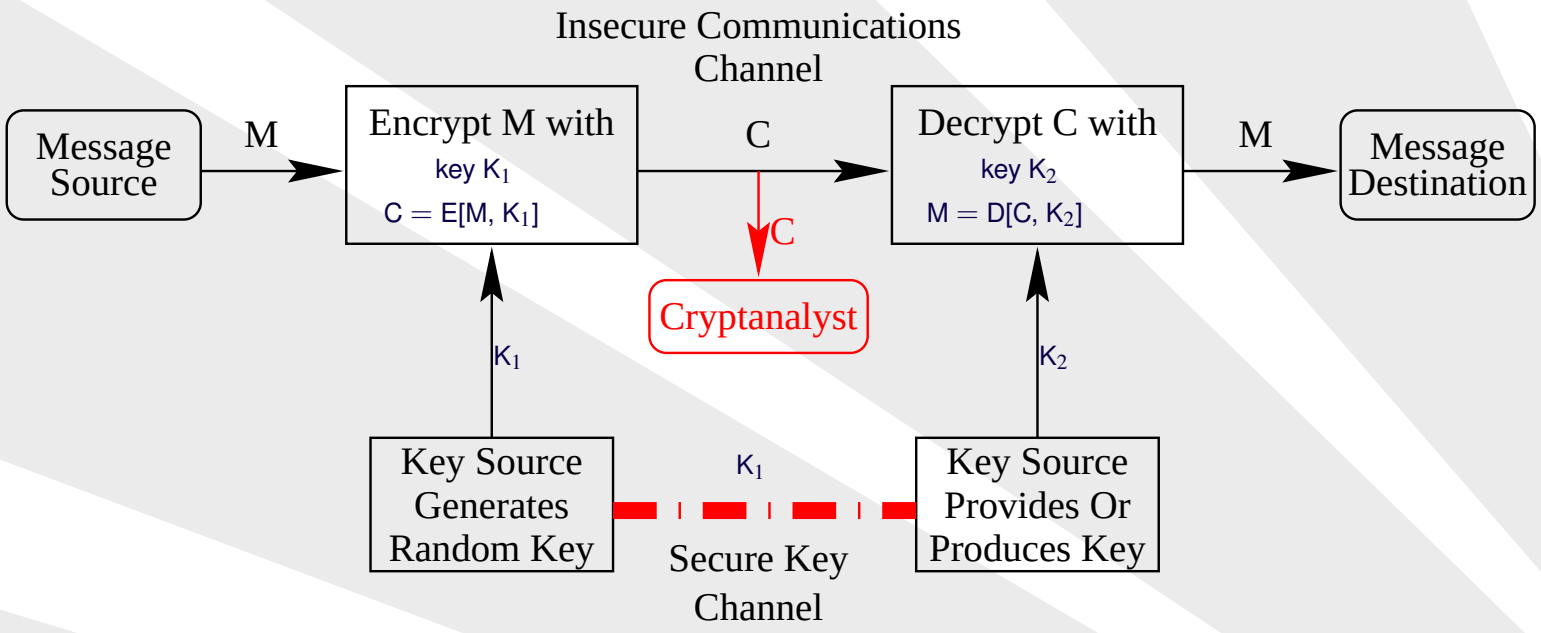
CS 556 – Computer Security
Spring 2018

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

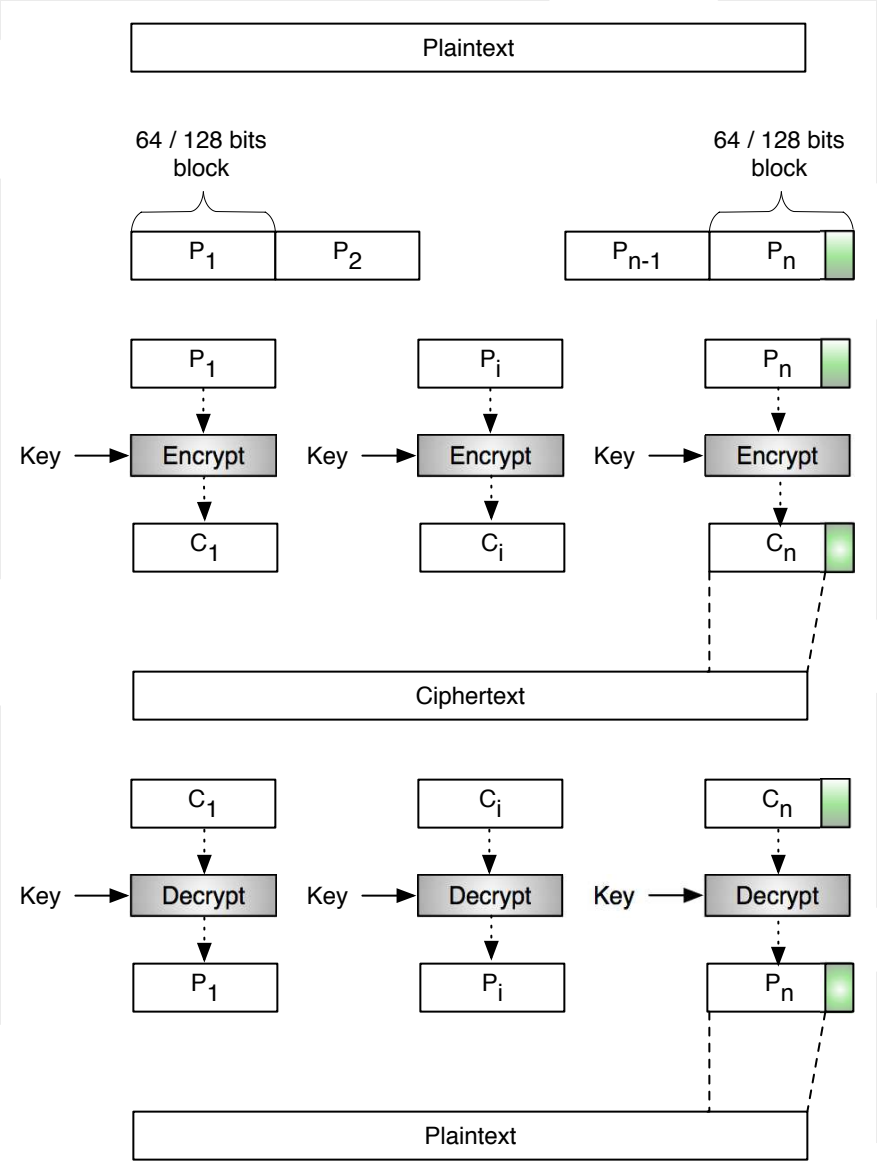
Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA

Secret Key Cryptosystems

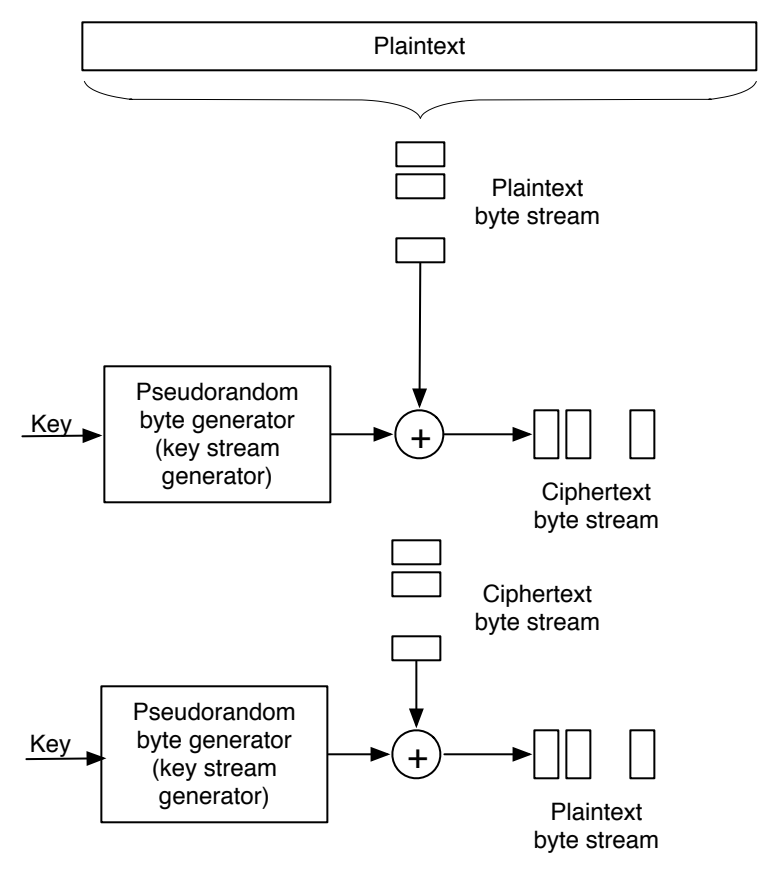
Secret Key Cryptosystem



Block Ciphers vs. Stream Ciphers (1)



Block Cipher vs. Stream Ciphers (2)



Basic Secret-Key Techniques

- Substitution
- Permutation or transposition
  - Reverse Cipher
  - Column Transposition
  - Rail Fence
  - Scytale Cipher
  - Nihilist Cipher
- Combination and iterations of these - Product ciphers

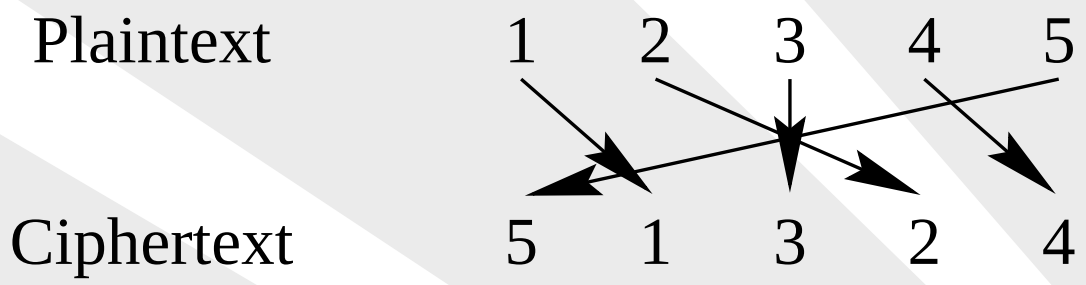
Simple Ciphers

Simple Alphabetic Substitution

Plaintext ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext PZQSGIMBWXDFKJVCHAOLUTERYN

- Also called Caesar cipher
- Huge key space: $26! \gg 10^{26}$
- Trivially broken for known plaintext attacks
- Easily broken for ciphertext only attacks (for natural language plaintext)
- Multiple encipherment does not help (no point in doing two substitutions in sequence)

Simple Permutation



- Key space N! for block size N
- Trivially broken for known plaintext attack
- Easily broken for ciphertext only attack (for natural language plaintext)
- Multiple encipherment does not help

Reverse Cipher

- Reverse the order of the letters in a message
  - Plaintext – ICAMEISAWICONQUERED
  - Ciphertext – DERDUQNOCIWASIEMACI

Column Transposition

1	2	3	4	5	6	7
l	a	s	e	f	b	e
a	m	s	c	a	n	b
e	m	o	d	u	l	a
t	e	d	t	o	c	a
r	r	y	m	o	r	e
i	n	t	e	l	l	i
g	e	n	c	e	t	h
a	n	r	a	d	i	o
w	a	v	e	s	q	x

Key; 4523617

Ciphertext:

ecdtm ecaef auool edsam
merne nasso dytnr vbnlc
rltiq laetr igawe baaei
hox

Rail Fence Cipher

- Write the message alternating letters in two rows
- Write the ciphertext from the rows

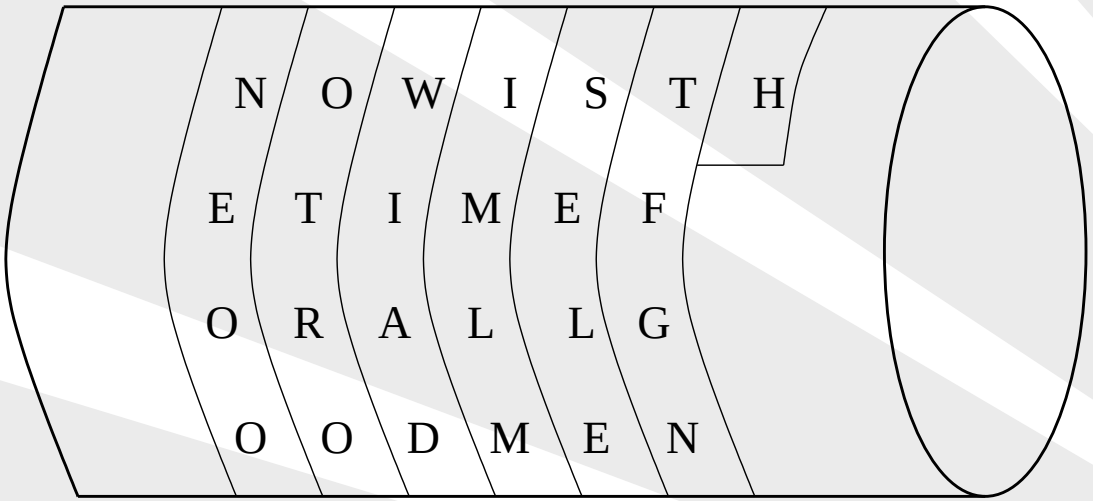
Plaintext

N		W		S		H		T		M		F		R		L		G		O		M		N
	O		I		T		E		I		E		O		A		L		O		D		E	

Ciphertext NWSHTMFRLGOMNOITEIEOALODE

Scytale Cipher

- A strip of paper was wound round a staff; message written along staff in rows; then paper removed leaving a strip of seemingly random letters



Ciphertext: NEOOOTROWIADIMLMSELETFGNH

Nihilist Cipher

- Combines row and column transposition
- Write message in rows in order controlled by key, read off by rows

Plaintext: NOWISTHETIMEFORALLGOODMEN

Key 2 1 3 5 4

	2	1	3	5	4
2	H	T	E	I	T
1	O	N	W	S	I
3	E	M	F	R	O
5	D	O	M	N	E
4	L	A	L	O	G

Ciphertext: HTEIT ONWSI EMFRO DOMNE LALOG

Stronger Ciphers

Product Ciphers

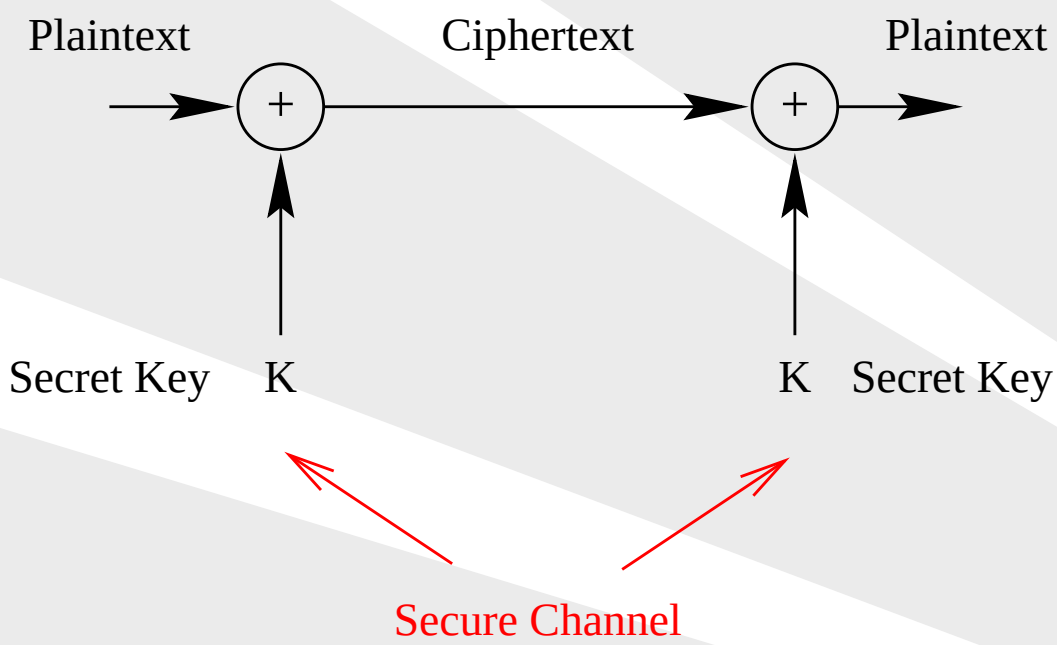
- Substitution followed by permutation followed by substitution followed by permutation ...
- Best known example is DES (Data Encryption Standard)
- Mathematics to design strong product cipher is classified

Product Ciphers - (cont'd)

- For known plaintext/ chosen plaintext/ chosen ciphertext, breakable by exhaustive search of key space
- Therefore security is based on - computational complexity of computing the key under these scenarios
  - size of the key

Vernam One-time Pad

Perfect Secrecy



A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Perfect Secrecy

- The Vernam one-time pad is the ultimate cipher, but impractical for most situations
- Requires a random key longer than the message
- The key cannot be reused
- Known plaintext reveals the portion of the key that has been used, but does not reveal anything about the future bits of the key

Data Encryption Standard

DES

- DES is a product cipher with 56 bit key and 64 bit block size for plaintext and ciphertext
- Developed by IBM and adopted by NIST (FIPS publication 46) with NSA approval, for unclassified information
- E and D are public, but the design principles are classified
- Has some four weak keys for which E[E[M, K], K] $=$ M that are identified as part of the standard and should not be used
- Has twelve semi-weak keys which comes in pairs K_1 and K_2 for which E[E[M, K_1], K_2] $=$ M

DES

- Has stood up remarkably well against 15 years of public cryptanalysis
- Adopted as ANSI DEA (Data Encryption Algorithm)
- Considered by ISO as a standard but abandoned due to concern that it may become too widespread and an enticing target for cryptanalysis

DES History

- 1977 Approved as Federal standard with 5 year cycle of recertification
- 1987 Reluctantly approved for 5 years
- 1993 Approved for another 5 years
- 1998 Re-examined and called for replacement
- 1999 DES re-affirmed for use till replacement found; preferred mode Triple DES
- 2001 Advanced Encryption Standard (FIPS 197) announced to replace DES
- 2005 DES withdrawn as national standard

DES Controversies

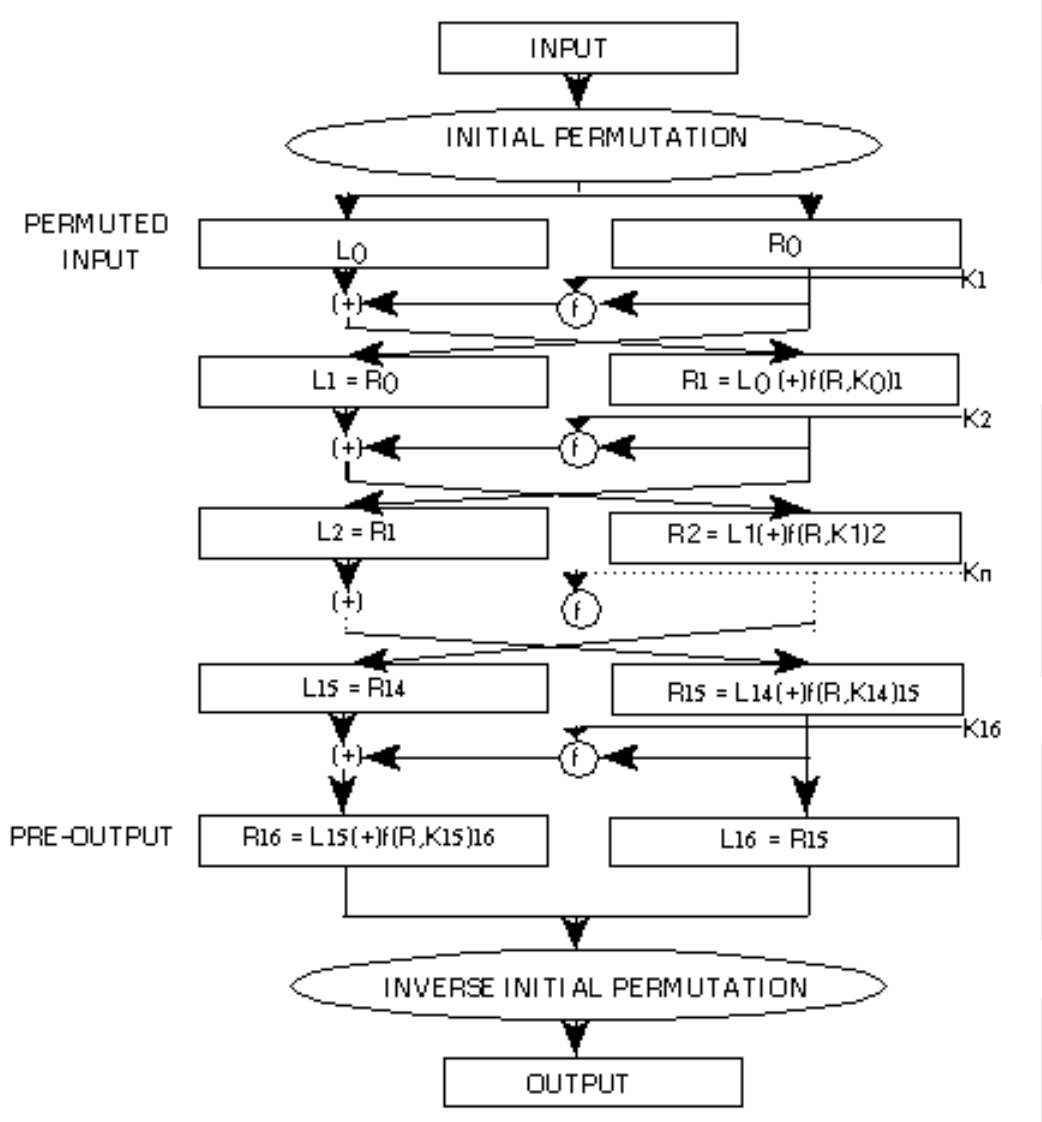
- Allegations of built in trapdoors have never been substantiated
  - The US Senate Select Committee on Intelligence exonerated the NSA from tampering with the design of DES in any way
- Major weakness is key size of 56 bits (on the threshold of allowing exhaustive search for known plaintext attacks)
  - Broken in 22 hours in 1999 by distributing the computing over the Internet (EFF's Deep Crack and distributed.net)
  - Broken in 1 day by FPGA based parallel machine in 2008
  - Main reason for replacement

DES Design

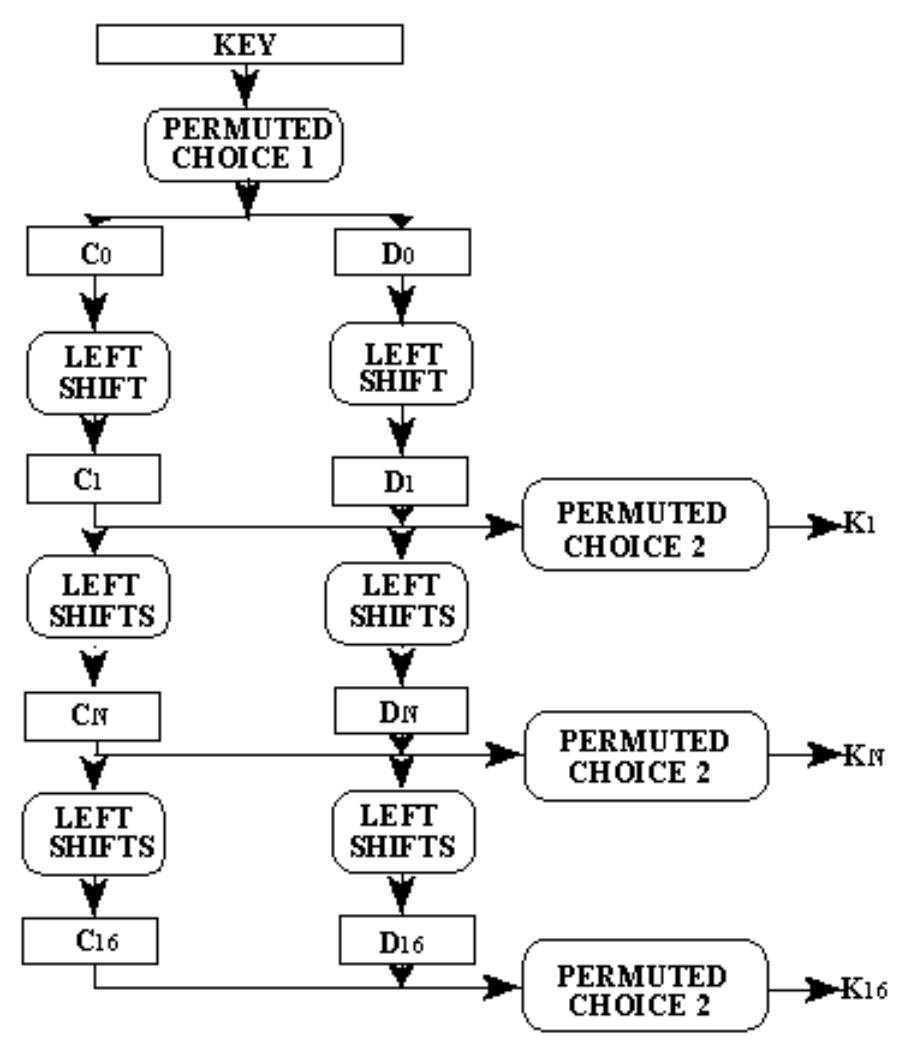
Overview

- The basic process in enciphering a 64-bit data block using the DES consists of:
  - an initial permutation (IP)
  - 16 rounds of a complex key dependent calculation (f)
  - a final permutation, being the inverse of IP

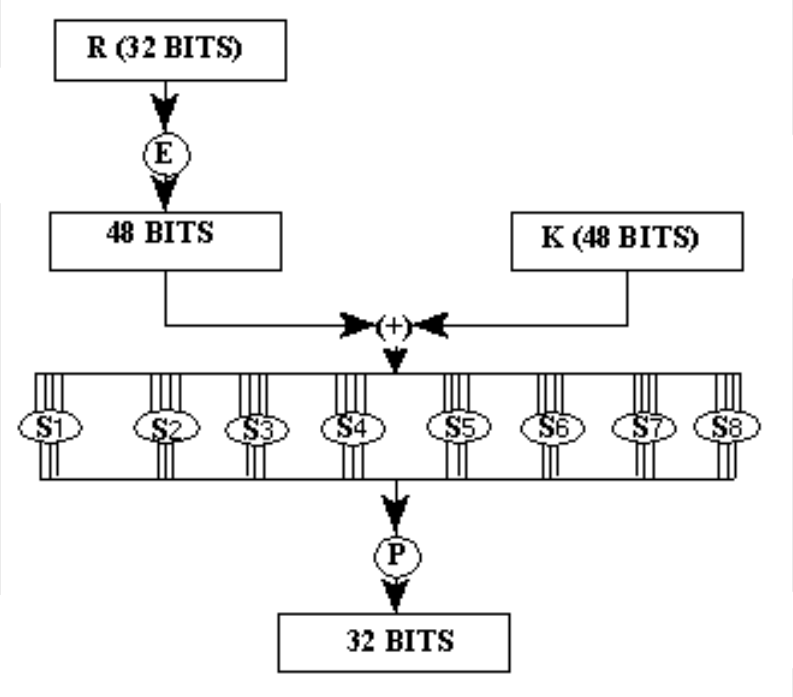
Overview



DES - Selecting Subkeys



DES Encryption - The f function



Breaking DES

DES Known Plaintext Attack

- 56 bit key can be broken on average in $2^{55} = 3.6 \times 10^{16}$ trials

trials / second	time required
1	10^9 years
10^3	10^6 years
10^6	10^3 years
10^9	1 year
10^{12}	10 hours

DES Known Plaintext Attacks

- Fastest DES chips can do close to 1 million encryptions per second
- A million chips in parallel can give us 10^{12} trials per second
- Estimated cost of such a special purpose machine is in 10's of millions of dollars at most, comparable to the most expensive supercomputers

DES Known Plaintext Attack

- Compare the numbers for a 76 bit key which can be broken on average in 2^{75} trials

trials / second	time required
1	10^{15} years
10^3	10^{12} years
10^6	10^9 years
10^9	10^6 years
10^{12}	10^3 years

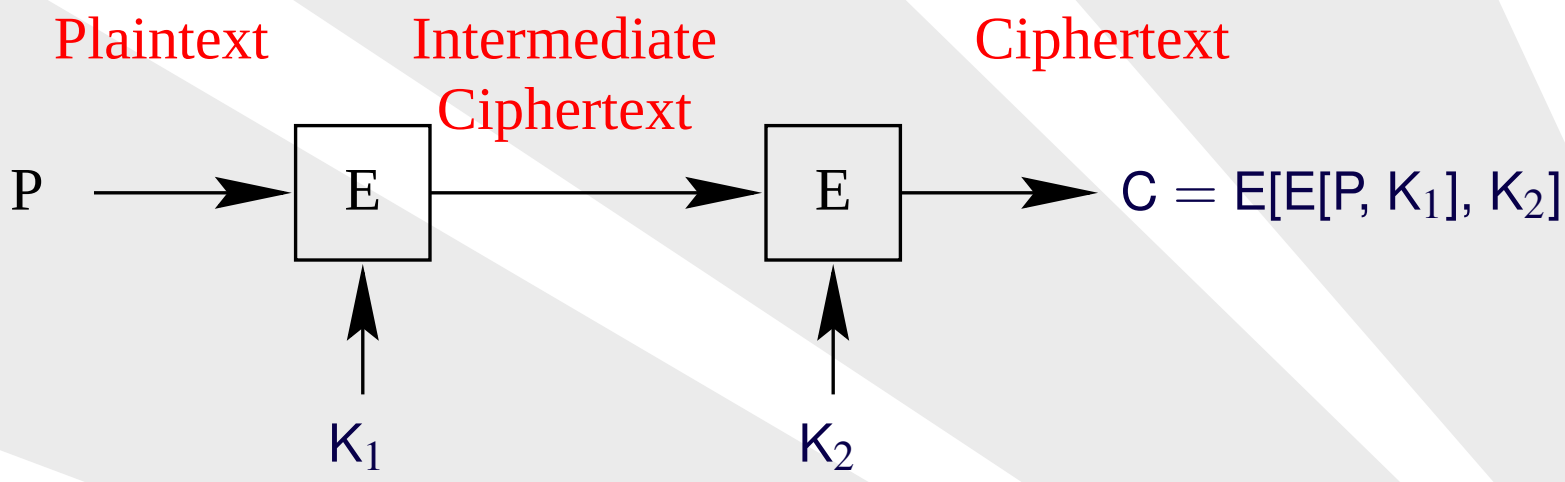
DES Chosen Ciphertext Attack

- Biham and Shamir have shown that differential cryptanalysis can break DES in 2^{48} trials - within the capabilities of the most powerful workstations
- Differential cryptanalysis requires vast amounts of chosen ciphertext and is not very practical (2^{47} pairs)
- DES-like ciphers with larger keys should also be susceptible to such attacks

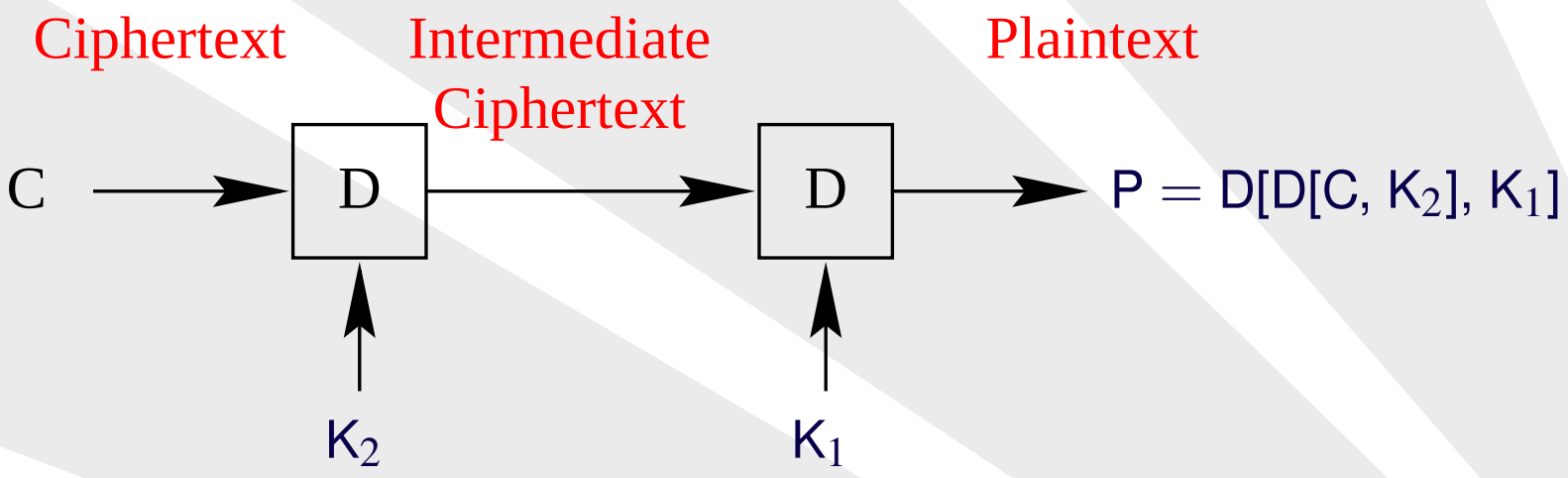
DES Multiple Encipherment

- In 1992 it was shown that DES is not a group.
  - That is there is no K such that $E[M, K] = E[E[M, K_1], K_2]$
  - So multiple encryption should be effective in giving a stronger cipher
    - However, this is not the case

DES Multiple Encipherment



DES Multiple Encipherment



Double DES - Attack

- Only as strong as DES with a 57 bit key and not a 112 bit key
  - Known plaintext meet-in-the-middle attack

Double DES Meet-in-the-Middle Attack

- Note that $C = E[E[P, K_1], K_2]$; then we have $X = E[P, K_1] = D[C, K_2]$
- The attack starts with a known pair (P, C)
- Step 1: Encrypt P for all 2^{56} possible values of K_1. Store these results (that is the X values) in a table and then sort the table by the values of X

The Meet-in-the-Middle Attack

- Step 2: Decrypt C using all possible 2^{56} values of K_2 . As each decryption is produced, check the result against the table (of X values) for a match.
- If a match occurs then test the two resulting keys against a new known plaintext-ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct key.

The Attack - Analysis

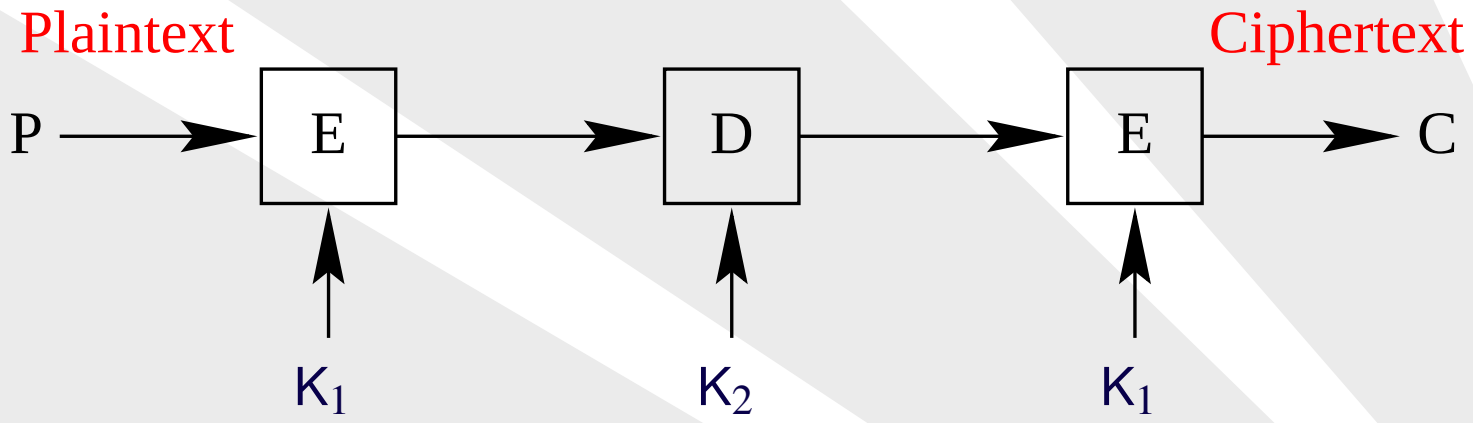
- For any given 64 bit plaintext P, there are 2^{64} ciphertext values that could be produced by double DES
- Double DES has a 112 bit key size - so in effect there are 2^{112} possible key values
- Therefore, on an average, for a given plaintext, the number of different 112 bit keys that will produce a given ciphertext is $2^{112}/2^{64} = 2^{48}$

Analysis (continued)

- Thus, the attack will produce about 2^{48} false alarms on the first (P, C) pair.
- A similar argument states that with an additional (P, C) pair the false alarm rate is reduced to $2^{48}/2^{64} = 2^{-16}$
  - that is if the attacks is performed on two blocks of known (P, C) pair the probability of the attack succeeding is $1 - 2^{-16} \approx 1$

DES Triple Encryption

Triple DES



Triple DES

- Technique suggested by Tuchman to avoid the vulnerability in double DES.
  - If $K_2 = K_1$, this amounts to a single encryption which is convenient
- Tuchman's technique is not part of the NIST standard; however adopted as ANSI X9.52 standard
- Can be broken in 2^{56} operations if one has 2^{56} chosen plaintext blocks
  - Could use distinct K_1, K_2, K_3
- Triple DES variant uses three consecutive encryption

Beyond DES

CCEP

- CCEP = Commercial COMSEC Endorsement Program
- Provide NSA designed secret crypto algorithms as black boxes which cannot be reverse engineered, and will be manufactured by selected vendors

CCEP – Type 1 and Type 2

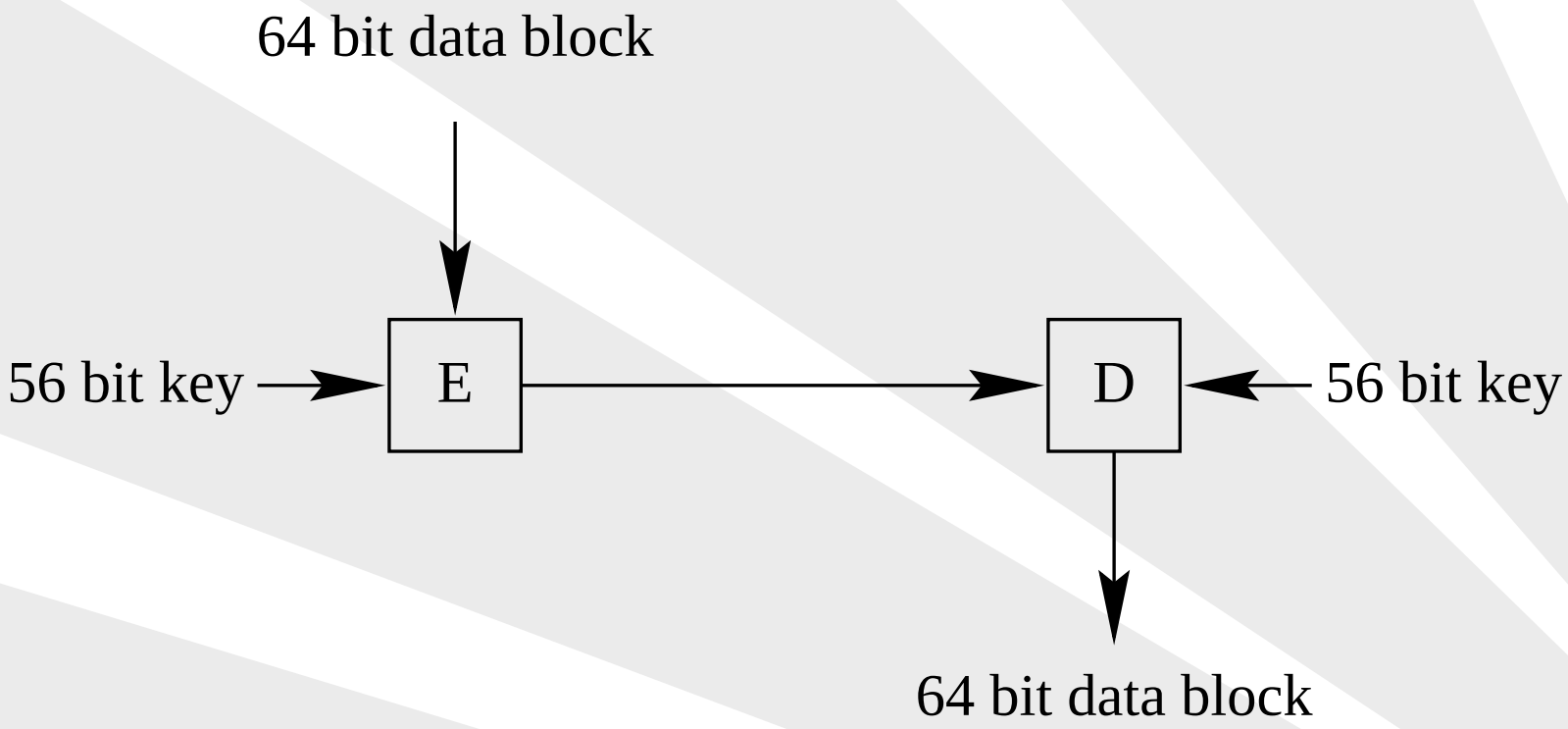
- Type 1 Product module
  - Can be sold only to US government agencies and US government contractor for processing classified data
- Type 2 Product module
  - Can be sold only to US government agencies and US firms for processing sensitive, unclassified data
- Under certain circumstances, NSA may approve Type 1 and Type 2 products for use by friendly governments

Using Symmetric Key Cryptosystem

Modes of Operation for Symmetric Key Crypto

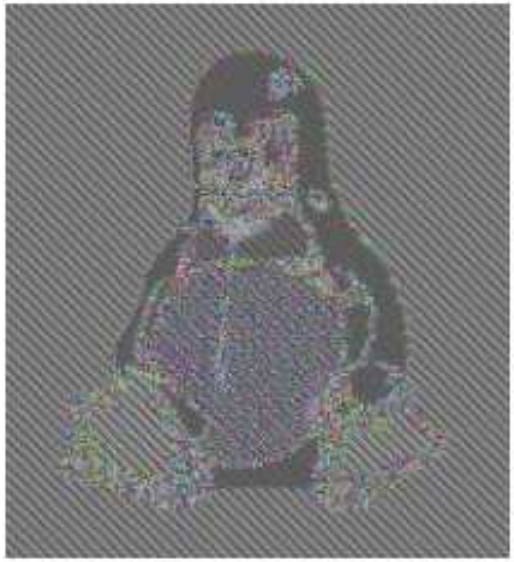
- 4 modes of operation
  - ECB - Electronic Code Book
  - CBC - Cipher Block Chaining
  - CFB - Cipher Feedback
  - OFB - Output Feedback
- For DES, these are part of the NIST standard
- They have been generalized into ANSI and ISO standards for modes of block ciphers

Electronic Code Book Mode



- Ok for small messages
- Identical data blocks will be identically encrypted

Problem with ECB Mode



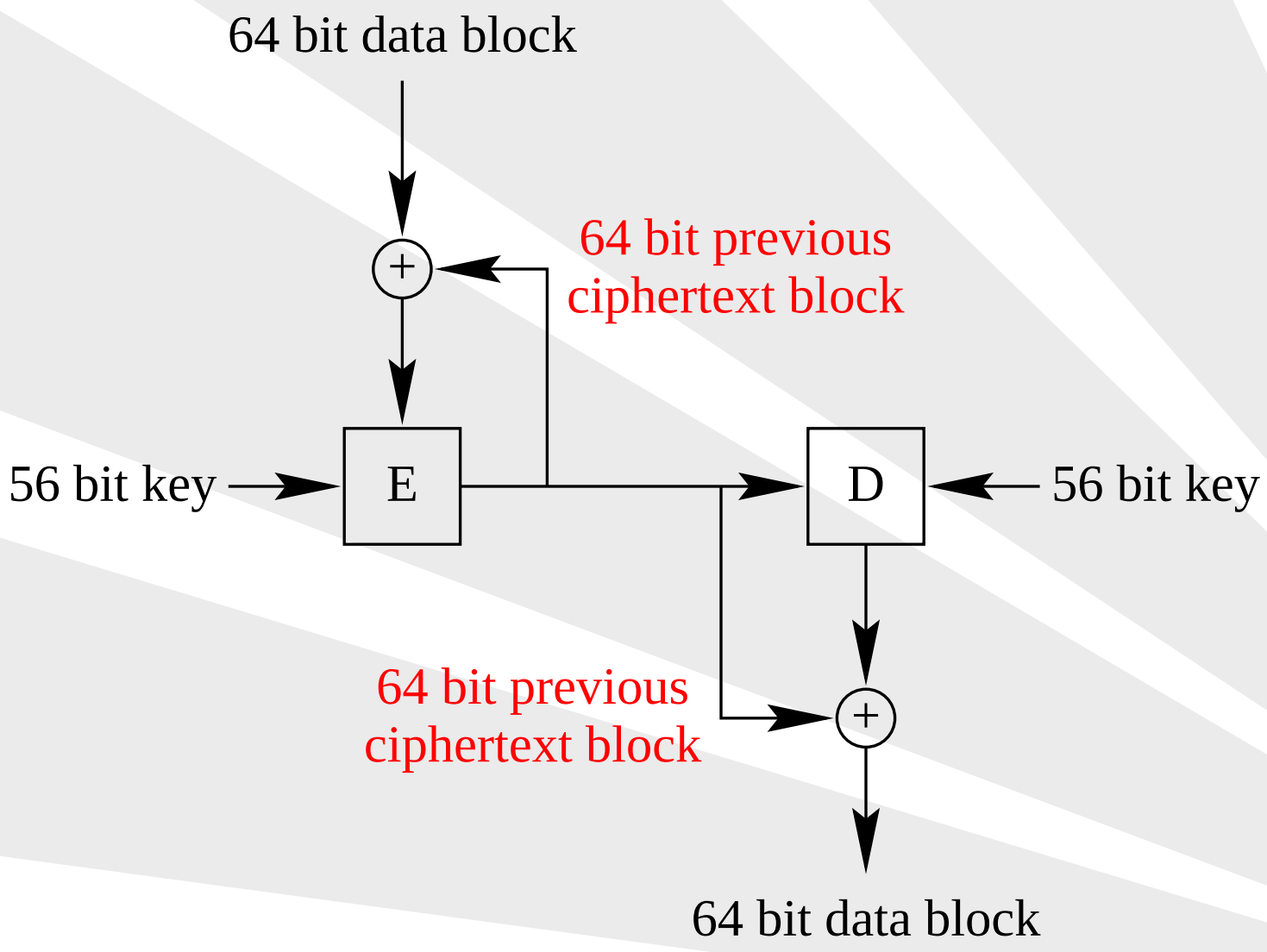
Attribution

Image source - http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Tux the Penguin, the Linux mascot. Image copyrighted by Larry Ewing 1996. Created using The GIMP

Tux image ECB encryption created by Wikipedia user Lunkwill

Cipher Block Chaining



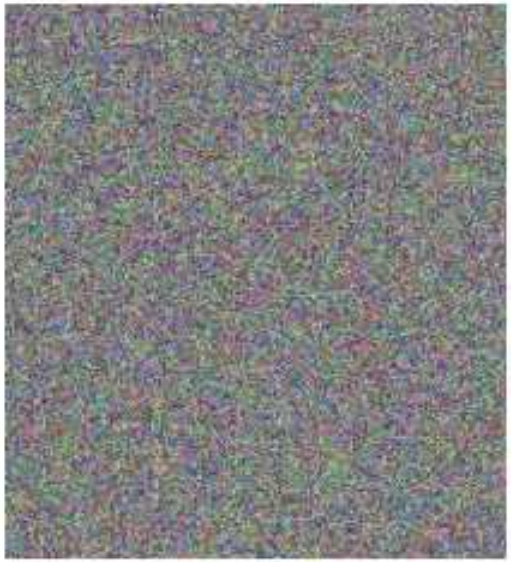
Cipher Block Chaining

- CBC seeks to make each ciphertext block a function of
  - the key and
  - all previous plaintext blocks
- Needs an Initialization Vector (IV) to serve as the first feedback block

Cipher Block Chaining

- IV need not be secret or random
- Integrity of IV is important, otherwise first data block can be arbitrarily changed
- IV should be changed from message to message, or first block of every message should be distinct
  - otherwise the first blocks will be encrypted identically

Encryption in CBC Mode



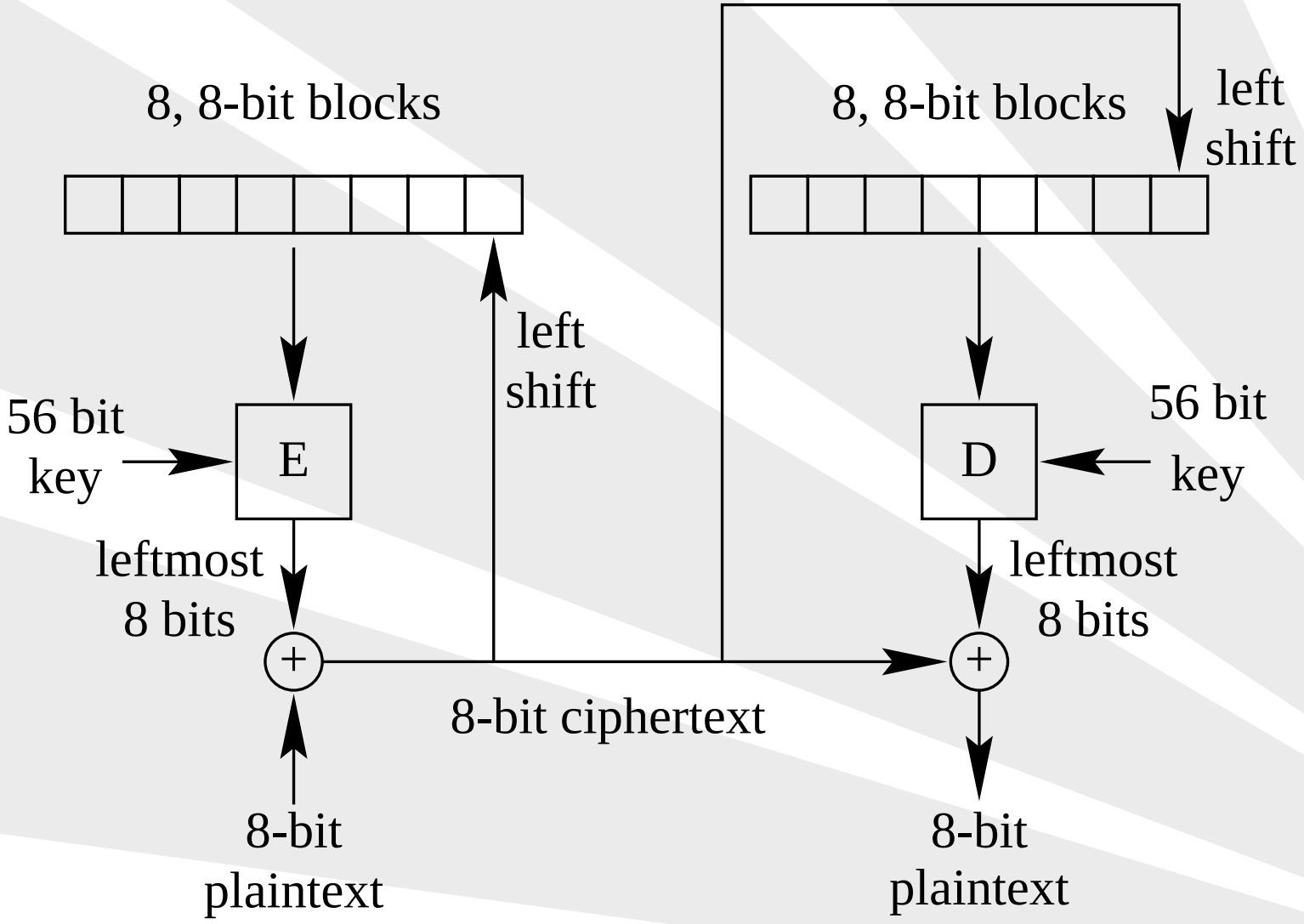
Attribution

Image source - http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Tux the Penguin, the Linux mascot. Image copyrighted by Larry Ewing 1996. Created using The GIMP

Tux image secure encryption created by Wikipedia user Lunkwill

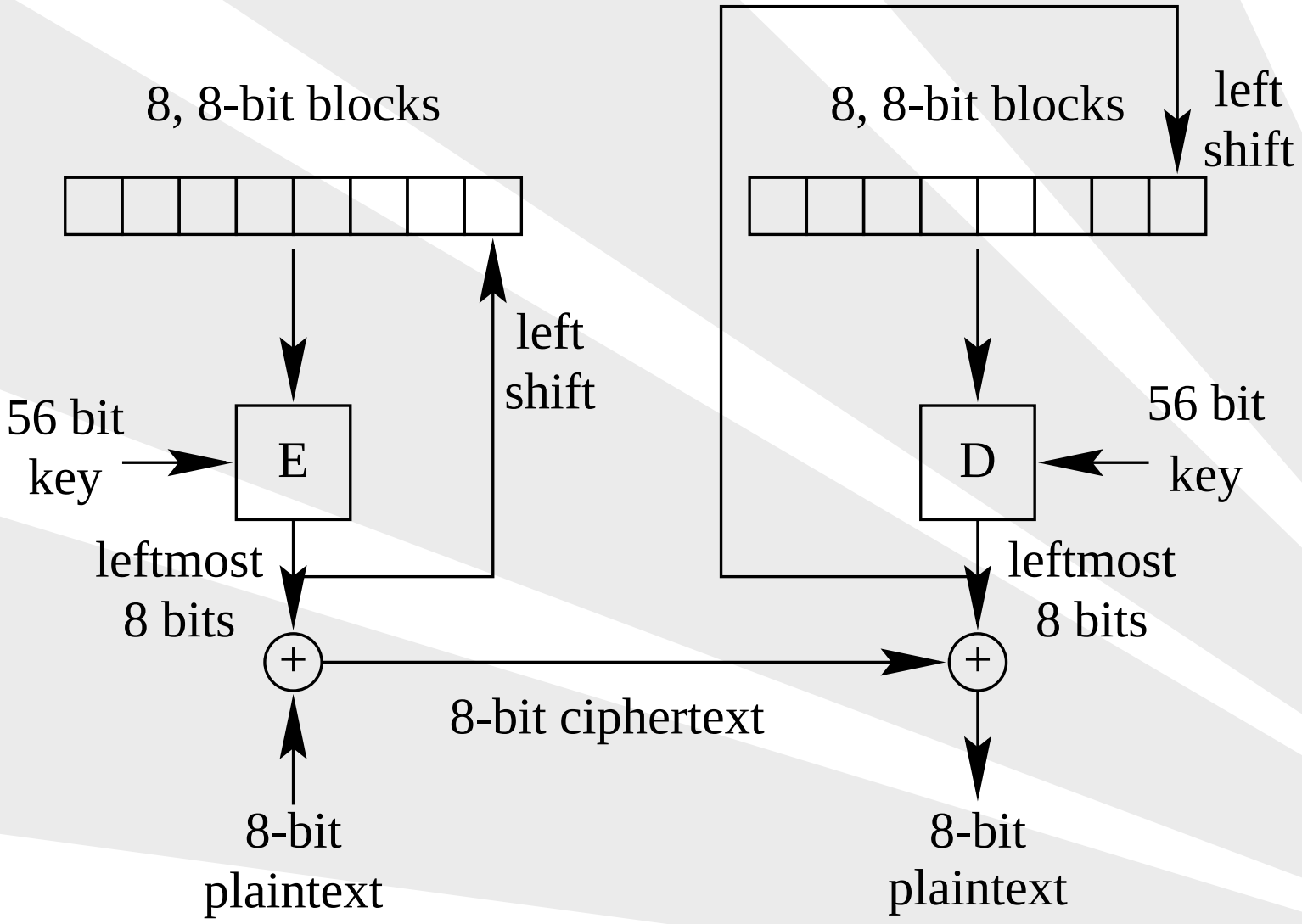
Cipher Feedback



Cipher Feedback

- Intended for character-by-character transmission, among other things
- Operates at $1/8^{th}$ the speed of CB or ECB
- We can have k-bit feedback, in general
- Needs a 64-bit Initialization Vector to initialize the shift register
- Error in 1 8-bit ciphertext will be extended to the next 8 8-bit decrypted ciphertexts

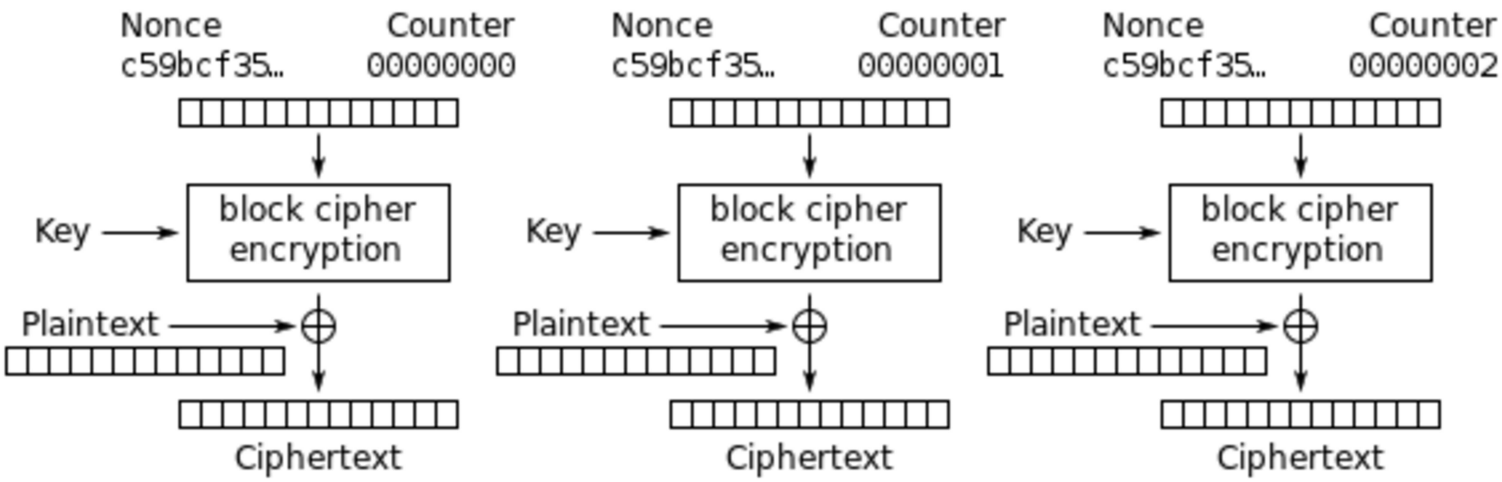
Output Feedback



Output Feedback

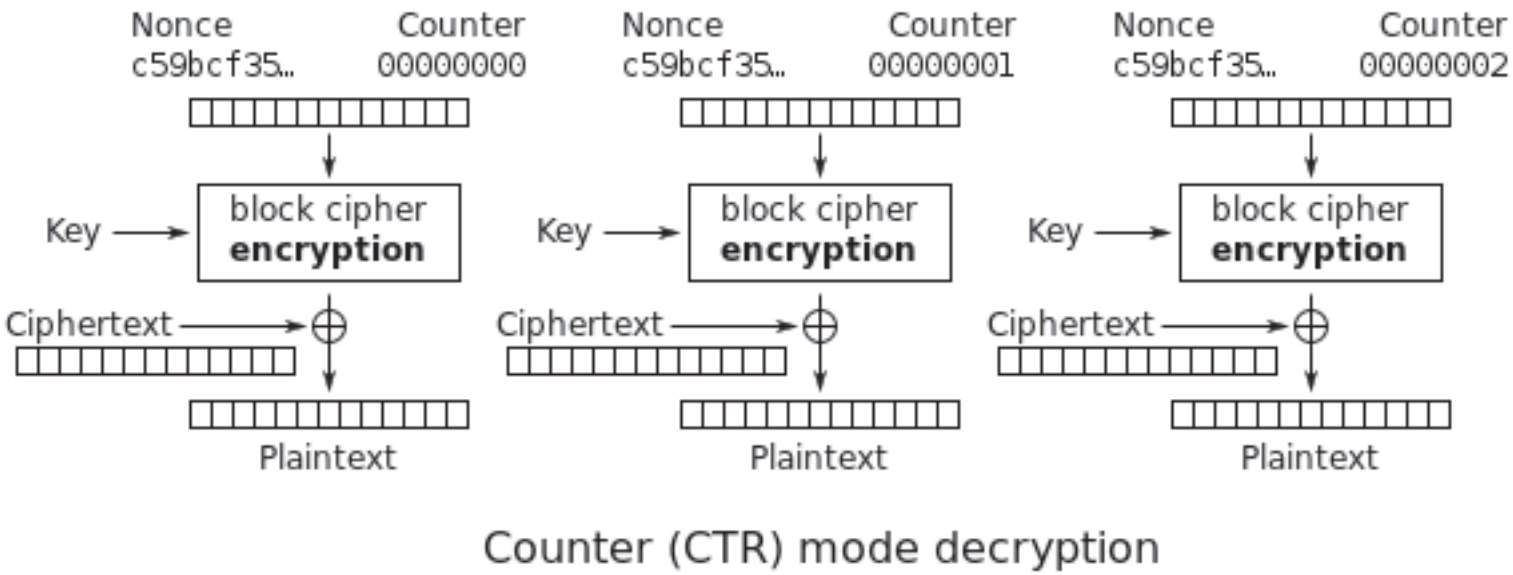
- Similar to CFB except that the key stream generated as input to exclusive OR is independent of plaintext
  - Error is not extended
- OFB is intended for use with speech or video (due to lack of error extension)
- ANSI and ISO only allow 64 bit feedback in OFB
  - otherwise average cycle of repetition in key stream is 2^{31}

Counter Mode for Block Ciphers



Counter (CTR) mode encryption

Counter Mode for Block Ciphers



Counter (CTR) mode decryption

Advanced Encryption Standard

- Federal Information Processing Standard 197
- Replacement for DES, became effective May 2002
- Standard to be reevaluated every 5 years

Advanced Encryption Standard

- Symmetric key block cipher
- Uses the Rijndael algorithm
- 128 bit data block size
- Variable key sizes of 128 bit or 192 bits or 256 bits
  - Rijndael was designed to handle additional block sizes, however they were not adopted in the standard