Historical Cryptography

2	1	3	5	4
T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

H	T	I	I	S
A	S	S	C	E
E	R	T	E	M
S	S	A	E	G

Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E
T	H	I	S	I	S	A	S	E	C	R	E	T	M	E	S	S	A	G	E

Agenda

- Terminology
- Ancient Cryptography
- Transposition Ciphers
- Substitution Ciphers
- Summary
- Exercises

Terminology

- Sender
- Receiver
- Attacker/adversary
- Plaintext
- Ciphertext
- Key
- Encrypting/enciphering
- Decrypting/deciphering
- Cryptanalysis

Ancient Cryptography

- Writing (when few can read)
- Nonstandard hieroglyphics
- Scytale (rhymes with “Italy”)
- Mirror writing

- These are “security through obscurity”

Formatting Messages

- Punctuation and spaces are removed
- Letters are capitalized
- Mono-spaced font
- Five-character groups

- “This is a secret message!” becomes:

```
THISI SASEC RETME SSAGE
```

Transposition Ciphers

- Sender:
  - Rearranges the plaintext letters to get the ciphertext
- Receiver:
  - Undoes the rearrangement to recover the plaintext

- Row/Column Substitution
- Column Transposition
- Route Ciphers

Row/Column Transposition

- Sender:
  - Write plaintext into a grid by rows
  - Read out ciphertext by columns
- Receiver:
  - Write plaintext into grid by columns
  - Read plaintext out by rows
- Key gives the grid dimensions

Example

- Plaintext: `THISI SASEC RETME SSAGE`
- Key: 4 x 5
- Ciphertext: `TSRSH AESIS TASEM GICEE`

T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

Cryptanalysis

- Factor the number of letters to get the grid size

Column Transposition

- Sender:
  - Write plaintext into a grid by rows
  - Shuffle the columns
  - Read out ciphertext by rows
- Receiver:
  - Write plaintext into grid by rows
  - Un-shuffle the columns
  - Read plaintext out by rows
- Key gives the column ordering

Example

- Plaintext: `THISI SASEC RETME SSAGE`
- Key: 21354
- Ciphertext: `HTIIS ASSCE ERTEM SSAEG`

2	1	3	5	4
T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

H	T	I	I	S
A	S	S	C	E
E	R	T	E	M
S	S	A	E	G

Cryptanalysis

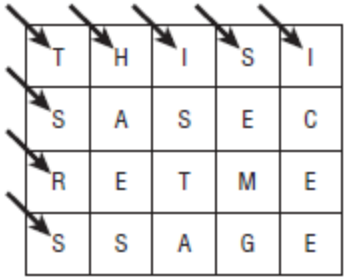
- If there are C columns, there are C! orderings
- For example, 10! = 3,628,800

Route Ciphers

- Sender:
  - Write plaintext into a grid or other arrangement
  - Read out ciphertext by following some path
- Receiver:
  - Write plaintext into grid by following the path
  - Read plaintext out of the grid
- Key gives the path

Example

- Plaintext: `THISI SASEC RETME SSAGE`
- Key: Read down diagonals
- Ciphertext: `SRSSE ATATG HSMEI EESCI`



Cryptanalysis

- If there are N letters, there are N! orderings
- In practice, not all orderings are easy enough to remember

Substitution Ciphers

- Letters in the plaintext are replaced with other letters
  - Caesar Substitution
  - Vigenère Cipher
  - One-Time Pad

Caesar Substitution

- Letters are shifted by some amount
- About 2,100 years ago, Julius Caesar (100 BC–44 BC) used a shift of 3 (A → D, B → E, etc.)
- Julius Caesar's nephew Augustus used a shift of 1

Example

- Plaintext: `THISI SASEC RETME SSAGE`
- Key: 3
- Ciphertext: `WKLVL VDVHF UHWPH VVDJH`

Cryptanalysis

- Letter frequencies

Vigenère Cipher

- Similar to Caesar substitution but a repeating key gives the shift for each message letter

Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E
T	H	I	S	I	S	A	S	E	C	R	E	T	M	E	S	S	A	G	E

- At one time, this cipher was considered unbreakable

Shift Table

Key Letter →

Message Letter ↓

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Cryptanalysis

- Consider every second letter, every third letter, every fourth letter, ..., until you find a frequency distribution that looks like English

One-Time Pad

- Similar to a Vigenère cipher where the key word is as long as the message
- Cross out pad letters as they are used

- Truly unbreakable!

Disadvantages

- The big problem is getting the pad to the receiver

Summary

- Terminology
- Ancient Cryptography
- Transposition Ciphers
  - Row/Column Substitution
  - Column Transposition
  - Route Ciphers
- Substitution Ciphers
  - Caesar Substitution
  - Vigenère Cipher
  - One-Time Pad

Exercises

- Chapter 16 Exercises 1 – 14.
- Read *Essential Algorithms, 2e* Chapter 16 pages 531 – 542. (The rest of Chapter 16.)