Classical Cryptography

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

1. Introduction

Cryptography

"The study of methods for sending messages in secret - the study of methods for transforming plaintext into ciphertext" [Mollin]

Cryptanalysis

The study of methods for breaking ciphertext.

Cryptology

The science of Cryptography and Cryptanalysis combined.

1. Introduction

Reasons for Cryptography

- Cost of Information
- Cost of denying service
- Vandalism
- Reputation risk for companies
- Computer crimes are quick
- Computers are mostly dumb

1. Introduction

1.2 Terminology

Plaintext unencrypted message

Ciphertext encrypted message

Encryption process of translating plaintext into ciphertext

Decryption process of translating ciphertext to plaintext

1.3 Aims of Cryptology

Confidentiality Keeping messages secure

Authentication Receiver of a message should be able to ascertain its origin

Integrity verification that a message has not been modified in transit

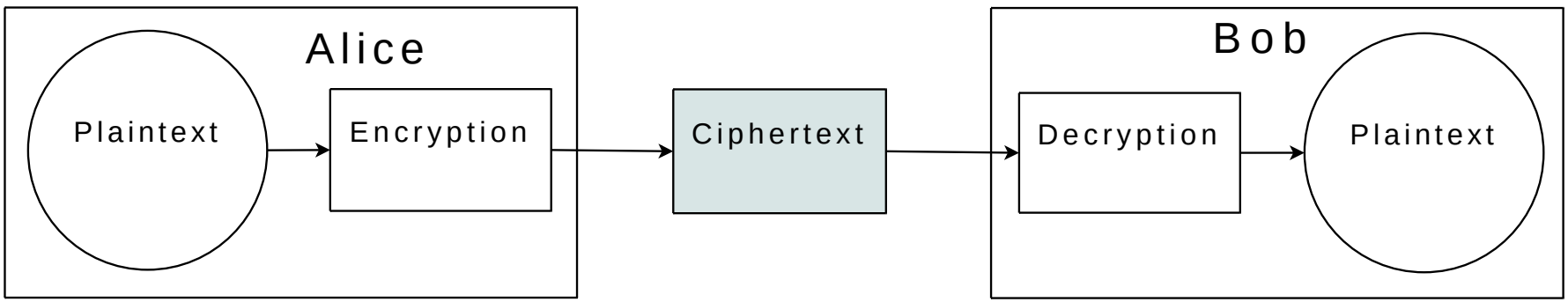
Non-repudiation A sender should not be able to later (falsely) deny that he sent a message

1.4 Cryptographic Process

Plaintext - M
Ciphertext - C
Encryption Process - E
Reverse of the encryption function - D

$E(M) = C$
$D(C) = M$
$D(E(M)) = M$

1. Introduction



1. Introduction

1.6 Algorithms and keys

Def - Cryptographic algorithm (cipher): mathematical function used to perform encryption and decryption. (Pair of functions, E and D)

Restricted Algorithm - security of cipher depends on keeping the algorithms secret

1.6 Algorithms and keys (Continued)

Disadvantages of restricted algorithms:

- Standardization and quality control not possible
- Every user group must have their own algorithm
- Any member leaking info compromises entire group's security
  - New algorithm must be devised
- Can't use off-the-shelf hardware or software

1.6 Algorithms and keys (Continued)

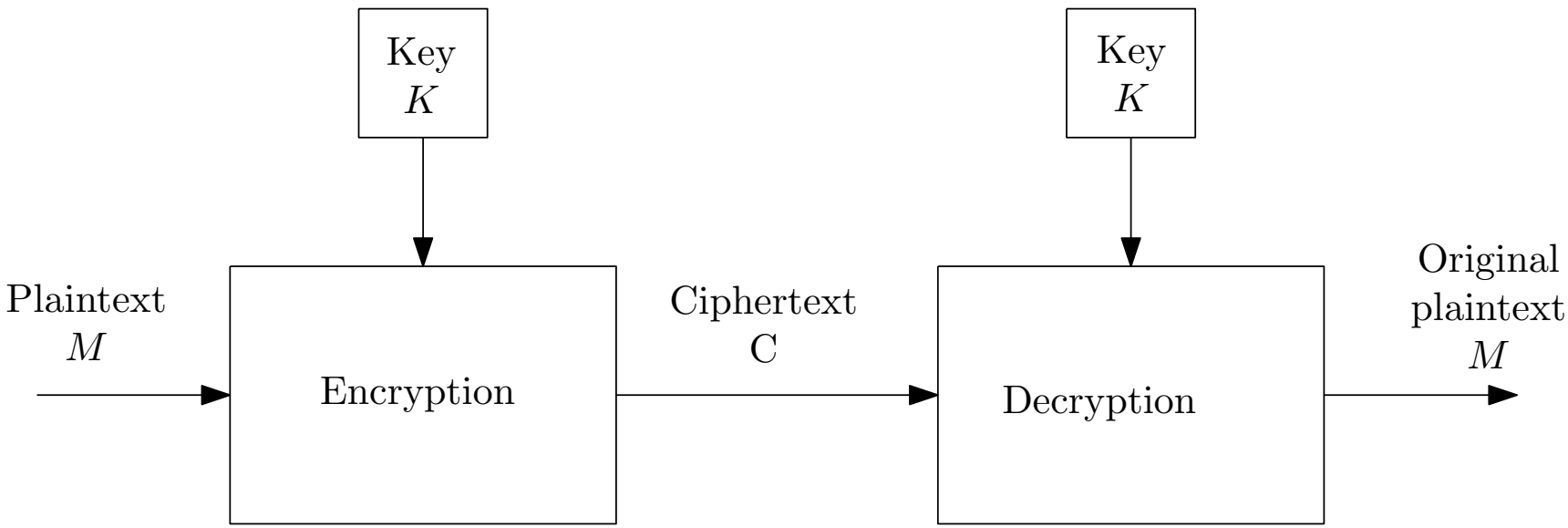
Key based algorithms overcame the difficulties associated with restricted algorithms

Algorithms workings can be widely published without compromising security

Keyspace: Number of possible values that a key can take

$E_K(M) = C$
$D_K(C) = M$
$D_K(E_K(M)) = M$

1. Introduction



1.6 Algorithms and keys (Continued)

Key based algorithm:

- Algorithm itself does not produce the element of security
- Security rests solely in the key(s)

1.7 Algorithm Types

Def - Symmetric algorithm: Algorithm with both encryption and decryption keys the same (or one can easily be derived from the other)

Disadvantage?

Can be divided into:

- stream ciphers
- block ciphers

1.7 Algorithm Types

Def - Stream cipher: cipher that operates on a continuous, arbitrary length stream of incoming data, producing one byte (/bit) of output for every byte (/bit) of input

Def - Block cipher: cipher that operates on a block of bits at a time

1.7 Algorithm Types

Def - Asymmetric algorithm: Algorithm with one key associated with encryption process and one key associated with decryption process. One key cannot easily be determinded from the other.

Also known as Public key algorithm

Encryption key (public key) can be made public, used by many to encrypt, only person that can decrypt is one with decryption key (private key).

1.8 Attack types

Def - Cryptanalysis: process of recovering the plaintext of a message from the ciphertext without access to the key.

- Total break $\rightarrow$ finds K, knows algorithm
- Global deduction $\rightarrow$ finds algorithm $A = D_K(C)$
- Local deduction $\rightarrow$ finds P for a specific C
- Information deduction $\rightarrow$ Some info gained on K or P, incomplete knowledge
- Compromise $\rightarrow$ loss of K through non-cryptanalytic means

1.8 Attack types (Continued)

Assume eavesdroppers have complete access to ciphertext $\rightarrow$
Security of cipher may not rely on security of channel

Assume attacker has full access to algorithm

1.8 Attack types (Continued)

Attack Economics:

Value of encrypted information $<$ Cost of breaking cryptosystem

1.8 Attack types (Continued)

- Ciphertext only attack
- Known Plaintext
- Chosen Plaintext Attack
- Adaptive Chosen Plaintext Attack
- Chosen Ciphertext Attack
- Chosen Key Attack
- Rubber-hose Cryptanalysis

1. Introduction

1.9 Some Basic Ciphers

Two main categories:

- Transposition ciphers
- Substitution ciphers

1.9 Some Basic Ciphers

Monoalphabetic Cipher

One Example: Caesar Cipher

A	B	C	D	E	F	G	H	I	...	U	V	W	X	Y	Z
d	e	f	g	h	i	j	k	l	...	x	y	z	a	b	c

1.9 Some Basic Ciphers

Encryption function?

A	B	C	D	E	F	G	H	I	...	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	...	20	21	22	23	24	25

1.9 Some Basic Ciphers

Encryption function?

A	B	C	D	E	F	G	H	I	...	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	...	20	21	22	23	24	25

$$C_i = E(M_i) = (M_i + 3) \mod 26$$

1. Introduction

1.9 Some Basic Ciphers

Example: TREATY IMPOSSIBLE

1. Introduction

1.9 Some Basic Ciphers

Monoalphabetic Cipher

One Example: Caesar Cipher

A	B	C	D	E	F	G	H	I	...	T	U	V	W	X	Y	Z
d	e	f	g	h	i	j	k	l	...	w	x	y	z	a	b	c

Example:

T	R	E	A	T	Y	·	I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b	·	l	p	s	r	v	v	l	e	o	h

1.9 Some Basic Ciphers

Another example:
wklv phvvdjh lv qrw wrr kdug wr euhdn

1. Introduction

1.10 Homework

hqfubswlrq lv d phdqv ri dwwdlqlqj vhfxuh frpsxwdwlrq ryhu lqvhfxuh fkdqqhov eb xvlqj hqfubswlrq zh glvjxlvh wkh phvvdjh vr wkdw hyhq li wkh wudqvplvvlrq lv glyhuwhg wkh phvvdjh zloo qrw eh uhyhdohg