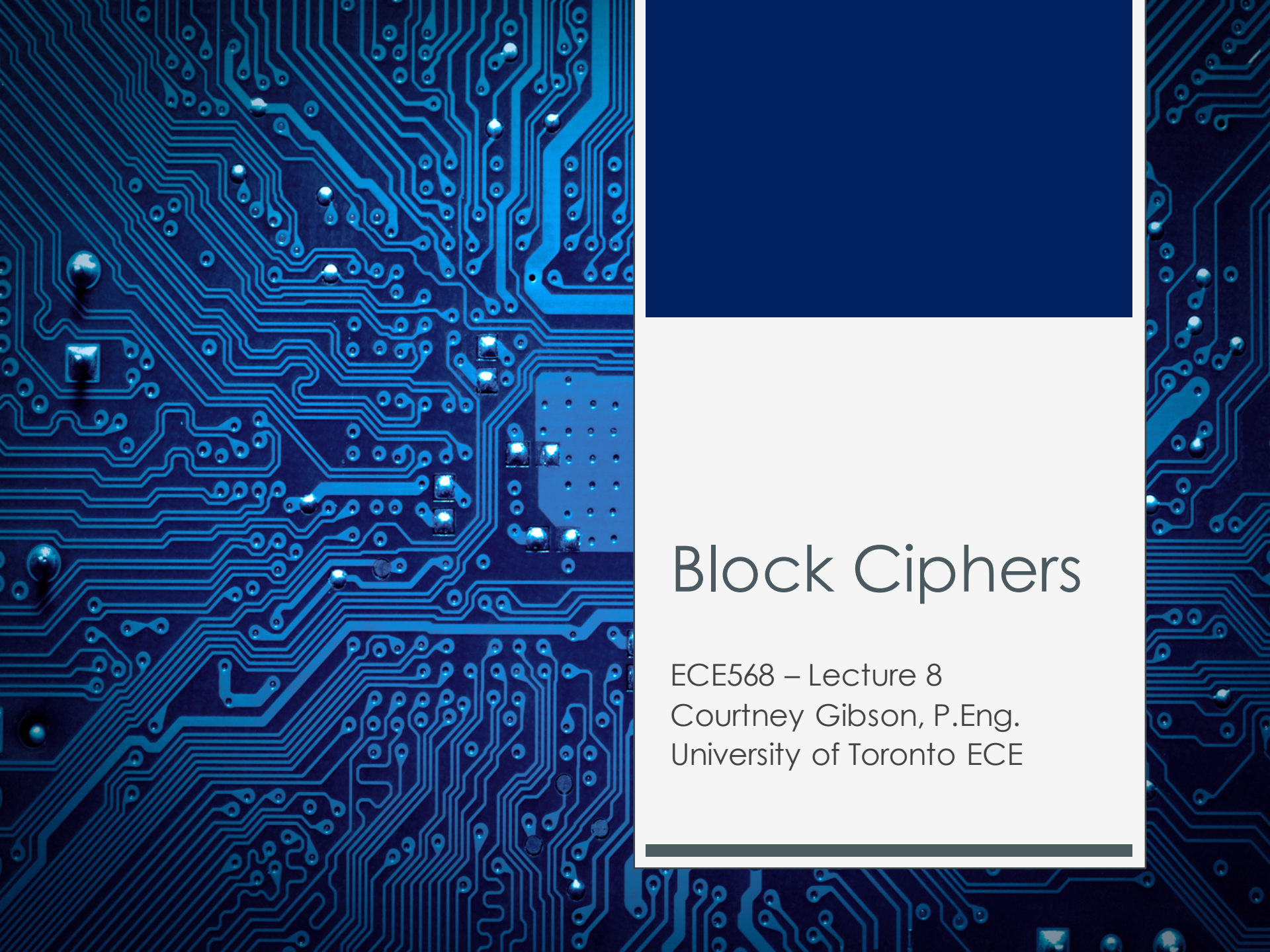


Block Ciphers

ECE568 – Lecture 8

Courtney Gibson, P.Eng.
University of Toronto ECE

Outline

Block Cipher Design

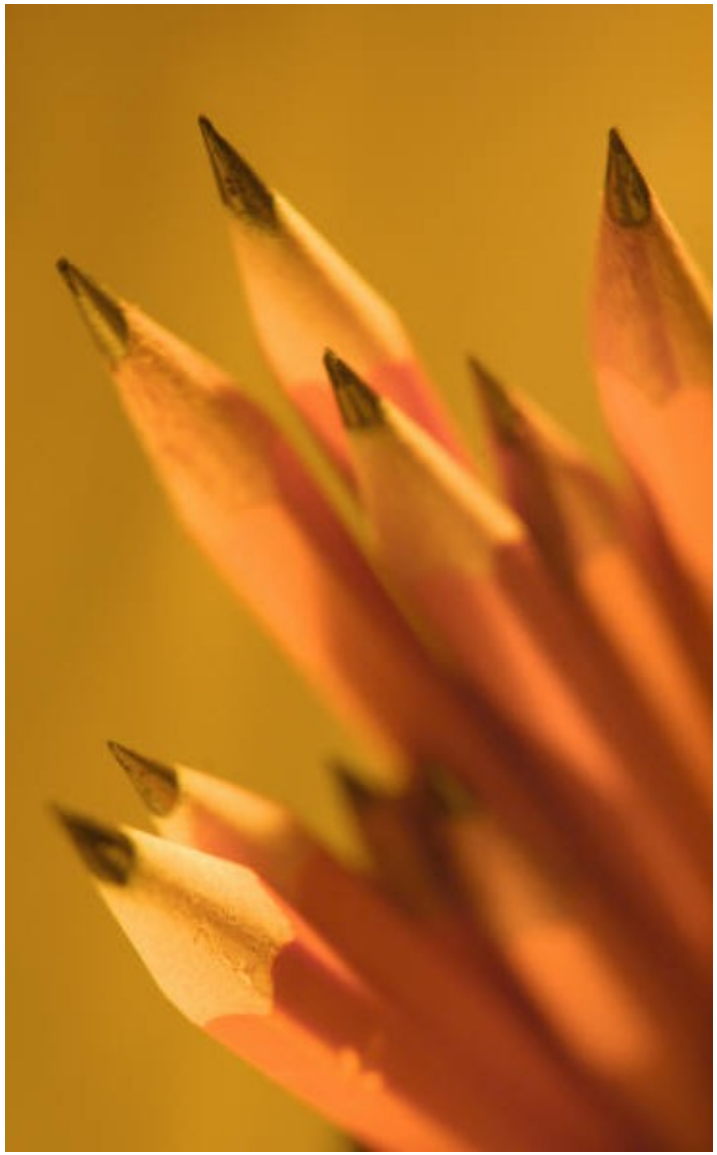
- Design goals
- Substitution, Transposition Ciphers

Common Block Ciphers

- DES
- AES

Block Cipher Encryption Modes

- ECB
- CBC
- Others



Block Cipher Design

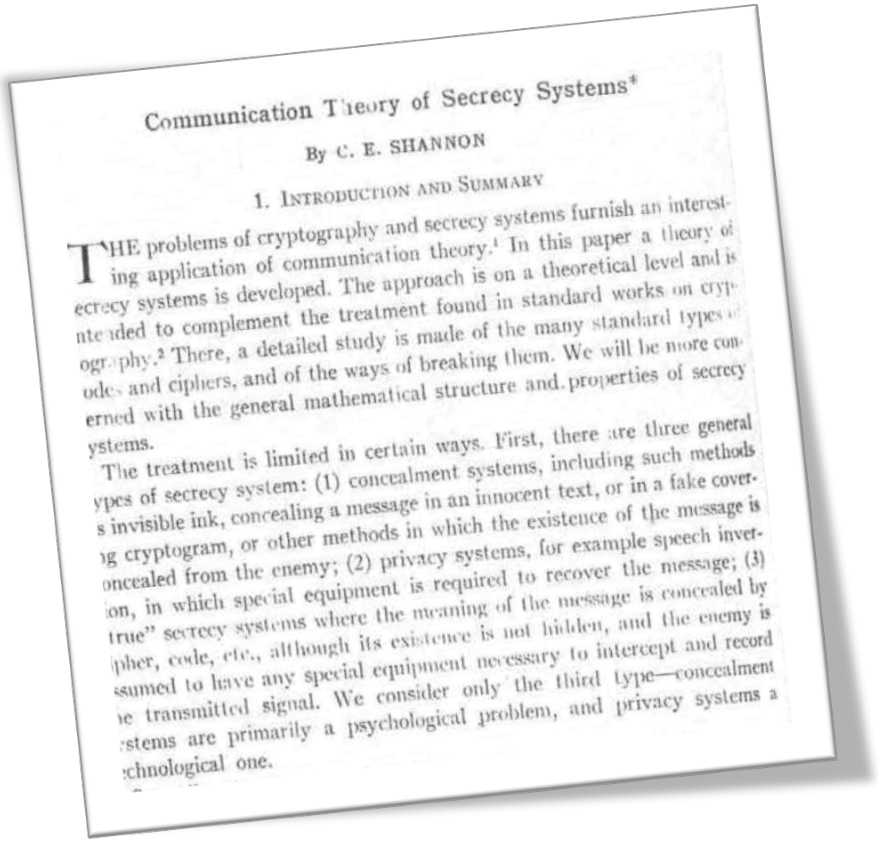
Confusion, diffusion, substitution, transposition, iterated block cipher, SP-network

Desirable Properties

Claude Shannon's 1949 paper, *Communication Theory of Secrecy Systems*, lays out much of the foundation for modern cryptography.

In it, he proposes two desirable goals for a good cryptosystem: **confusion** and **diffusion**.

A good block cipher uses both techniques.



Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. Introduction and Summary

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake cover- ing cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.

Properties: Confusion

Confusion: obscuring of the relationship between the plaintext and the ciphertext

- Primary goal is to make statistical analysis difficult, even if the attacker has a large number of known plaintext/ciphertext pairs
- Encoding should be **non-linear**:

$$E_k(M_1 + M_2) \neq E_k(M1) + E_k(M_2)$$

- Each character of the ciphertext should depend on the entire key

Properties: Diffusion

Diffusion: spreading the influence of individual plaintext characters over much of the ciphertext

- Each output bit is affected by many input bits
- Ideally, flipping a single bit of either the key or the plaintext should change half the output bits (*i.e.*, the probability of bit_i flipping is 0.5 for any value of i)
- Repetitive patterns in plaintext are spread over the entire ciphertext, thus hiding statistical information about the plaintext

Block Cipher Design

Two simple ciphers, each quite weak on their own, are often employed to design secure block ciphers:

- A **substitution cipher** replaces characters in the plaintext with other characters from the same alphabet, with a one-to-one mapping (confusion)
- A **permutation cipher** transposes the plaintext characters (diffusion)

An **iterated block cipher** repeatedly applies these two ciphers in different combinations

Substitution-Permutation Network

Many currently-used algorithms combine several rounds of simple substitution and permutation in a form of iterated block cipher, called an **SP-network** (SPN)

- Keys are typically applied by XOR'ing input/output of each stage

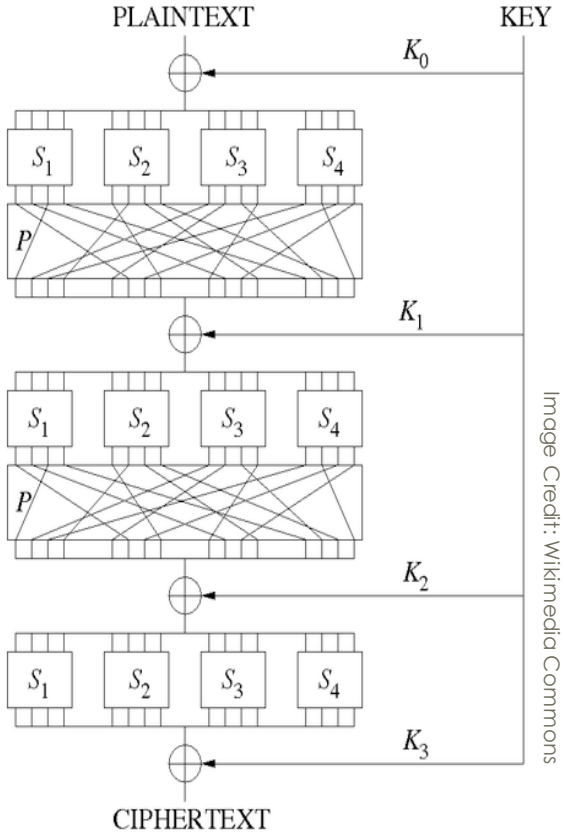


Image Credit: Wikimedia Commons

Common Block Ciphers

AES, DES, 3DES

Common Block Ciphers

The two most common block ciphers presently in public use are those specified by the National Institute of Standards and Technology (NIST):

- **DES:** Data Encryption Standard
- **AES:** Advanced Encryption Standard

- AES replaced DES as the official standard encryption algorithm in 2000
- Both are iterated block ciphers
- Many others exist but we will focus on these two

History: DES

Non-military encryption in the early 70's relied on poorly standardized and often proprietary systems

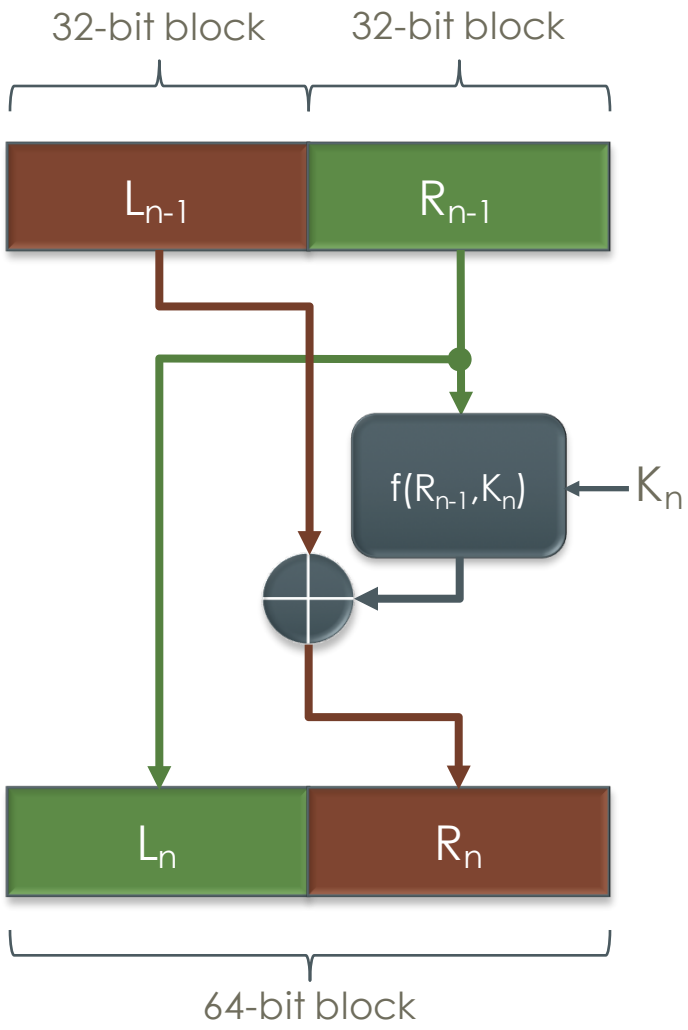
- NIST made an effort to standardize encryption with a reliably strong, well-studied cipher
  - IBM produced a candidate, based on the Lucifer cipher, which eventually won the DES competition in Nov. 1976
  - The standard provided strong security, good performance
  - Easy to implement
  - Could be used in a variety of applications
- Evaluated and pronounced secure by the NSA
  - The involvement of the NSA created much distrust and speculation at the time, has since been mostly allayed
- DES uses a 56 bit key, a block length of 64 bits
  - Now considered insecure for many applications, because of the short key length
  - NIST certification has been withdrawn

Structure of DES

DES uses a structure known as a **Feistel Network**. The network consists of sixteen rounds:

- In each round, the input is split into a left half L, and a right half R
- The two halves are switched, and some computation modifies half of the input bits
- Each round includes computation with a portion of the key (a **subkey** K_n)

The output of one round becomes the input for the next



Subkey Generation

The 56-bit key is put through a key schedule to create sixteen subkeys (K_n), one for each round:

- The 56-bit key is split into two 28-bit halves
- Each half is shifted left by 1 or 2 bits (depending on the round)
- 24-bits are selected from each of the 28-bit halves to make a 48-bit subkey (K_n)

Exact number of shifts and bit selections have been carefully selected

- The constants used to pick selections are based on a random distribution
- Specific details are available in any good crypto reference (see end of these slides)

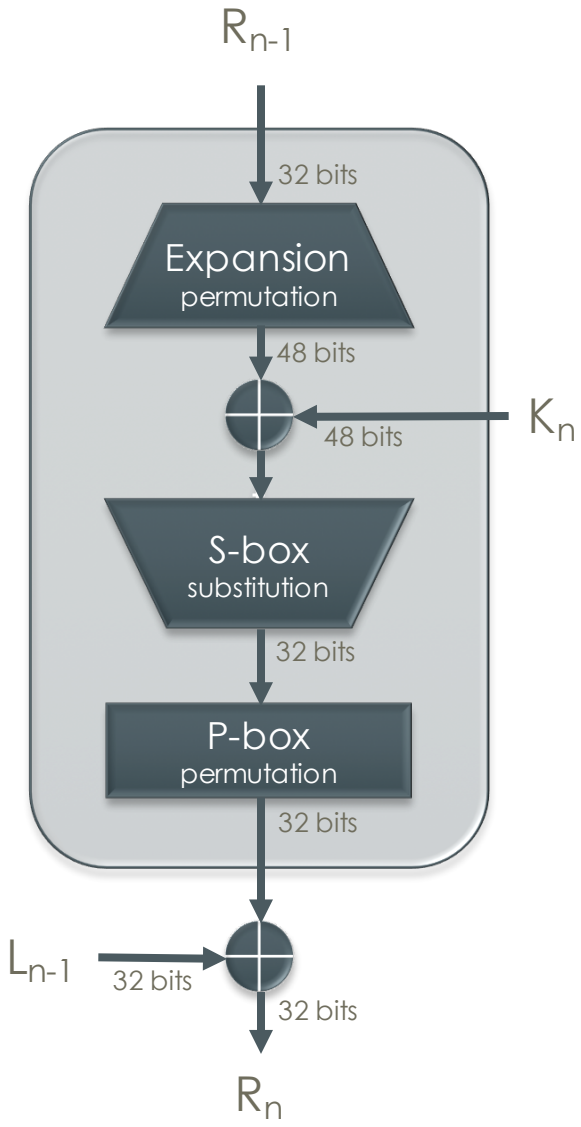
DES Computation

Each f(R_{n-1},K_n) contains:

- Expansion permutation of 32-bit input (R_{n-1}) into 48 bits
- XOR with a 48-bit subkey (K_n)
- S-box substitution boxes that compress 48-bits into 32-bit output
- Permutation of 32-bit output

Design of the S-boxes is very important as this is the only non-linear element in the cipher

- Selected by the NSA using an unknown method



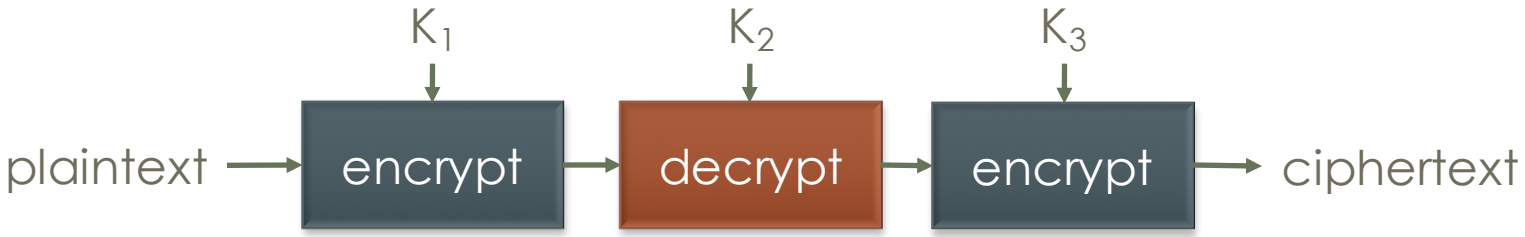
3DES

The main problem with DES is that its 56-bit key has become inadequate

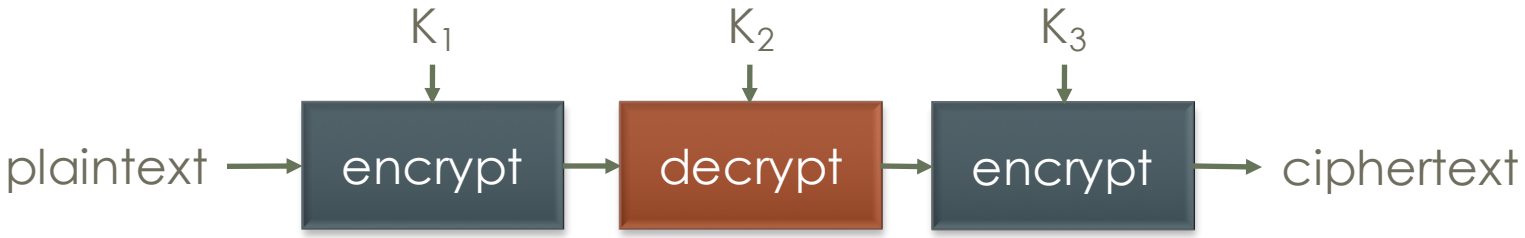
- With powerful computers, it has become realistic to use a brute force attack (*i.e.*, try all 2^{56} key combinations) to decrypt ciphertext without knowing the key in less than a day

One solution is to use a longer key length and chain the DES algorithm together multiple times

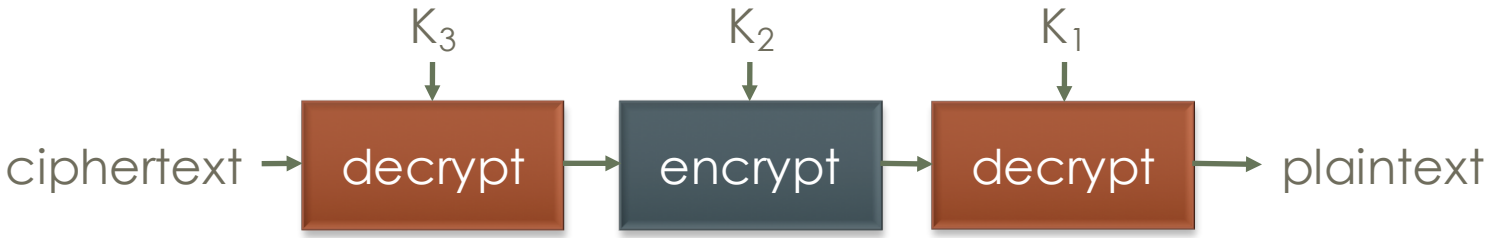
- Remaining applications that use DES use **3DES** (triple-DES), splitting a 168-bit key into three 56-bit parts, and running the algorithm three times



3DES



$$ciphertext = E_{K3}(D_{K2}(E_{K1}(plaintext)))$$



$$plaintext = D_{K1}(E_{K2}(D_{K3}(ciphertext)))$$

History: AES

In January 1997, NIST ran a competition to replace DES, which was 20 years old at the time. The requirements for AES were:

- Symmetric block cipher
- Its workings would be defined/known publically
- Increasing key length should be possible
- Easily implementable in hardware and software
- Freely available

After rigorous testing, **Rijndael** (created by Joan Daemen and Vincent Rijmen) was selected as the winner and designated the Advanced Encryption Standard (AES) cipher.

- Currently approved under Federal Information Processing Standard (FIPS) for Top Secret data

AES

Supports variable key and block lengths:

- Can use 128-, 192- or 256-bit keys
- Can operate on 128-, 192- or 256-bit blocks
- Any combination of key and block length is possible
- Extensions exist to allow it to take block and key lengths of 160 and 224 bits

Each input block is used to form a matrix of bytes:

- The matrix always has 4 rows, and a variable number of columns, depending on block size
  - *e.g.*, 128-bit (16-byte) block uses a 4x4 matrix
- Operations in GF(2) finite field, with 2 elements (0, 1)
  - Addition is XOR, multiplication is AND
- This matrix is called the **state**

AES Computation

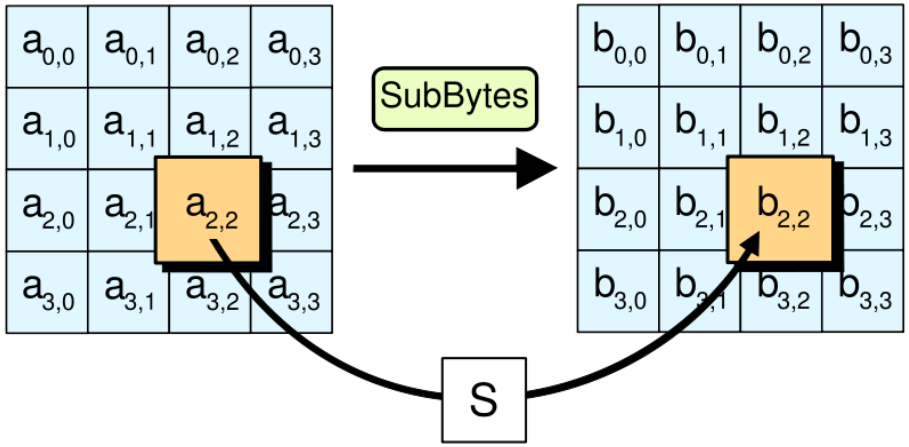
Like DES, AES is based on rounds

- The number of rounds is based on the key length and block size (varies from 10-14)
- Each round consists of four stages:
  - **Byte Substitution** transformation
  - **Shift Rows** transformation
  - **Mix Columns** transformation
  - Addition of **Round Keys**

AES: Byte Substitution

A **non-linear substitution** step that replaces each byte with another

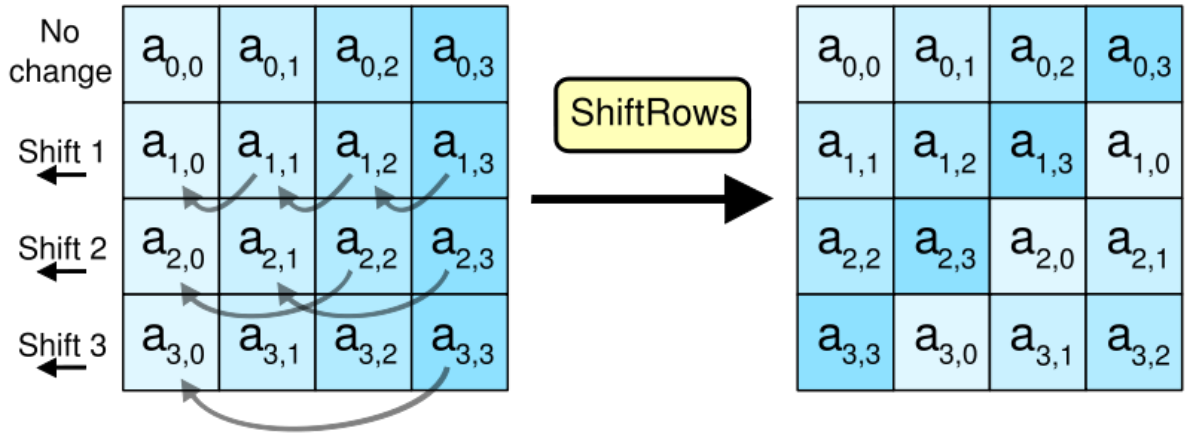
- Substitution is performed using a 256-entry lookup table called an S-box (8-bit input produces 8-bit output) with a fixed, one-to-one mapping
- Substitution uses a known good non-linear function
  - Prevents attacks based on simple algebraic properties



AES: Shift Rows

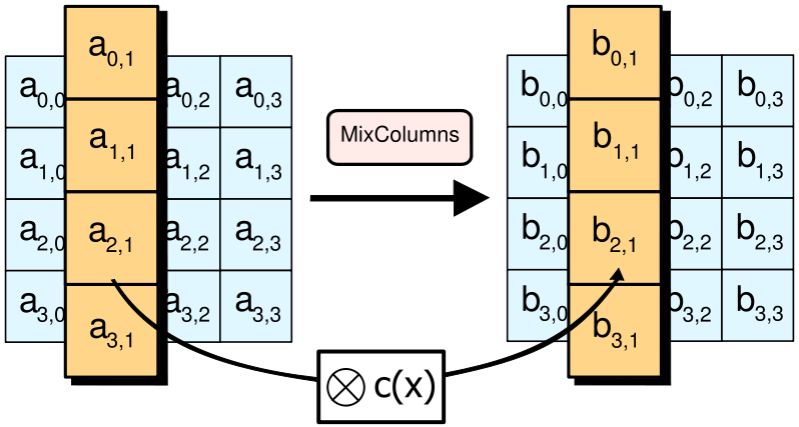
This stage operates on the rows of the state and **cyclically shifts** the bytes in each row by an offset

- A column of the output state of this step consists of bytes from each column of the input state
- Larger blocks have slightly different offsets



AES: Mix Columns

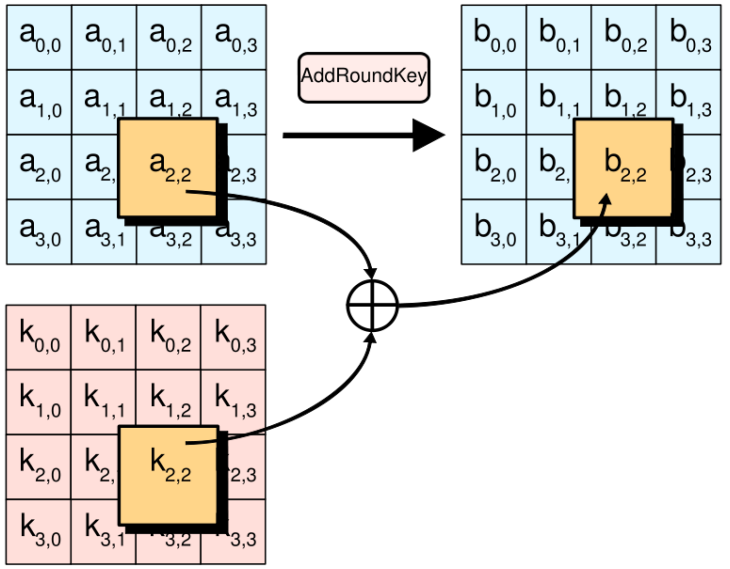
- Each column in the state is treated as a vector and the following matrix is applied to **mix the elements** of each column
- The previous two steps provide diffusion in the cipher



$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

AES: Round Keys

- Round keys are generated from the original key (Ki)for each round via a key schedule algorithm, similar to DES
- The **round key is XORed with the state** to produce the input to the next round



AES: Review

- Each input block is used to form a matrix of bytes
- Each round consists of 4 stages
  - **Byte Substitution:** byte-by-byte substitution (only non-linear transformation)
  - **Shift Rows:** each row in the state is shifted by an offset
  - **Mix Columns:** The elements of a column are mixed amongst each other
  - **Round Keys:** The round key is XOR'ed in
- Notable differences over DES:
  - S-boxes selection was not random: based on a mathematical function
  - Shift values and number of rounds are both based on the key size and block size

AES Today

- AES became effective as a standard May 26, 2002
- Today, AES is one of the most popular block cipher algorithms, available in many different encryption packages
- AES is the first publicly accessible and open cipher approved by the NSA for Top Secret information

Block Cipher Encryption Modes

ECB, CBC, CFB, OFB

Block Cipher Encryption Modes

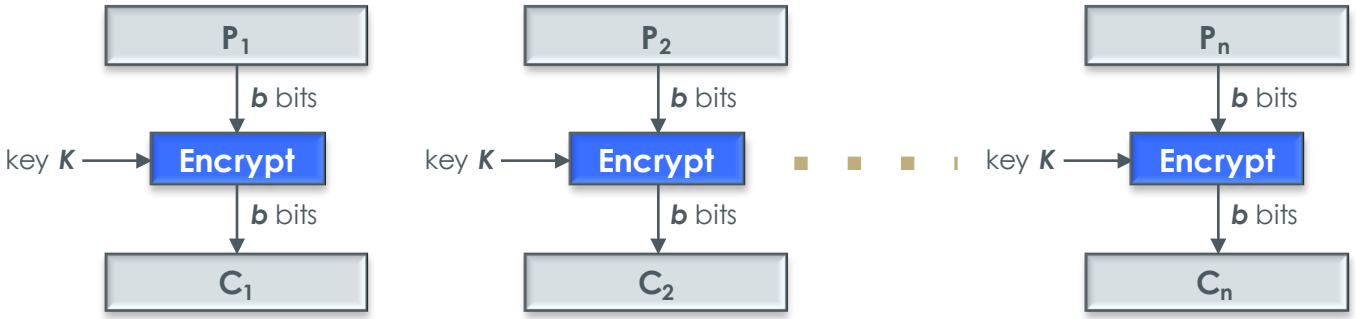
Block ciphers are often used to encrypt data consisting of multiple blocks

- How can multiple blocks be encrypted safely?
- There are several algorithms available and they are measured on the following criteria
  - **Security:** What are the security properties?
  - **Performance:** What throughput can be supported?
  - **Error Propagation:** What is the effect of a bit error during transmission of the cipher text?
  - **Error Recovery:** Can we recover from a transmission error? Does an error affect all blocks, or can we continue decryption? How much data has to be retransmitted?

Electronic Codebook (ECB)

ECB is the simplest mode:

- The message is broken into block-sized chunks
- Padding is added to the last block
- Each chunk is encrypted independently

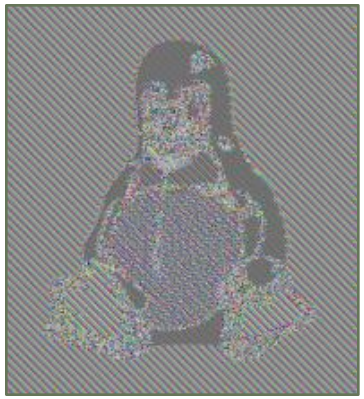


ECB Performance

Highly-parallelizable, but its security is poor:

- An adversary can add, delete or reorder blocks
- Plaintext blocks always encrypt to the same ciphertext blocks: the ciphertext can reveal macro-structure of the plaintext data

Original



ECB Mode

More Secure

Image Source: Wikimedia Commons

ECB Properties

Error Propagation

- Any transmission errors in the ciphertext will only affect the corresponding plaintext block
- The plaintext block will be changed completely randomly

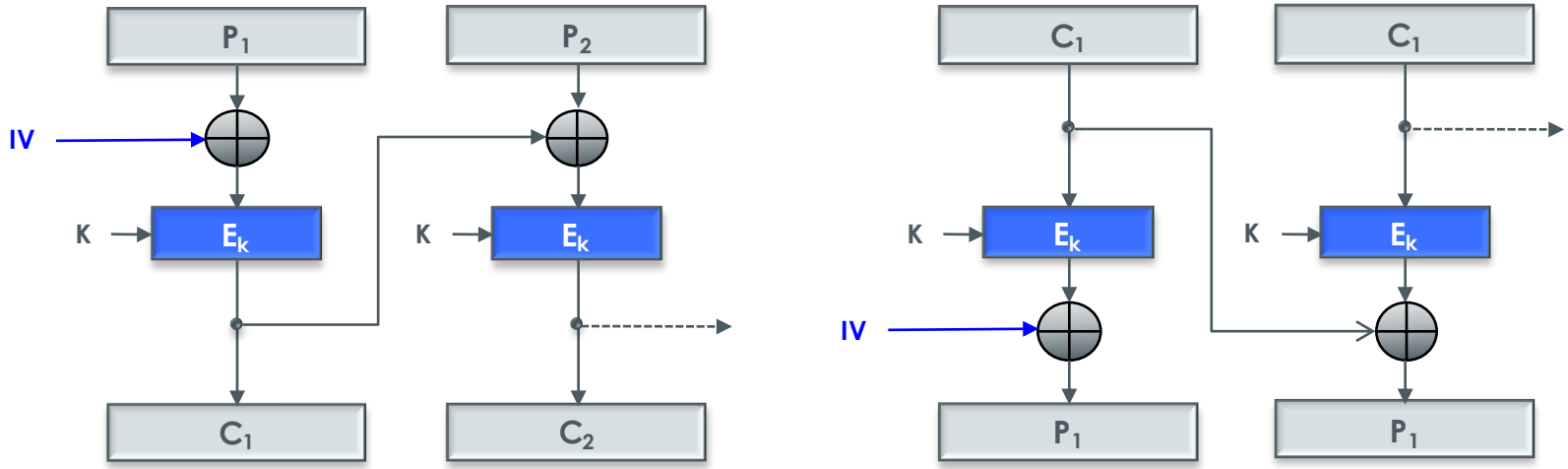
Error Recovery

- Recovery is easy
- The error is only limited to the affected block, all blocks before and afterwards will be decrypted properly
- Only retransmit affected blocks
- Does not stop decryption, just skip the bad blocks

Cipher Block Chaining (CBC)

An alternate mode, CBC makes every blocks' input dependent on the cipher text (output) of the previous block

- Initial Value (IV) does not have to be secret, but shouldn't be reused for multiple messages



CBC Performance

Security

- Cipher Block Chaining has good security
- Any change in the plaintext affects all later blocks
- Different blocks with the same input plaintext have different output ciphertext
- A modification to a ciphertext block affects at most two blocks during decryption

Performance

- No parallelism for encryption: must be sequential
- Decryption can be parallelized

CBC Properties

Error Propagation

- A transmission error only affects the current block and the following block

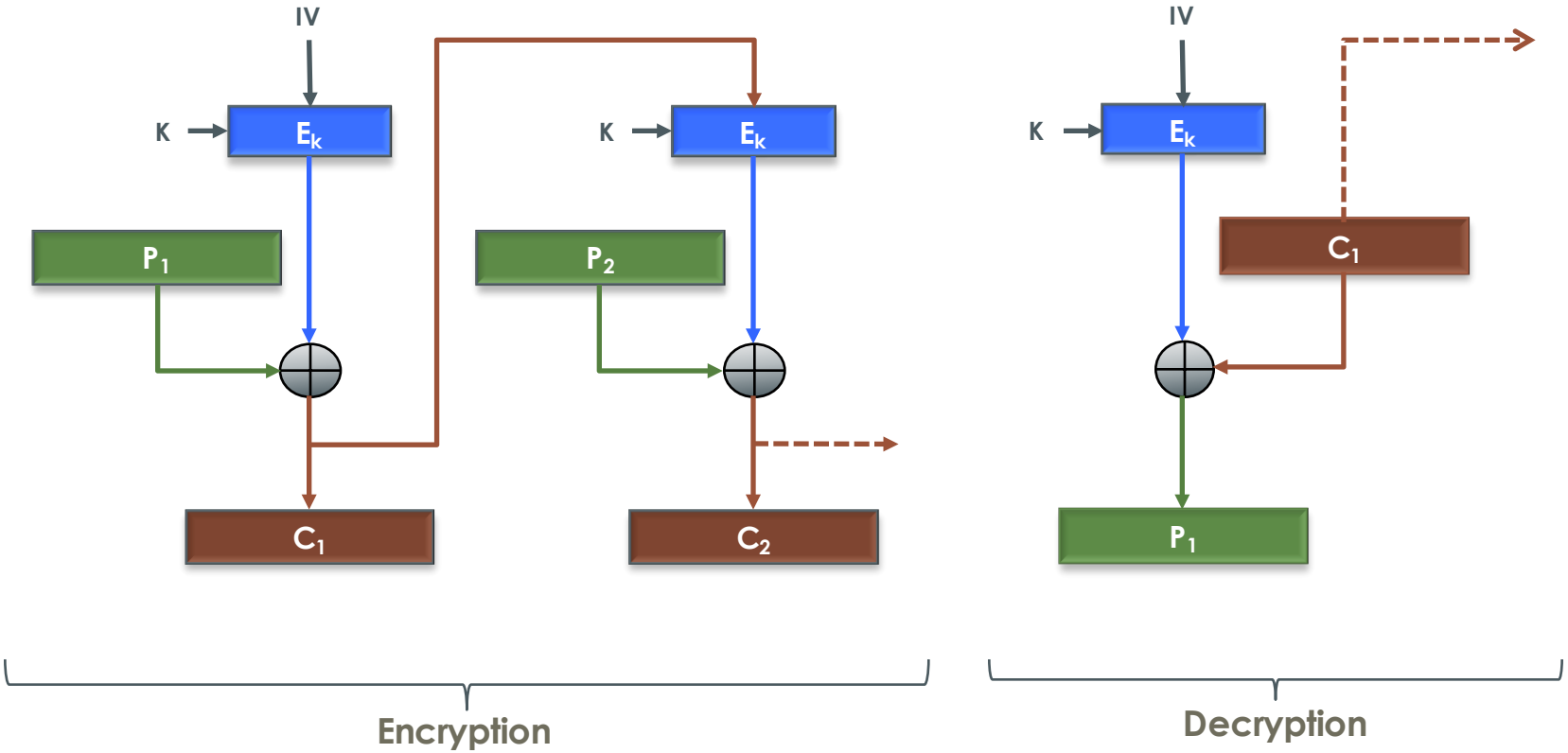
Error Recovery

- The receiver can drop the affected blocks and still continue decryption

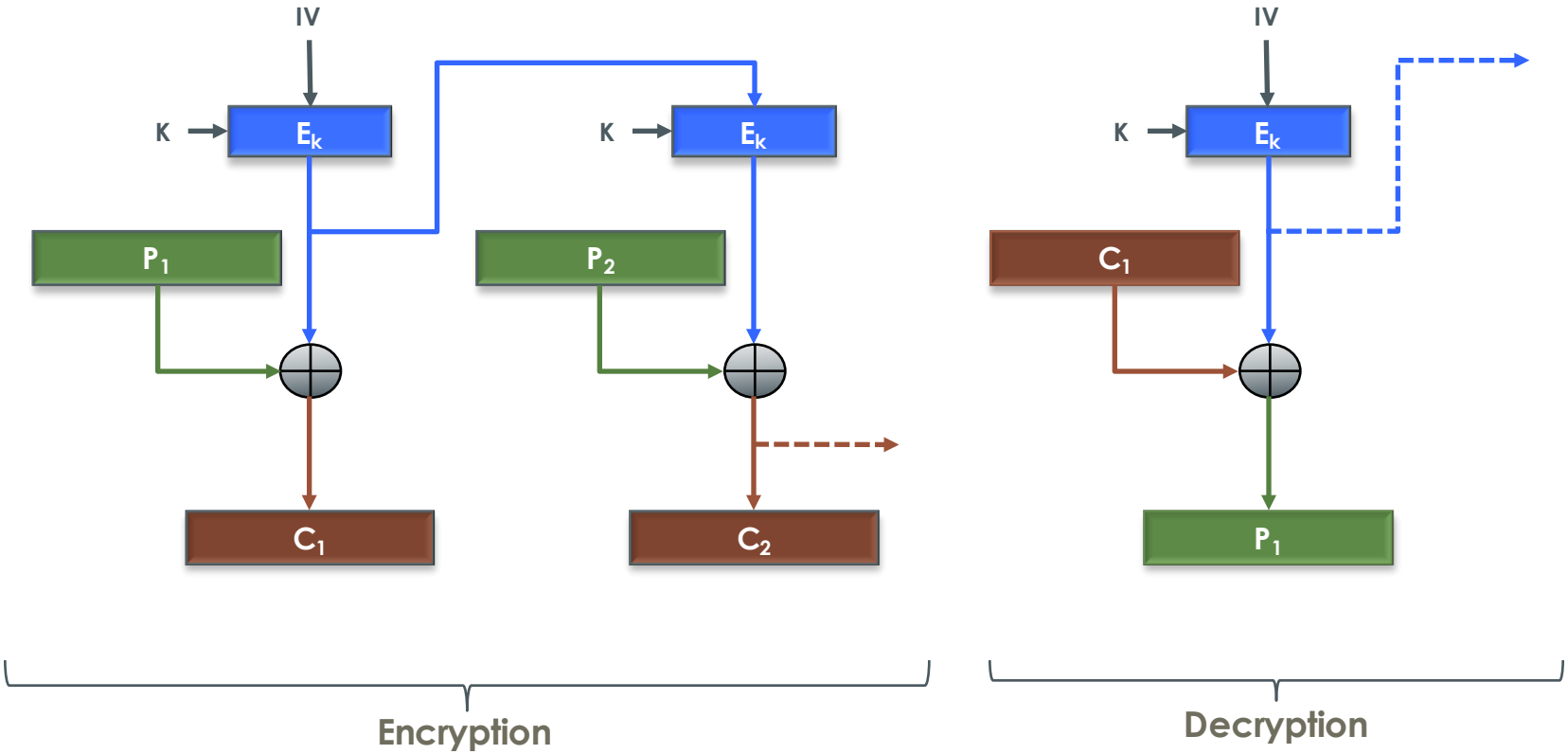
Other Modes: CFB, OFB

CFB (Cipher Feedback) mode and **OFB** (Output Feedback) mode allow encryption and decryption in units of less than a full block at a time (*i.e.*, they convert block ciphers into stream ciphers)

Cipher Feedback (CFB)



Output Feedback (OFB)



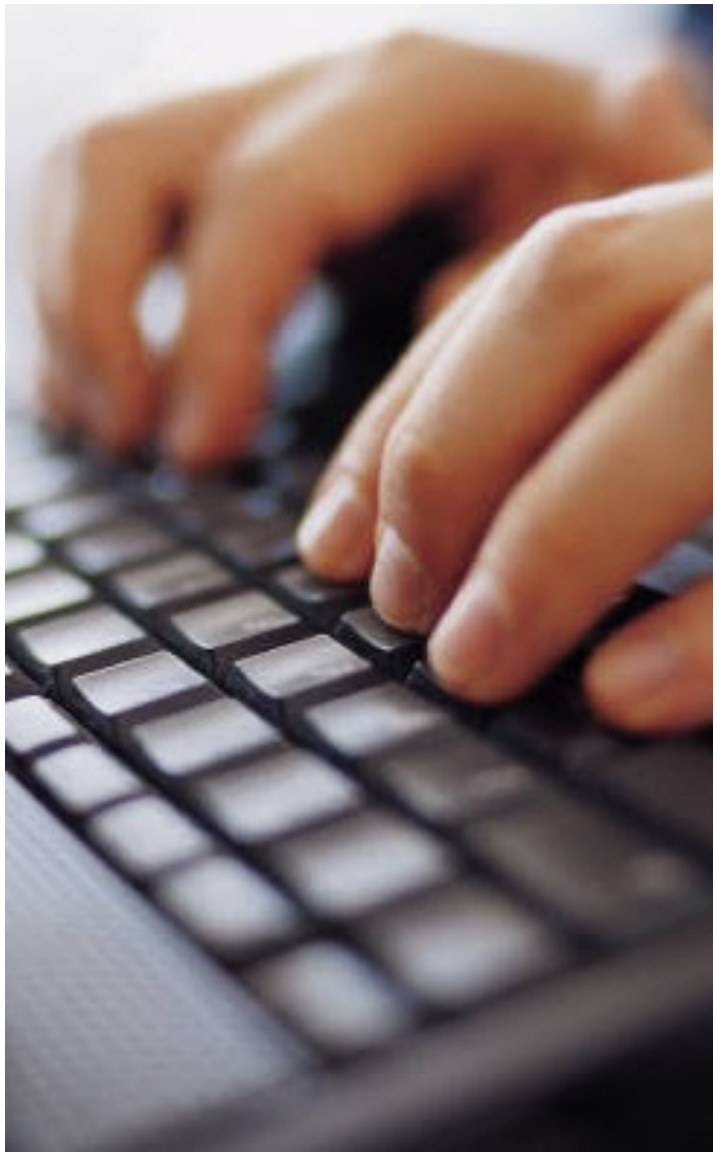
CFB and OFB Properties

- Cipher Feedback and Output Feedback modes have security, error propagation and recovery properties similar to those of stream ciphers
  - Discussed in the next slidepack
- They are slightly more efficient because no padding is necessary
- In CFB, pipelining is possible
- In OFB, the key stream is independent of the plaintext: allows performing the cipher operations in advance (speeding up encryption and decryption), and easily supports error correction coding

Other Modes

A number of other commonly-used modes exist: ciphertext stealing (XTS), etc..

Adds some algorithm complexity: beyond what we are covering in this course.



Summary


TrueCrypt Volume Creation Wizard
TRUECRYPT
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
?
< Prev
Next >
Cancel

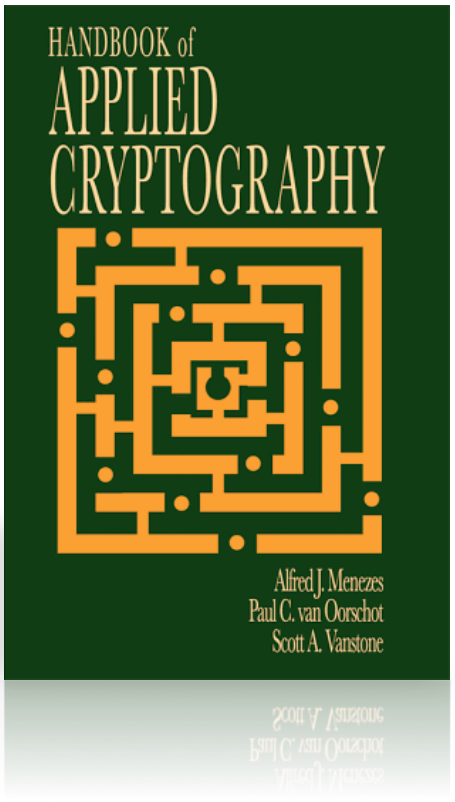
Further Reading

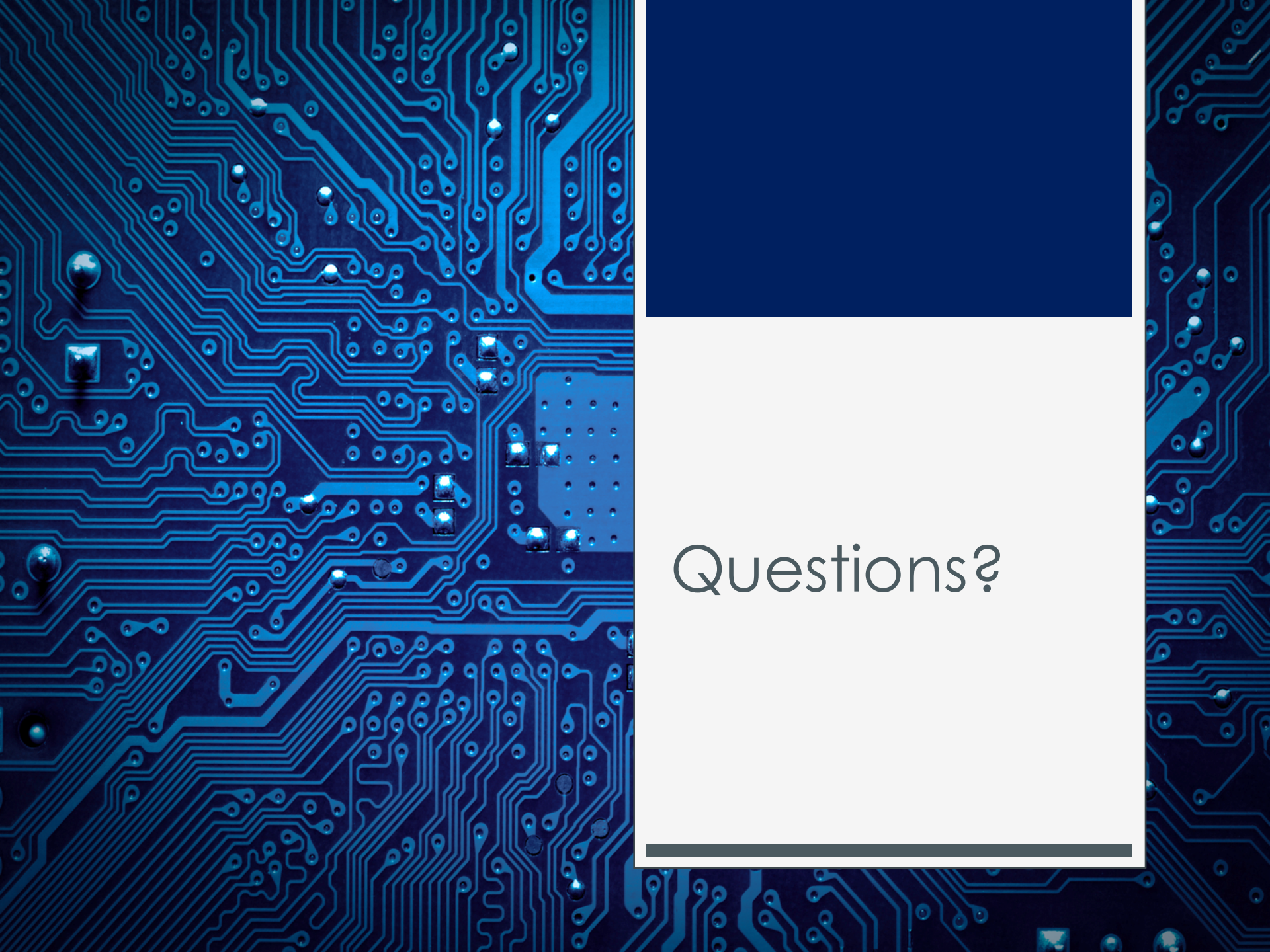
Handbook of Applied Cryptography (5th edition)

Menezes, Oorschot, Vanstone

Available as a free download:

www.cacr.math.uwaterloo.ca/hac




Questions?