

More On Cryptography

CS 239

Computer Security

January 25, 2006

CS 239, Winter 2006

Lecture 5
Page 1

Outline

- Permutation ciphers
- Stream and block ciphers
- Uses of cryptography

CS 239, Winter 2006

Lecture 5
Page 2

Permutation Ciphers

- Instead of substituting different characters, scramble up the existing characters
- Use algorithm based on the key to control how they're scrambled
- Decryption uses key to unscramble

CS 239, Winter 2006

Lecture 5
Page 3

Characteristics of Permutation Ciphers

- Doesn't change the characters in the message
 - Just where they occur
- Thus, character frequency analysis doesn't help cryptanalyst

CS 239, Winter 2006

Lecture 5
Page 4

Columnar Transpositions

- Write the message characters in a series of columns
- Copy from top to bottom of first column, then second, etc.


CS 239, Winter 2006

Lecture 5
Page 5

Example of Columnar Substitution

How did this transformation happen?

T	r	a	n	s	i
e	r	\$	l	o	
o	t	o	m		
y	s	a	v	i	
n	g	s	a	c	
e	o	u	n	t	



T	e	o	y	n	e
r	r			g	o
a	t	s	s	u	
n	\$	e	a	n	
s	l		v	a	t
f	o	m	i	c	

Looks a lot more cryptic written this way:

Te0yncrr goa tssun\$oa ns1 vatf0mic

CS 239, Winter 2006

Lecture 5
Page 6

Attacking Columnar Transformations

- The trick is figuring out how many columns were used
- Use information about digrams, trigrams, and other patterns
- Digrams are letters that frequently occur together (re, th, en, for example)
- For each possibility, check digram frequency

CS 239, Winter 2006

Lecture 5
Page 7

For Example,

- In our case, the presence of numerals in the text is suspicious
 - One might guess the numerals belong together
 - And maybe the dollar sign with them
- Most of this analysis is more complicated

CS 239, Winter 2006

Lecture 5
Page 8

Double Transpositions

- Do it twice
- Using different numbers of columns each time
- Find pairs of letters that probably appeared together in the plaintext
- Figure out what transformations would put them in their positions in the ciphertext

CS 239, Winter 2006

Lecture 5
Page 9

Generalized Transpositions

- Any algorithm can be used to scramble the text
- Usually somehow controlled by a key
- Generality of possible transpositions makes cryptanalysis harder

CS 239, Winter 2006

Lecture 5
Page 10

Which Is Better, Transposition or Substitution?

- Well, neither, really
- Strong modern ciphers tend to use both
- Transposition scrambles text patterns
- Substitution hides underlying text characters/bits
- Combining them can achieve both effects
 - If you do it right . . .

CS 239, Winter 2006

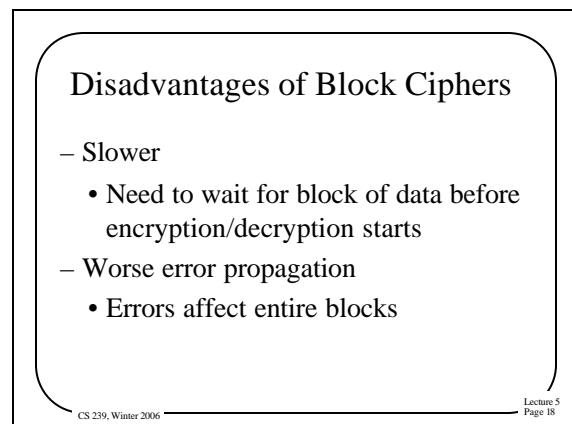
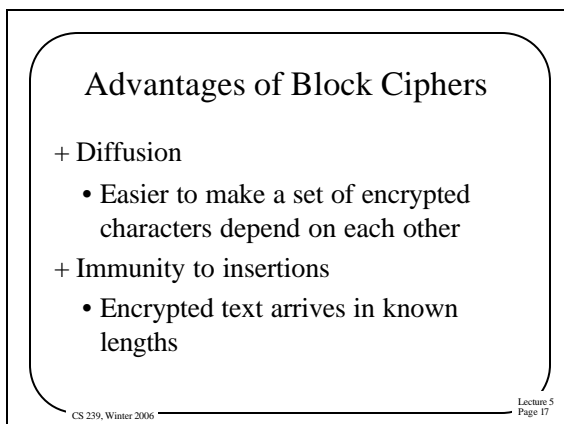
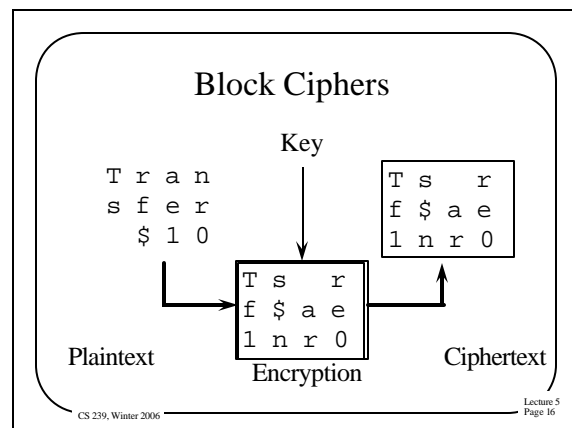
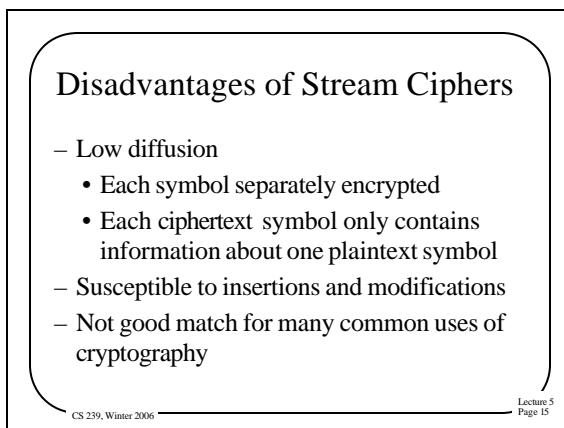
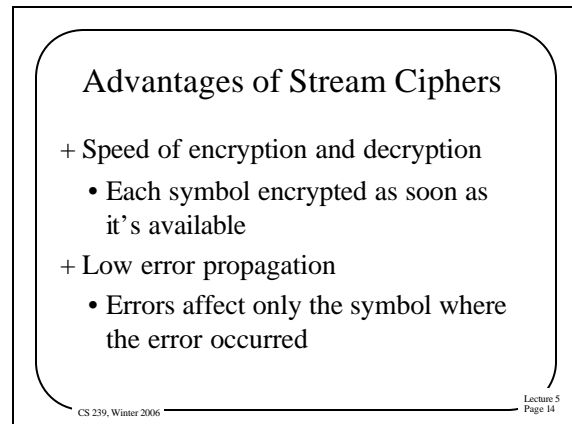
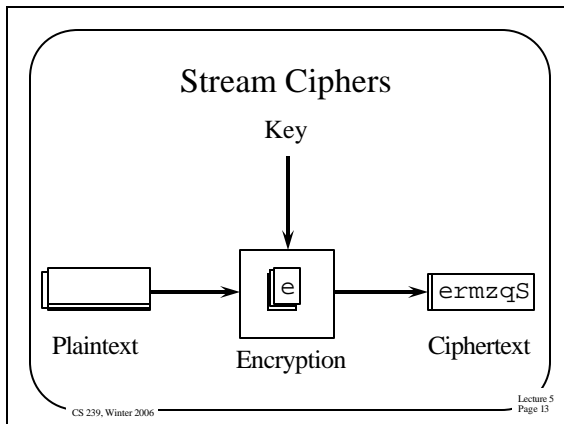
Lecture 5
Page 11

Stream and Block Ciphers

- Stream ciphers convert one symbol of plaintext immediately into one symbol of ciphertext
- Block ciphers work on a given sized chunk of data at a time

CS 239, Winter 2006

Lecture 5
Page 12



Desirable Characteristics of Ciphers

- Well matched to requirements of application
 - Amount of secrecy required should match labor to achieve it
- Freedom from complexity
 - The more complex algorithms or key choices are, the worse

CS 239, Winter 2006

Lecture 5
Page 19

More Characteristics

- Simplicity of implementation
 - Seemingly more important for hand ciphering
 - But relates to probability of errors in computer implementations
- Errors should not propagate

CS 239, Winter 2006

Lecture 5
Page 20

Yet More Characteristics

- Ciphertext size should be same as plaintext size
- Encryption should maximize *confusion*
 - Relation between plaintext and ciphertext should be complex
- Encryption should maximize *diffusion*
 - Plaintext information should be distributed throughout ciphertext

CS 239, Winter 2006

Lecture 5
Page 21

Uses of Cryptography

- What can we use cryptography for?
- Lots of things
 - Secrecy
 - Authentication
 - Prevention of alteration

CS 239, Winter 2006

Lecture 5
Page 22

Cryptography and Secrecy

- Pretty obvious
- Only those knowing the proper keys can decrypt the message
 - Thus preserving secrecy
- Used cleverly, it can provide other forms of secrecy

CS 239, Winter 2006

Lecture 5
Page 23

Cryptography and Authentication

- How can I prove to you that I created a piece of data?
- What if I give you the data in encrypted form?
 - Using a key only you and I know
- Then only you or I could have created it
 - Unless one of us told someone else the key . . .

CS 239, Winter 2006

Lecture 5
Page 24

Some Limitations on Cryptography and Authentication

- If both parties cooperative, cryptography can authenticate
 - Problems with non-repudiation, though
- What if three parties want to share a key?
 - No longer certain who created anything
 - Public key cryptography can solve this problem
- What if I want to prove authenticity without secrecy?

CS 239, Winter 2006

Lecture 5
Page 25

Cryptography and Non- Alterability

- Changing one bit of an encrypted message completely garbles it
 - For many forms of cryptography
- If a checksum is part of encrypted data, that's detectable
- If you don't need secrecy, can get the same effect
 - By just encrypting the checksum

CS 239, Winter 2006

Lecture 5
Page 26

Cryptography and Zero- Knowledge Proofs

- With really clever use, cryptography can be used to prove I know a secret
 - Without telling you the secret
- Seems like magic, but it can work
- Basically, using multiple levels of cryptography in very clever ways

CS 239, Winter 2006

Lecture 5
Page 27