Image: Avocet Hardware

UNIVERSITY OF Southampton
School of Electronics
and Computer Science

Security 1

ELEC3227/ELEC6255

Alex Weddell
asw@ecs.soton.ac.uk

Overview

- Aspects and considerations for security
- Symmetric ciphers
- Cipher modes

Aspects of Security

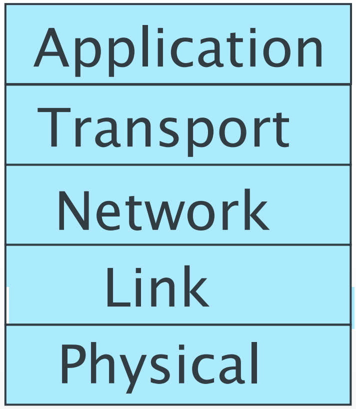
Network security problems are in four intertwined areas:

1. Secrecy (confidentiality)
2. Authentication (verifying identity of the other party)
3. Nonrepudiation (signatures)
4. Integrity control (ensuring a message is genuine)

UNIVERSITY OF Southampton
School of Electronics and Computer Science

The 5-layer Model

- Security issues affect all layers
  - Application: user authentication/nonrepudiation
  - Transport: end-to-end encryption (process-to-process)
  - Network: firewalls can block bad packets
  - Link: packets encrypted on a link-by-link basis (link encryption)
  - Physical: physical protection around cables



Adversaries and Threats

- Different threats require different defences.

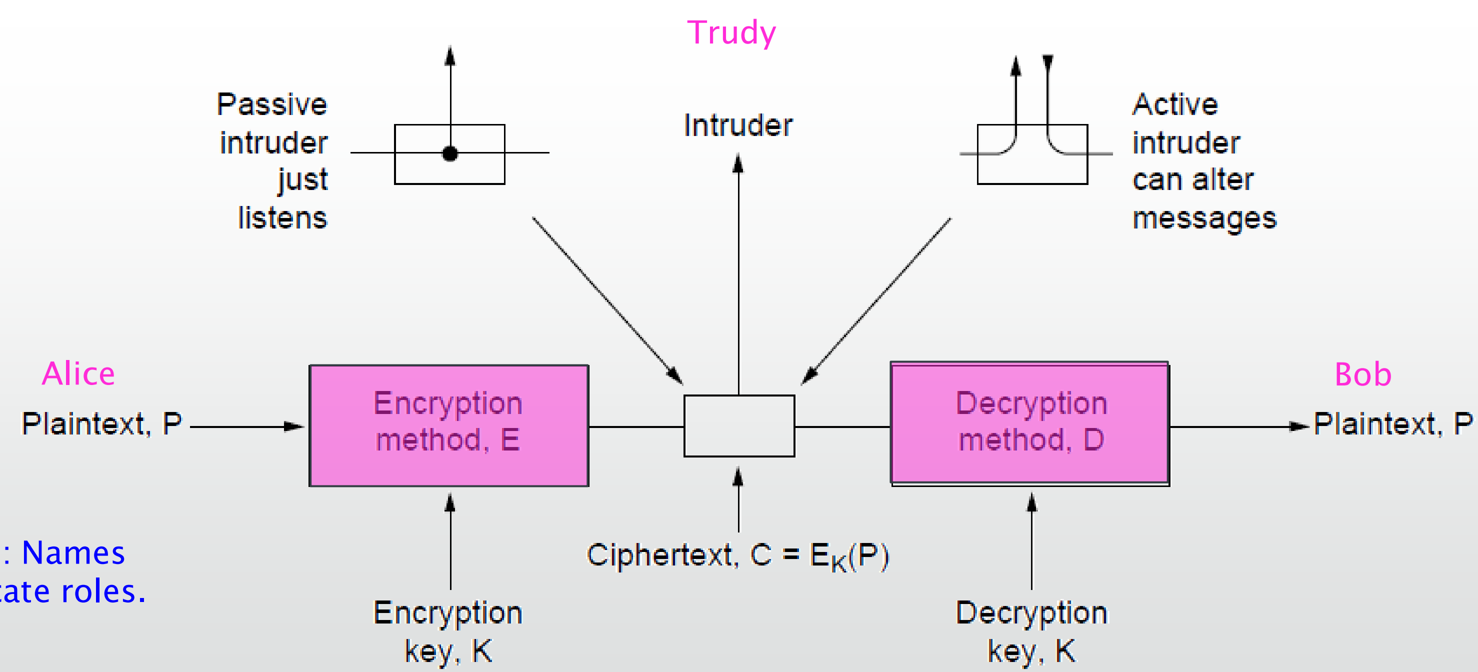
Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Cryptography

- Cryptography is a basic building block for security
- We will look at:
  - Substitution ciphers
  - Transposition ciphers
  - One-time pads
- Most popular types of encryption:
  - Symmetric Key: same key used to both encrypt and decrypt, popular for data communications protocols.
  - Public Key: different keys used to encrypt and decrypt (public key, private key), popular for encrypting keys and sometimes data.

The Encryption Model

- The encryption model (for a symmetric-key cipher)
  - Kerckhoff's principle: Algorithms (E, D) are public
  - Only the keys (K) are secret



Note: Names indicate roles.

Substitution Ciphers

- Substitution ciphers replace each letter, or group of letters, in the message with another letter or group of letters to disguise it.
- A simple single-letter substitution cipher:

plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Transposition Ciphers

- Transposition ciphers reorder letters but don't disguise them…
- Simple column transposition cipher:

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

One-Time Pads

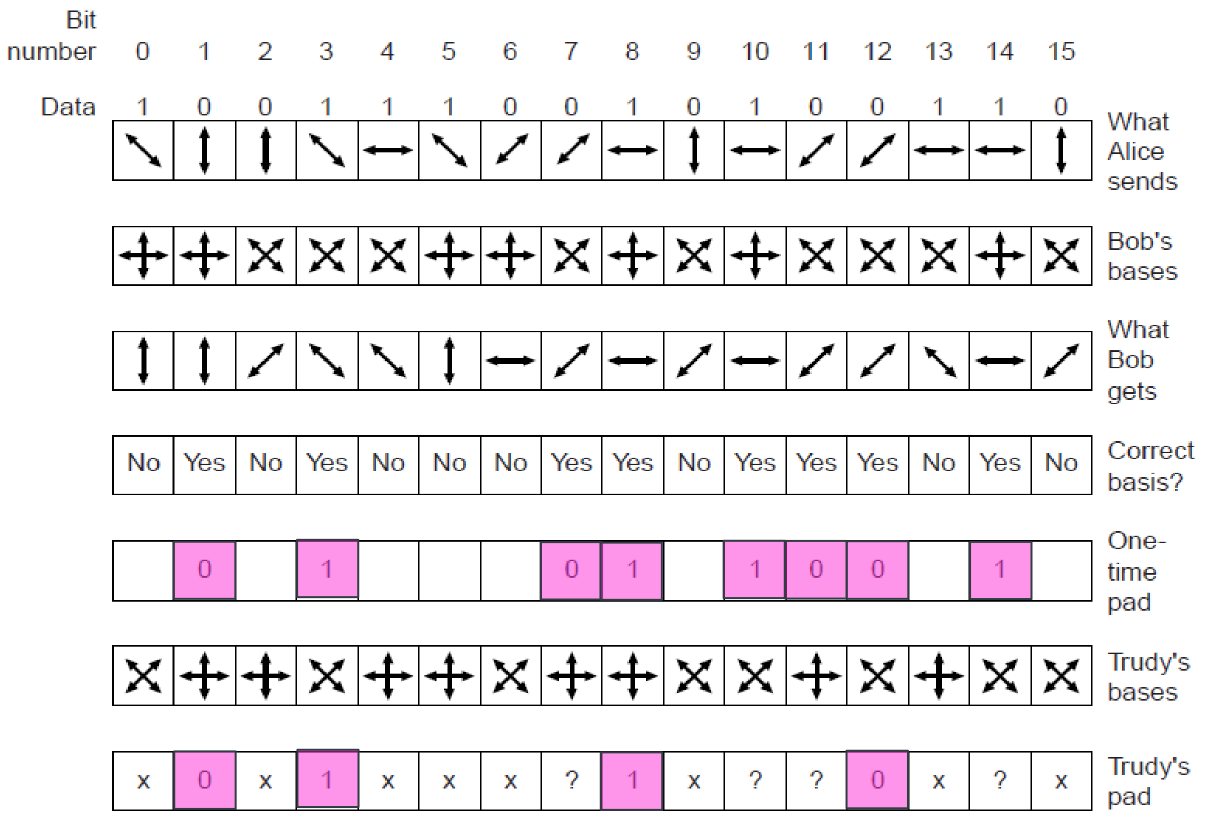
- Simple scheme for perfect secrecy
- XOR message with pad to encrypt/decrypt
- Pad is as long as the message, and **can't be reused**!
  - It's a "one-time" pad to guarantee secrecy
- As long as pads are never re-used or revealed, this approach is unbreakable.

Message 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Pad 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Ciphertext:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Pad 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Plaintext 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

Different secret pad decrypts to the wrong plaintext

Quantum Cryptography

- Alice sending Bob a one-time pad with quantum crypto.
  - Bob’s guesses yield bits; Trudy misses some
  - Bob can detect Trudy since error rate increases



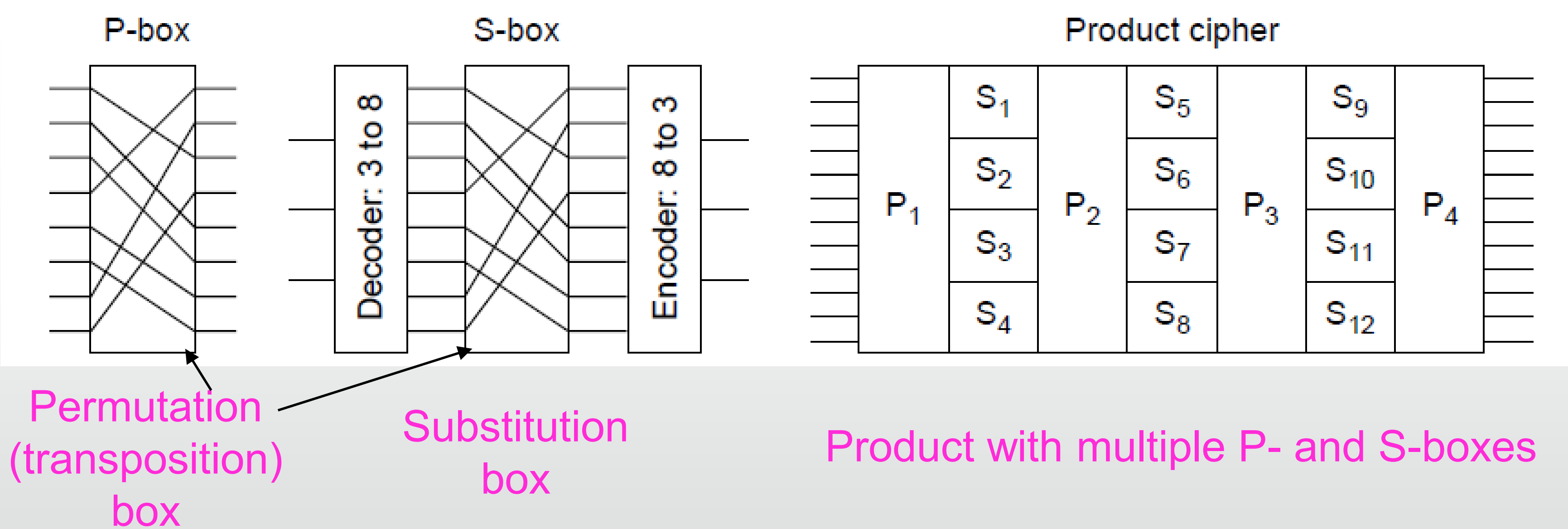
Fundamental Principles

1. Messages must contain some **redundancy**
    - Redundancy = info not needed to understand the message so that active intruders cannot send random junk and have it be interpreted as a valid message
    - All encrypted messages decrypt to something
    - Redundancy lets receiver recognize a valid message
    - But redundancy helps attackers break the design

2. Some method is needed to foil **replay attacks**
    - Without a way to check if messages are fresh then old messages can be copied and resent
    - For example, add a date stamp to messages

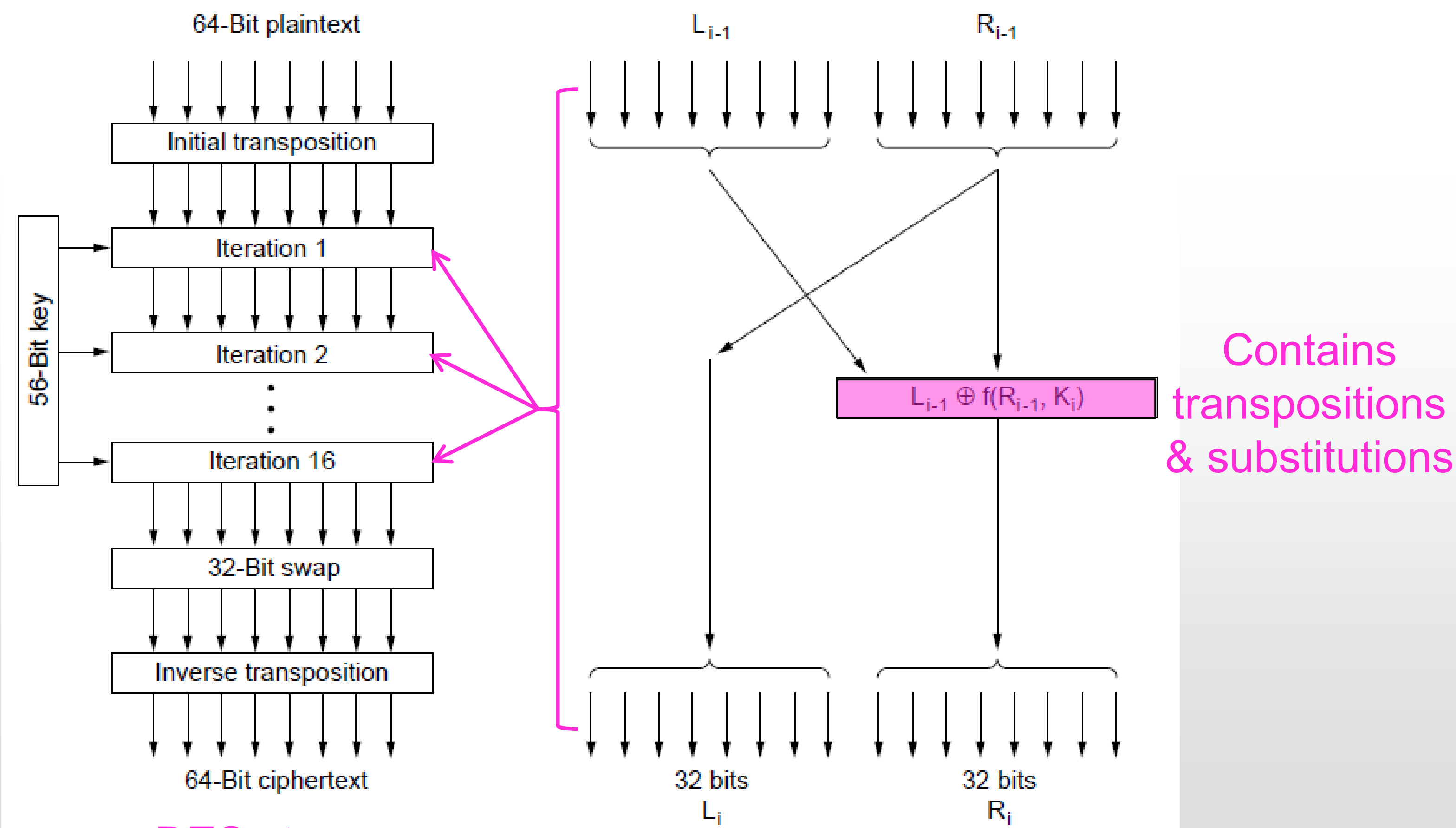
Symmetric Key Algorithms

- Use the same secret key to encrypt and decrypt; block ciphers operate on a block at a time
  - Same number of bits in as bits out
  - Product cipher combines transpositions/substitutions



Data Encryption Standard

- DES was widely-used, but is no longer secure

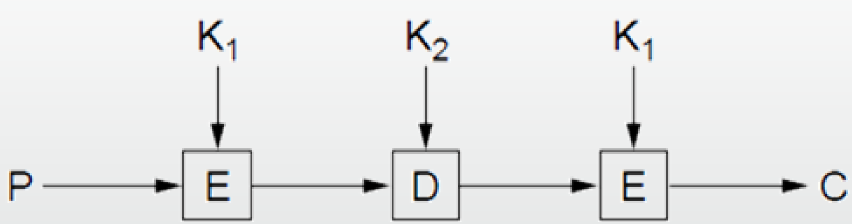


DES steps

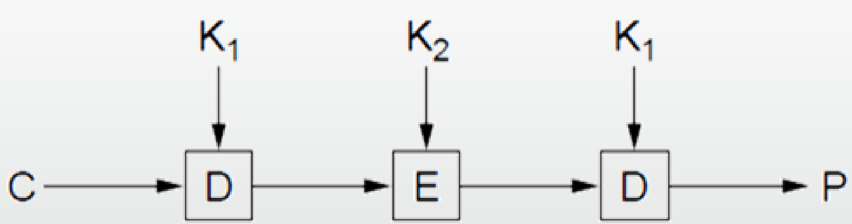
A single iteration

Data Encryption Standard

- Triple encryption (“3DES”) with two 56-bit keys
  - Gives a key strength of 112 bits – though 112 bits no longer considered adequate!
  - Setting $K_1 = K_2$ allows for compatibility with DES
- Was introduced in 1979, popular through the 1990s. Uses 2 DES keys for encryption and 3 iterations (stages) of DES, using key 1 for 1st and 3rd iteration and key 2 for 2nd iteration.



Triple DES encryption



Triple DES decryption

The Importance of Key Length

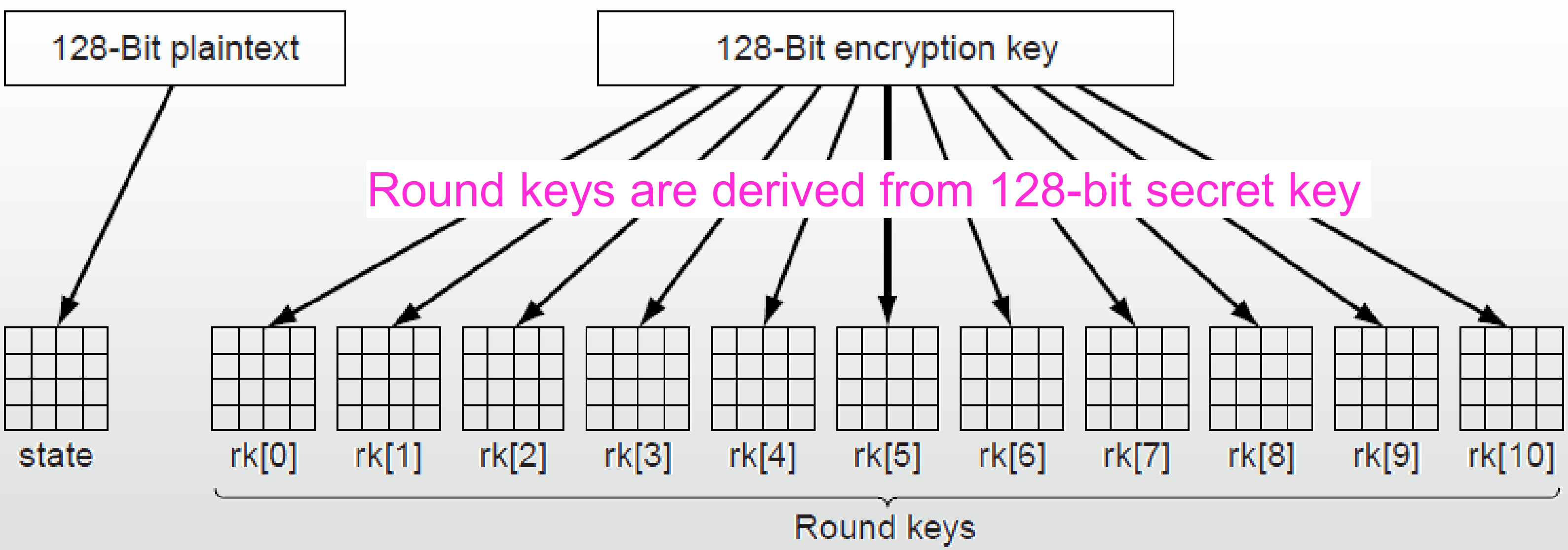
- In general, longer keys mean a higher level of protection for a each cipher.
- Key length measured in bits; 128-bit keys used with RC4 symmetric-key cipher (supported by SSL) are approx $3x10^{26}$ stronger than with 40-bit keys.
- However, some ciphers need longer keys to achieve same protection level
  - RSA (public-key encryption) can only use subset of possible values.
- NIST now recommends 2048-bit keys for RSA (should provide protection to 2030), gives equivalent protection to 112-bit symmetric key.

Advanced Encryption Standard

- AES replaces 3DES. Introduced in 2001 by US Government (NIST). Supports block size of 128-bits and encryption key lengths of 128, 192, or 256 bits.
- AES is the successor to 3DES:
  - Symmetric block cipher, key lengths up to 256 bits
  - Openly designed by public competition (1997-2000)
  - Available for use by everyone
  - Built as software (e.g., C) or hardware (e.g. x86, microprocessors/transceivers)
  - Winner was Rijndael cipher
  - Now a very widely used standard

Advanced Encryption Standard

- AES uses 10 rounds for 128-bit block and 128-bit key
  - Each round uses a key derived from 128-bit key
  - Each round has a mix of substitutions and rotations
  - All steps are reversible to allow for decryption



Cipher Modes

- Cipher modes set how long messages are encrypted
- Encrypting each block independently, called ECB (Electronic Code Book) mode, is vulnerable to shifts:

Name	Position	Bonus
Adams, Leslie	Clerk	$10
Black, Robin	Boss	$500,000
Collins, Kim	Manager	$100,000
Davis, Bobbie	Janitor	$5
16	8	8

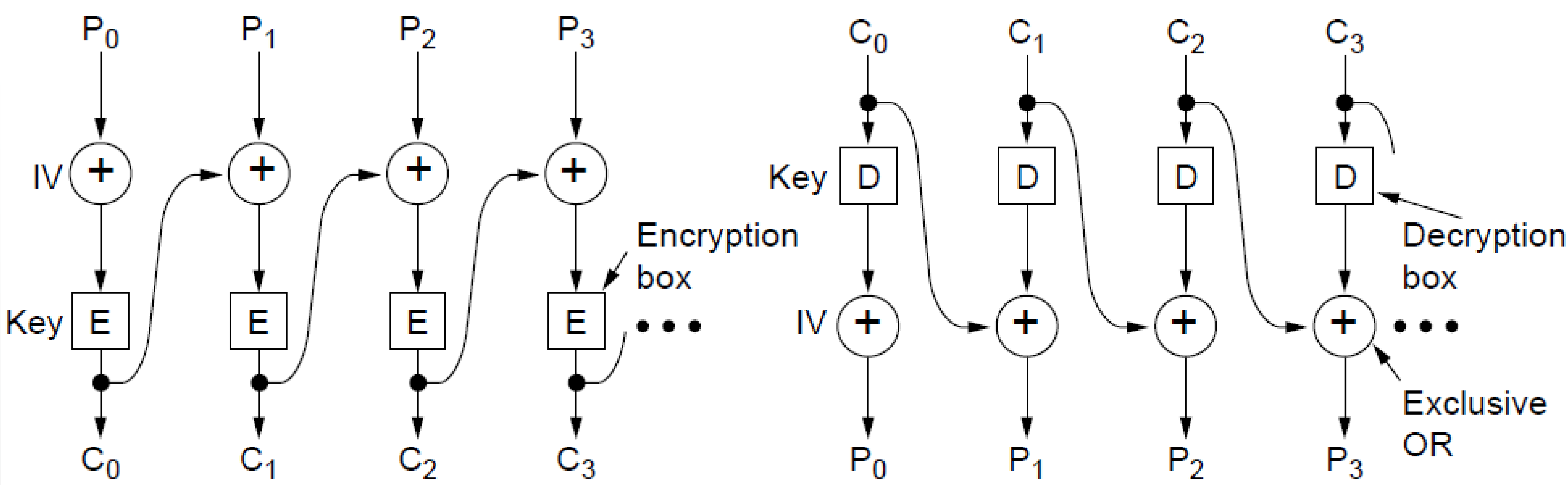
With ECB mode, switching encrypted blocks gives a different but valid message

Leslie gets a large bonus!

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Cipher Modes

- CBC (Cipher Block Chaining) is a widely used mode
- Chains blocks together with XOR to prevent shifts
- Has a random IV (~~Initial Value~~ Initialisation Vector) for different output



CBC mode encryption

CBC mode decryption

Cipher Modes

- Insecure encryption of an image using Cipher Block Chaining (CBC) encryption

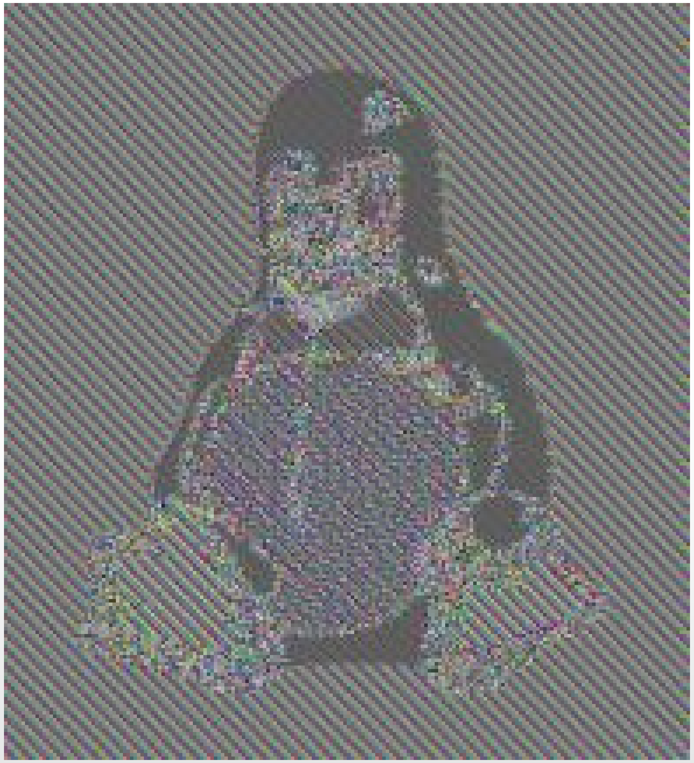
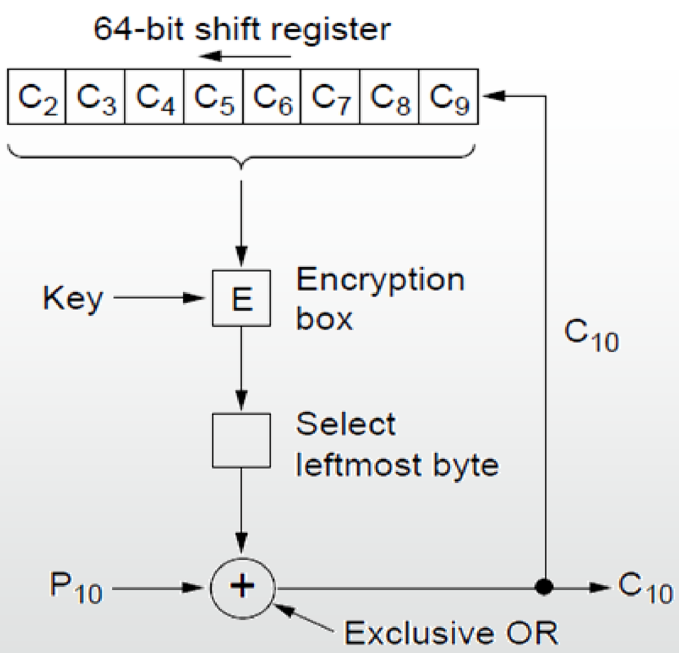


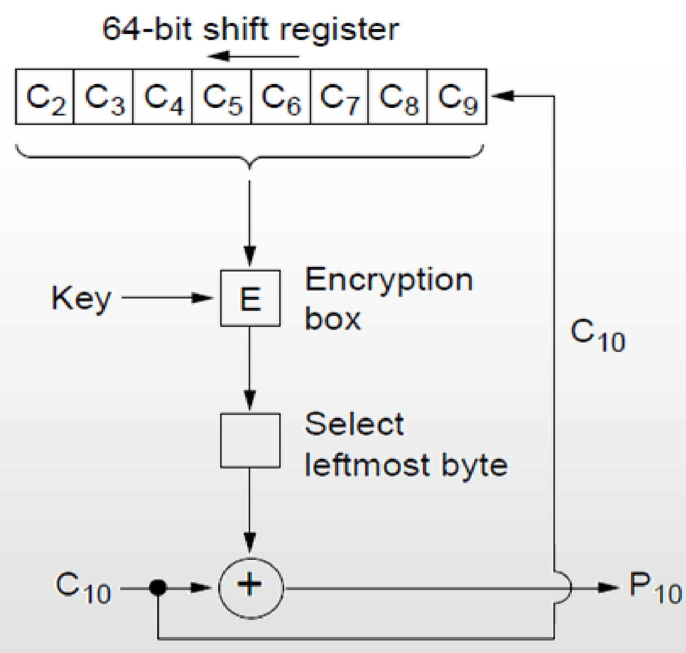
Image from Wikimedia Commons. Larry Ewing, the owner of the original image, lewing@isc.tamu.edu, The GIMP

Cipher Modes

- Many other modes with advantages/disadvantages…
- Example: cipher feedback mode is similar to CBC mode, but operates byte-by-byte, rather than block-by-block



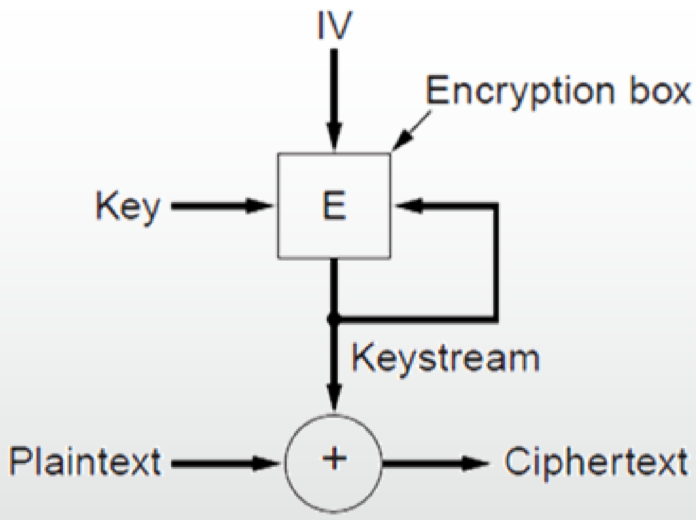
Encryption



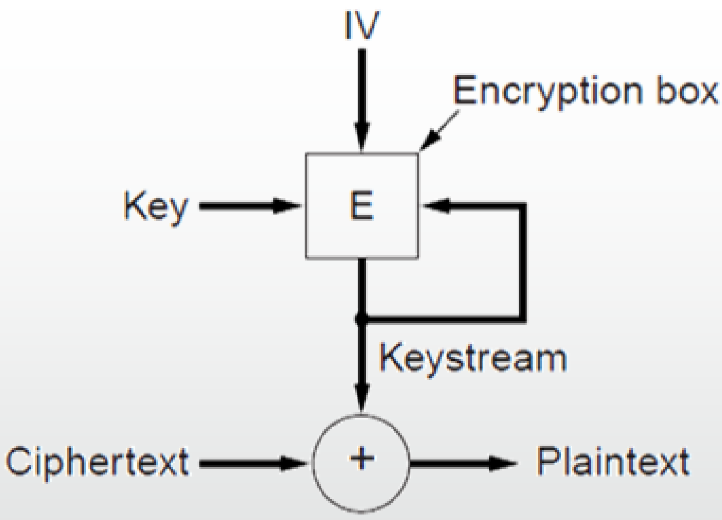
Decryption

Cipher Modes

- A stream cipher uses the key and IV to generate a stream that is a one-time pad; can't reuse (key, IV) pair
- Doesn't amplify transmission errors like CBC mode



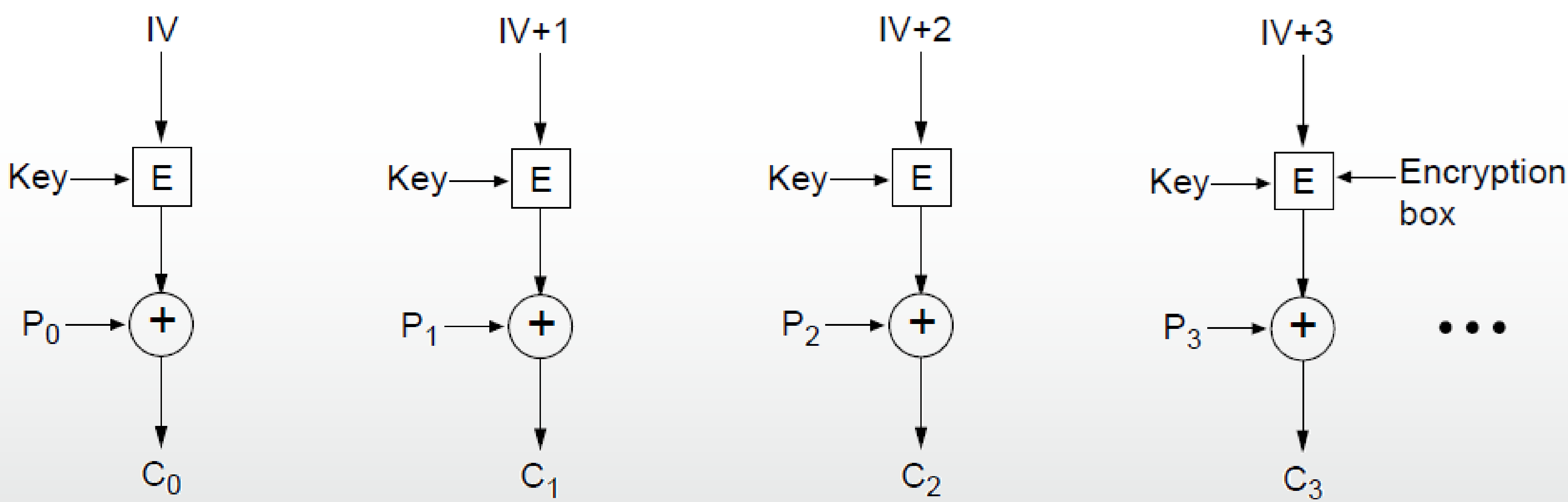
Encryption



Decryption

Cipher Modes

- Counter mode (encrypt a counter and XOR it with each message block) allows random access for decryption



Encryption above; repeat the operation to decrypt

UNIVERSITY OF Southampton
School of Electronics
and Computer Science

Other Ciphers

- Some common symmetric-key cryptographic algorithms
  - Can be used in combination, e.g., AES over Twofish

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

- Note that in recent years AES (Rijndael) performance has significantly improved with hardware optimisations.

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Summary

- Aspects and considerations for security
- Symmetric ciphers
- Cipher modes

Next lecture

- Public/private keys
- Use of encryption in internet communications