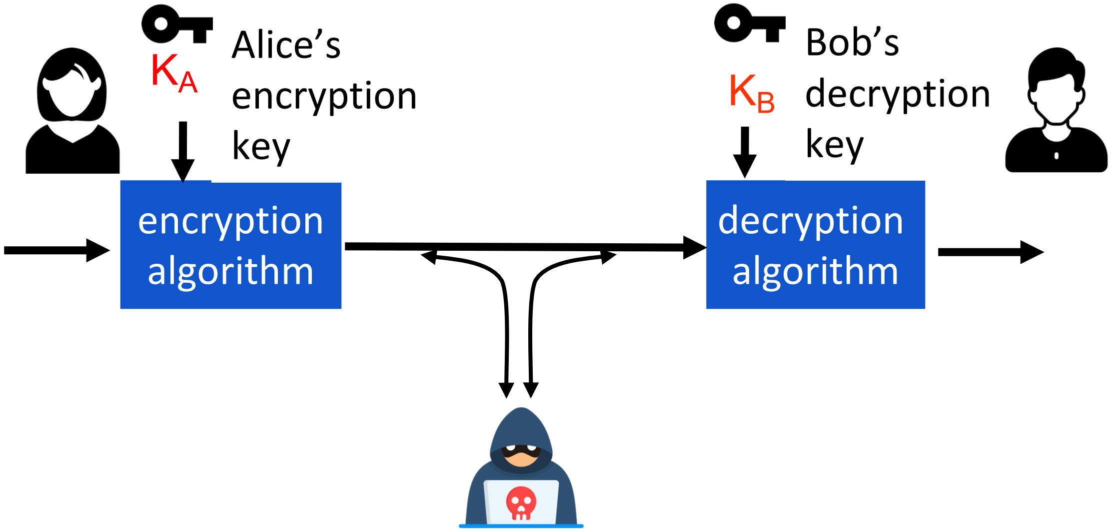
- Most people argue cryptology is a branch of mathematics
- Security is about math, engineering, hardware, software, people, etc.
- Attackers try to find the weakest link. In most cases, this is not the mathematics
- Example: HeartBleed

- Cryptographic tools are essential in designing secure solutions and their understanding is crucial to correct usage

Types of Cryptography

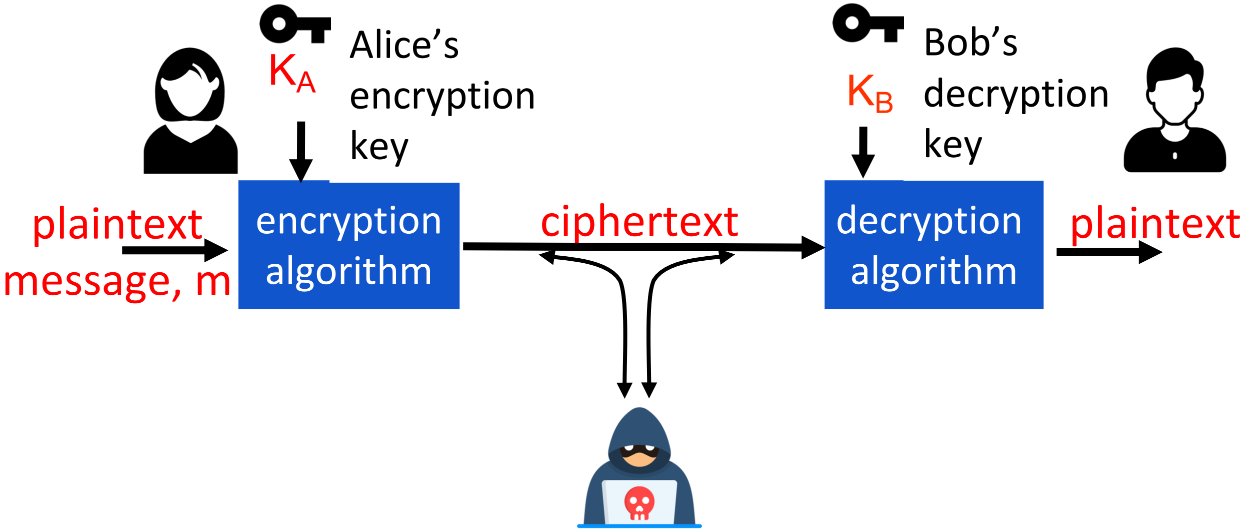
- Crypto often uses keys:
  - Algorithm is known to everyone
  - Only “keys” are secret
- Symmetric key cryptography
  - Involves the use one key
- Public key cryptography
  - Involves the use of two keys
- Hash functions
  - Involves the use of no keys
  - Nothing secret: How can this be useful?

The language of cryptography



K_A/K_B: sequence that controls the operation and behavior of the cryptographic algorithm
Keyspace: Total number of possible values of keys in a crypto algorithm

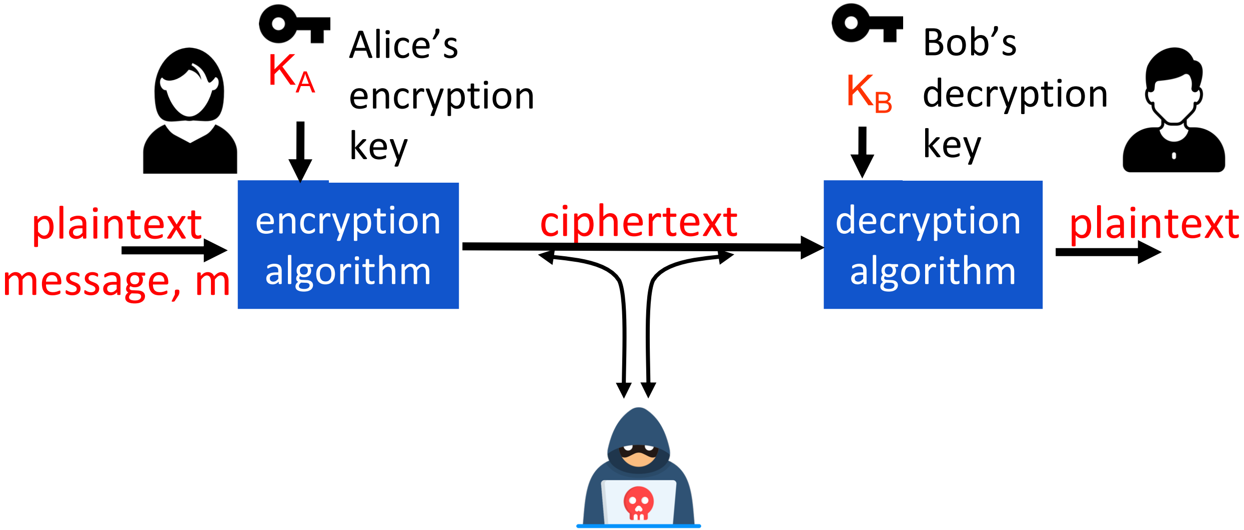
The language of cryptography



Plaintext (m): the message to be transmitted or stored.

Ciphertext: the disguised message.

The language of cryptography



Encryption ($K_A(m)$): the process of disguising a message so as to hide the information it contains; this process can include both encoding and enciphering

$m = K_B(K_A(m))$: decrypted with key K_B

The language of cryptography

Protocol: an algorithm, defined by a sequence of steps, precisely specifying the actions of multiple parties in order to achieve an objective.

Cryptosystem: The combination of algorithm, key, and key management functions used to perform cryptographic operations

Simple encryption scheme

Substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

E.g.:

```
 Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Key: the **mapping** from the set of 26 letters to the set of 26 letters

Breaking an encryption scheme

- Cipher-text only attack: Trudy has ciphertext that she can analyze
  - Two approaches:
    - Search through all keys (brute-force): must be able to differentiate resulting plaintext from gibberish
    - Statistical analysis

- Known-plaintext attack: trudy has some plaintext corresponding to some ciphertext
  - e.g., in Caesar cipher, trudy determines pairings for a,l,i,c,e,b,o,

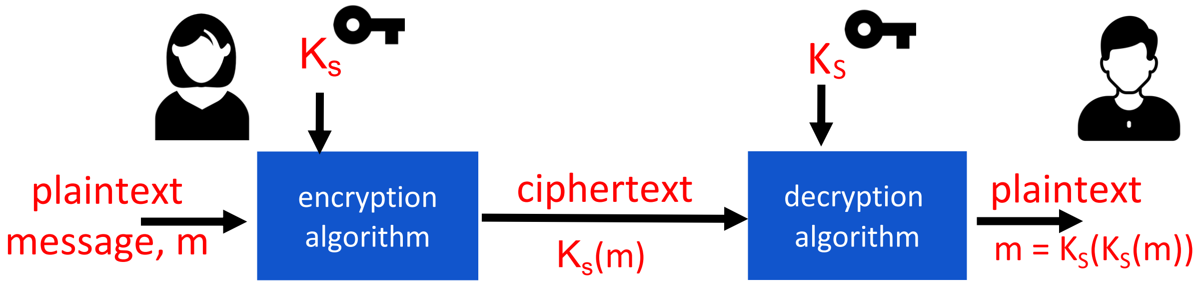
- Chosen-plaintext attack (CPA): Trudy can get the cyphertext for some chosen plaintext

Symmetric Key Cryptography

Symmetric key cryptography

- Symmetric (or secret-key) encryption means that the same key is used both for encryption and decryption
- The key must remain secret at both ends
- Such algorithms are:
  - normally very fast
  - can be used as primitives in more complex cryptographic protocols
  - the key often has a short lifetime

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful, all future and past messages encrypted with that key are compromised

Brute-Force Attacks

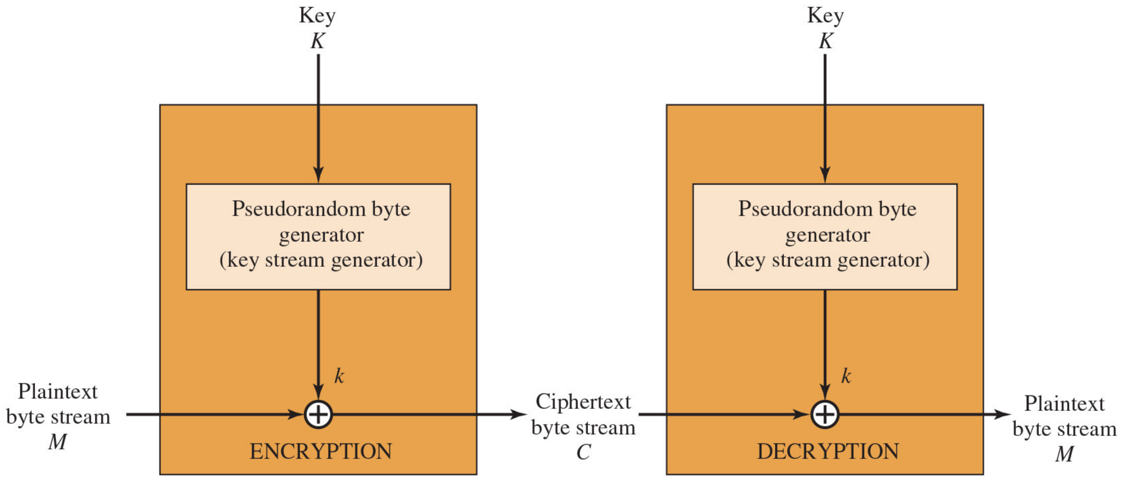
- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - On average half of all possible keys must be tried to achieve success

Symmetric key cryptography

- There are two types of symmetric key algorithms:
  - stream ciphers
    - the message is processed as a stream
    - pseudo-random generator is used to produce a long key stream from a short key
  - block ciphers
    - the key has a fixed size
    - prior to encryption, the message is partitioned into blocks
    - each block is encrypted and decrypted separately

Stream Ciphers

- Process message **bit** by **bit** (as a stream)
- Have a **pseudo** random keystream combined (XOR) with plaintext bit by bit
- Randomness of stream key completely destroys statistically properties in message



(b) Stream encryption

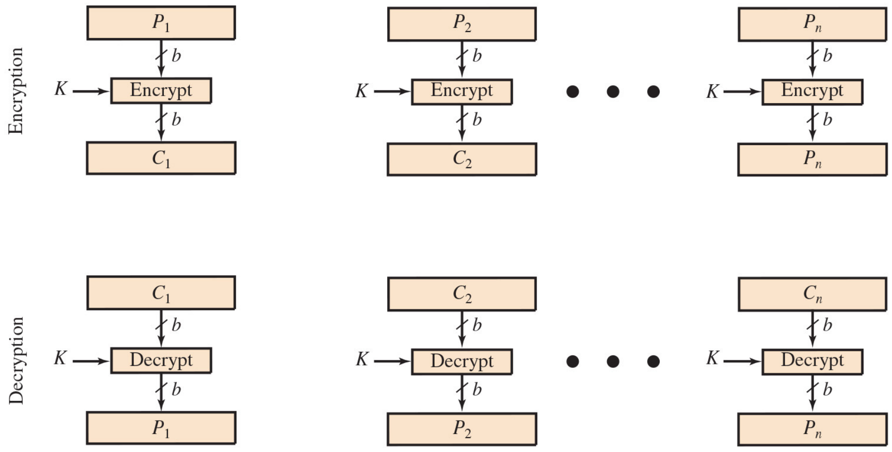
Stream Cipher in Practice

- **RC4** Stream Cipher
  - A variable-key-size stream cipher with byte-oriented operations
  - Used in the SSL/TLS (Secure Sockets Layer/Transport Layer Security) standards (HTTPS)
  - Also used in the WEP (Wired Equivalent Privacy) protocol and the newer Wi-Fi Protected Access (WPA) protocol

- **ChaCha20** Stream Cipher
  - The 20-round version of the ChaCha stream cipher family
  - Uses a pseudorandom round function based on add-X OR-rotate (AXR) operations on an internal state of sixteen 32 bit words arranged as a 4×4 matrix
  - Adopted as a replacement for RC4 in several algorithms

Block Ciphers

- Divide input bit stream into n-bit sections



(a) Block cipher encryption (electronic codebook mode)

- In a good block cipher, each output bit is a function of all n input bits and all k key bits

Block Ciphers

- The algorithm maps an **n-bit plaintext block** to an **n-bit ciphertext block**

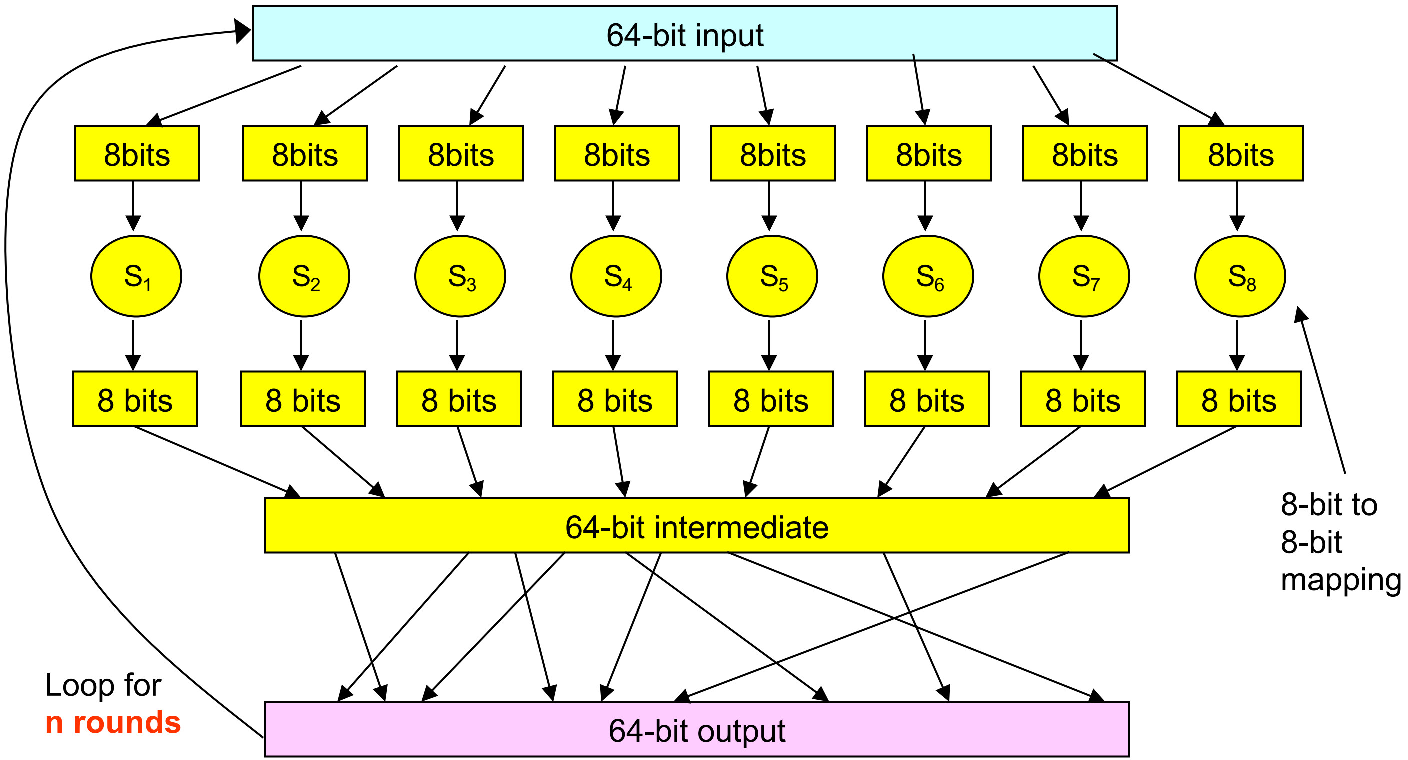
- Often a sequence of permutations and substitutions is used

- A common design for an algorithm is to proceed in iterations
  - one iteration is called a **round**
  - each round consists of similar operations
  - $\mathbf{i}^{th}$ round key $\mathbf{k_i}$ is derived from the secret key **k** using a fixed, public algorithm

Design Principles of Block Ciphers

- Confusion-diffusion paradigm
  - split a block into small chunks
  - define a substitution on each chunk separately (confusion)
  - mix outputs from different chunks by rearranging bits (diffusion)
  - repeat to strengthen the result

Prototype function



Why rounds in prototype?

- If only a single round, then one bit of input affects at most 8 bits of output.
- In 2nd round, the 8 affected bits get scattered and inputted into multiple substitution boxes.
- How many rounds?
  - How many times do you need to shuffle cards
  - Becomes less efficient as n increases

Block Ciphers in Practice

- **Data Encryption Standard (DES)**
  - 64-bit blocks and 56-bit keys
  - Small key space makes exhaustive search attack feasible since late 90s

- **Triple DES (3DES)**
  - Nested application of DES with three different keys KA, KB, and KC
  - Effective key length is 168 bits, making exhaustive search attacks unfeasible

- **Advanced Encryption Standard (AES)**
  - 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
  - Exhaustive search attack not currently possible
  - AES-256 is the symmetric encryption algorithm of choice
    - E.g., CryptoLocker Virus

Data Encryption Standard (DES)

- For many years was the most widely used encryption scheme
  - Referred to as the Data Encryption Algorithm (DEA)
  - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
  - It was expected to be used as a standard for 10-15 years
  - Number of rounds is 16

- Strength concerns:
  - Concerns about the algorithm itself
    - DES is the most studied encryption algorithm in existence
  - Concerns about the use of a 56-bit key
    - The speed of commercial off-the-shelf processors makes this key length woefully inadequate

Attacks on DES

- Brute force attack: try all possible 2^{56} keys
  - time-consuming, but no storage requirements
- Differential cryptanalysis: traces the difference of two messages through each round of the algorithm
  - was discovered in early 90s
  - not effective against DES
- Linear cryptanalysis: tries to find linear approximations to describe DES transformations
  - was discovered in 1993
  - has no practical implication

Brute Force Search Attacks on DES

- It was conjectured in 1970s that a cracker machine could be built for $20 million
- In 1990s RSA Laboratories called several DES challenges
  - Challenge II-2 was solved in 1998 by Electronic Frontier Foundation
    - a DES Cracker machine was built for less than $250,000 and found the key was in 56 hours
  - Challenge III was solved in 1999 by the DES Cracker in cooperation with a worldwide network of 100,000 computers
    - the key was found in 22 hours 15 minutes
    - http://www.distributed.net/des

Increasing Security of DES

- DES uses a 56-bit key and this raised concerns
- One proposed solution is double DES
  - apply DES twice by using two different keys k1 and k2
  - encryption $c = E_{k2}(E_{k1}(m))$
  - decryption $m = D_{k1}(D_{k2}(c))$
- The resulting key is $2 \cdot 56 = 112$ bits, so it should be more secure, right?
  - an attack called meet-in-the-middle discovers keys k1 and k2 with 2^{56} computation and storage
  - better, but not substantially than regular DES

Triple DES (3DES)

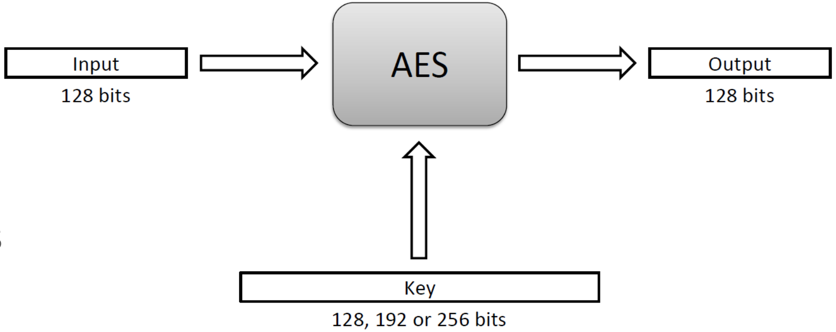
- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
  - 168-bit key length overcomes DES's vulnerability to brute-force attack
  - Underlying encryption algorithm is the same as in DES
  - There is no known practical attack against either version
- Drawbacks:
  - Algorithm is sluggish in software
  - Uses a 64-bit block size

Summary of Attacks on DES

- DES – best attack: brute force search
  - try all possible 2^{56} keys
  - no other requirements
- Double DES
  - best attack: meet-in-the-middle
  - requires 2 plaintext-ciphertext pairs
  - requires 2^{56} space and about 2^{56} work
- Triple DES
  - best practical attack: brute force search

Advanced Encryption Standard (AES)

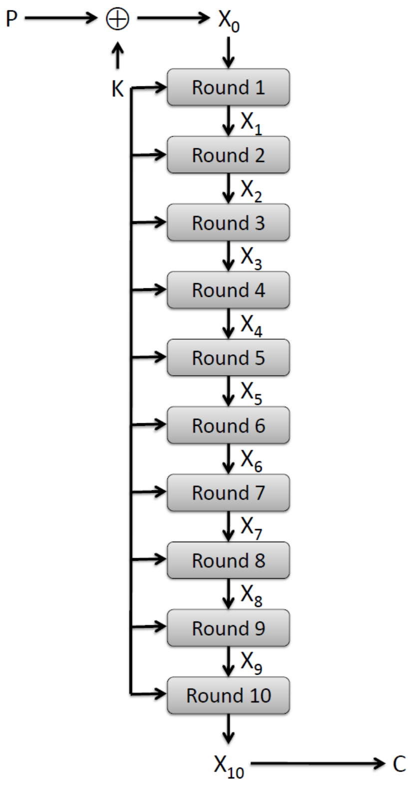
- In 1997 NIST made a formal call for an unclassified publicly disclosed encryption algorithm available worldwide and royalty-free
  - the goal was to replace DES with a new standard called AES
  - the algorithm must be a symmetric block cipher
  - the algorithm must support (at a minimum) 128-bit blocks and key sizes of 128, 192, and 256 bits
- The evaluation criteria were:
  - security
  - speed and memory requirements
  - algorithm and implementation characteristics



AES Round Structure

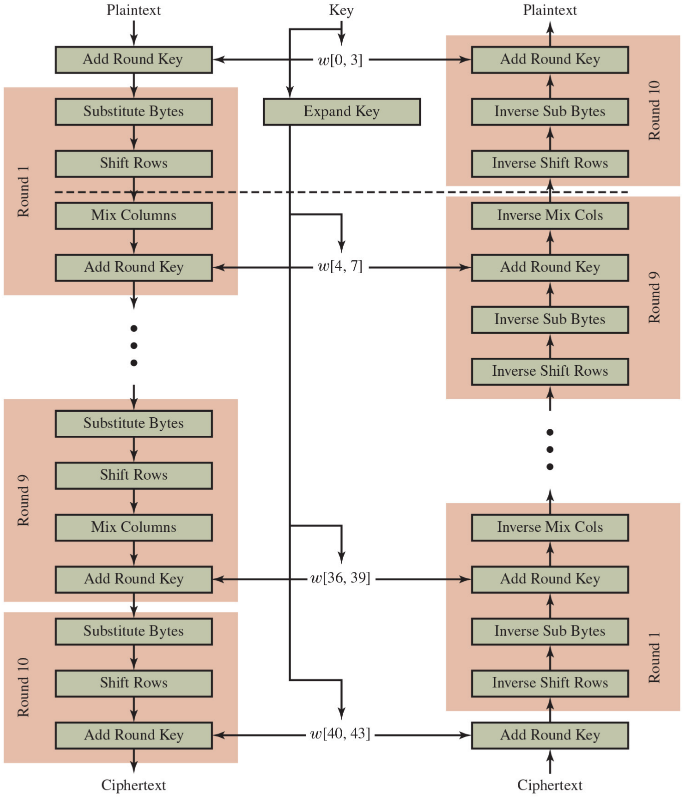
- The 128-bit version of the AES encryption algorithm proceeds in ten rounds.
- Each round performs an invertible transformation on a 128-bit array, called **state**.
- The initial state X_0 is the XOR of the plaintext P with the key K:

  X_0 = P XOR K.
- Round i (i = 1, …, 10) receives state X_{i-1} as input and produces state X_i.
- The ciphertext C is the output of the final round: C = X_{10}.



AES Rounds

- Each round is built from four basic steps:
  1. **SubBytes step**: an S-box substitution step
  2. **ShiftRows step**: a permutation step
  3. **MixColumns step**: a matrix multiplication step
  4. **AddRoundKey step**: an XOR step with a **round key** derived from the 128-bit encryption key



(a) Encryption
(b) Decryption

AES

- simple design but resistant to known attacks
- very efficient on a variety of platforms including 8-bit and 64-bit platforms
- highly parallelizable
- had the highest throughput in hardware among all AES candidates
- well suited for restricted-space environments (very low RAM and ROM requirements)
- optimized for encryption (decryption is slower)

Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions / μs	Time Required at 10^{13} decryptions / μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191}\ \mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255}\ \mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

Symmetric Key Cryptography

- So far we've covered:
  - what secure symmetric encryption is
  - high-level design of stream ciphers
  - high-level design of block ciphers
  - DES
  - AES
- Next, we'll talk about:
  - **block** cipher encryption modes and limitations