Classical Encryption Techniques

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

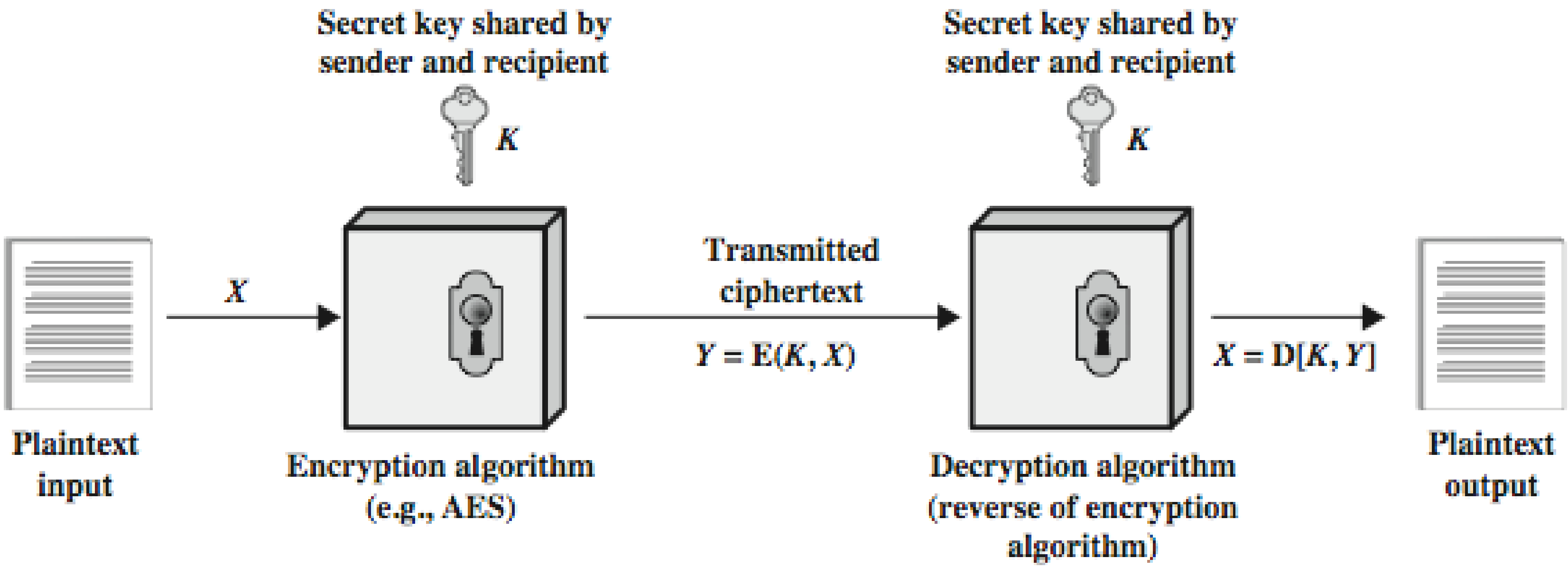
Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-14/

1. Symmetric Cipher Model
2. Substitution Techniques
3. Transposition Techniques
4. Product Ciphers
5. Steganography

These slides are based on Lawrie Brown's slides supplied with William Stalling's book "Cryptography and Network Security: Principles and Practice," 5th Ed, 2011.

Symmetric Cipher Model



$$Y = \mathrm{E}(\mathrm{K}, X)$$
$$X = \mathrm{D}(\mathrm{K}, Y)$$

K=Secret Key

Same key is used for encryption and decryption.

$\Rightarrow$ Single-key or private key encryption.

Example: Divide by 9. $480 = 53 \times 9 + 3 \Rightarrow 531$

Some Basic Terminology

- **Plaintext** - original message
- **Ciphertext** - coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology** - field of both cryptography and cryptanalysis

Cryptography Classification

- By type of encryption operations used
  - Substitution: Meet Me $\Rightarrow$ Offu Of
  - Transposition: Meet Me $\Rightarrow$ Me etM
  - Product
- By number of keys used
  - Single-key or Secret Key
  - Two-key or Public Key
- By the way in which plaintext is processed
  - Block: ABCD EFGH IJKL
  - Stream: ABCDEFGHIJKL

Cryptanalysis

- Objective: To recover key not just message
- Approaches:
  - Cryptanalytic attack
  - Brute-force attack
- If either succeed all key use is compromised
- Brute-force attack:

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^6 years

Substitution

- **Caesar Cipher**: Replaces each letter by 3rd letter on
- Example:

  meet me after the toga party

  PHHW PH DIWHU WKH WRJD SDUWB
- Can define transformation as:

  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

  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
- Mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Then have Caesar cipher as:

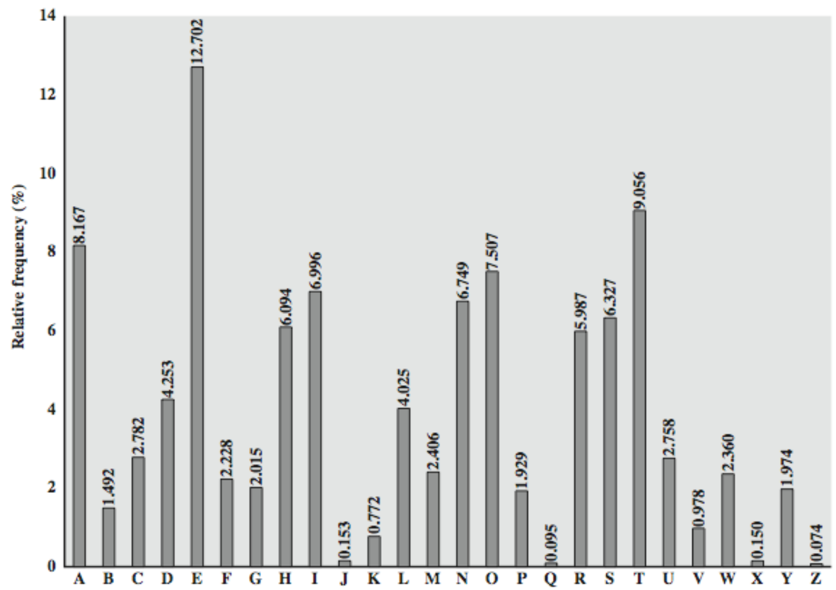
  $c = \mathrm{E}(\mathrm{k}, p) = (p + k) \bmod (26)$

  $p = \mathrm{D}(\mathrm{k}, \mathrm{c}) = (\mathrm{c} - k) \bmod (26)$
- Weakness: Total 26 keys

Substitution: Other forms

- Random substitution:
  Plain: abcdefghijklmnopqrstuvwxyz
  Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

  The key is 26 character long
  => 26! (= 4 x 10^{26}) Keys in place of 26 keys
- Letter frequencies to find common letters: E,T,R,N,I,O,A,S



Substitution: Other forms (Cont)

- Use two-letter combinations: Playfair Cipher
- Use multiple letter combinations: Hill Cipher

Poly-alphabetic Substitution Ciphers

- Use multiple ciphers. Use a key to select which alphabet (code) is used for each letter of the message
- Vigenère Cipher: Example using keyword *deceptive*

  key: deceptivedeceptivedeceptive

  plaintext: wearediscoveredsaveyourself

  ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

One-Time Pad

- If a truly random key as long as the message is used, the cipher will be secure
- Called a One-Time pad
- Is unbreakable since ciphertext bears no statistical relationship to the plaintext
- Since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- Can only use the key **once** though
- Problems in generation & safe distribution of key

Transposition (Permutation) Ciphers

- Rearrange the letter order without altering the actual letters
- **Rail Fence Cipher**: Write message out diagonally as:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

- Giving ciphertext: MEMATRHTGPRYETEFETEOAAT
- **Row Transposition Ciphers**: Write letters in rows, reorder the columns according to the key before reading off .

Key: 4312567

Column Out 4 3 1 2 5 6 7

Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

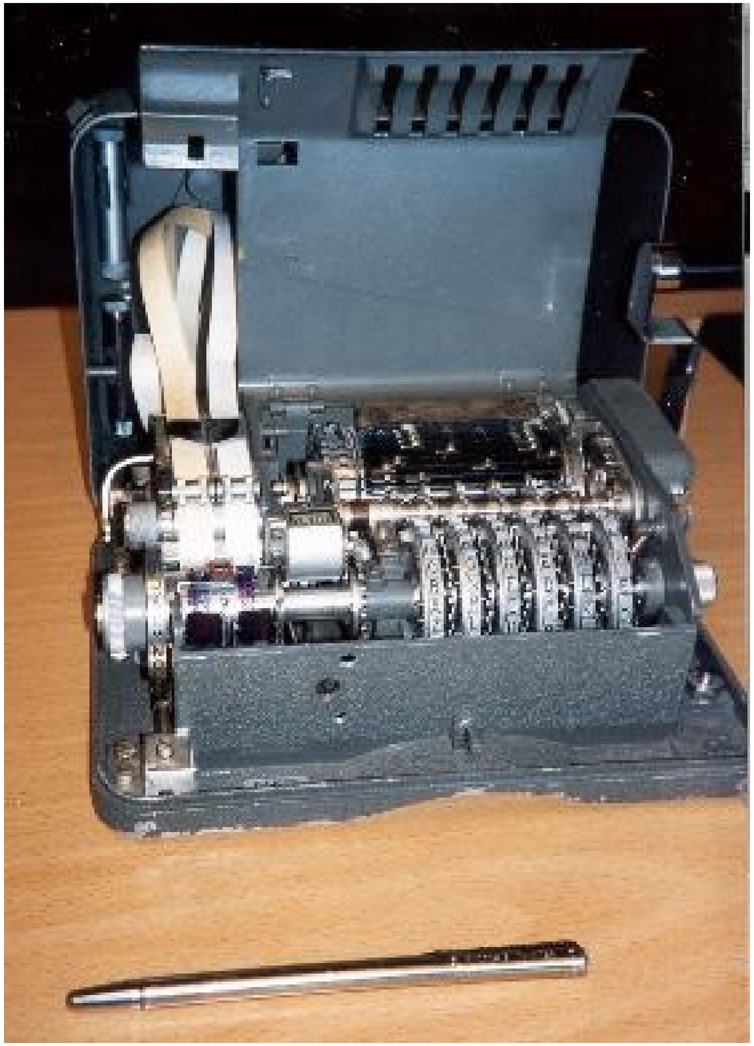
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Product Ciphers

- Use several ciphers in succession to make harder, but:
  - Two substitutions make a more complex substitution
  - Two transpositions make more complex transposition
  - But a substitution followed by a transposition makes a new much harder cipher
- This is a bridge from classical to modern ciphers

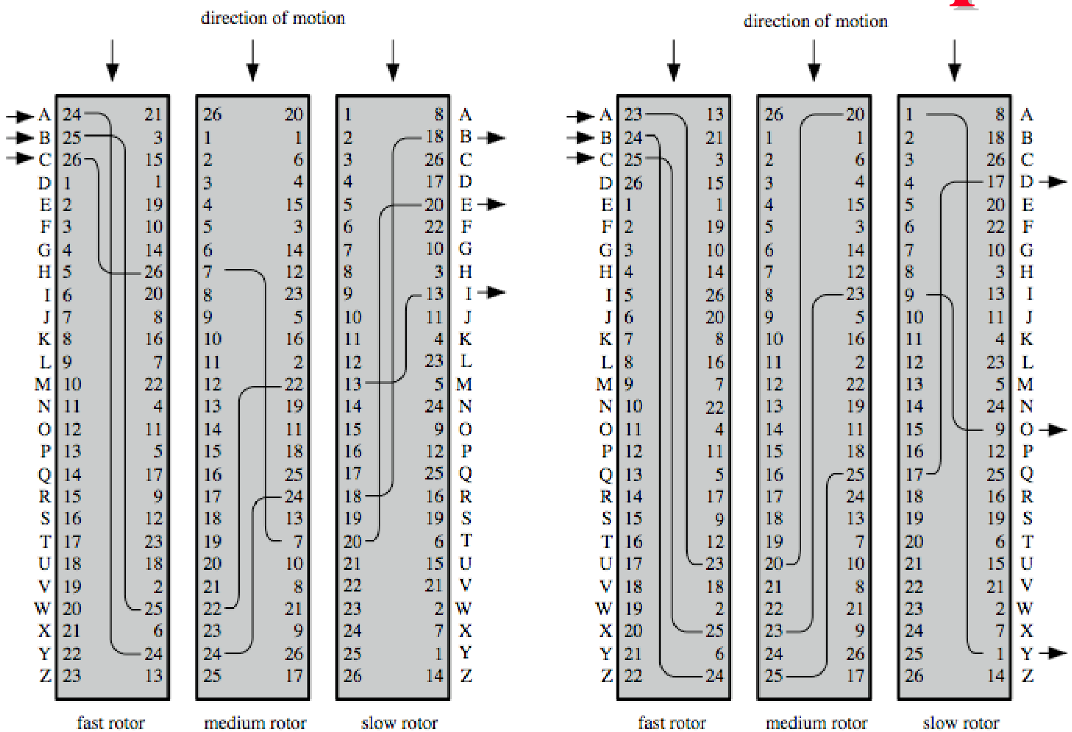
Rotor Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WW2
  - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher
- Used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted



Hagelin Rotor Machine

Rotor Machine Principle



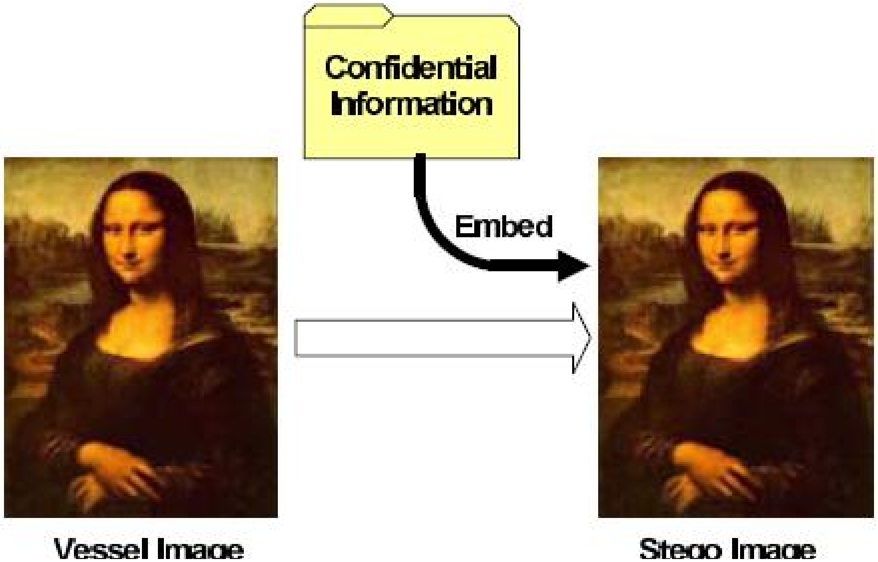
(a) Initial setting

(b) Setting after one keystroke

- A becomes Y (First rotor). Y becomes R (2nd rotor). R becomes B (3rd rotor).
- After each letter, first rotor moves 1 position. After each full rotation of 1st rotor, 2nd rotor moves by 1 position.
- Cycle length = 26^3

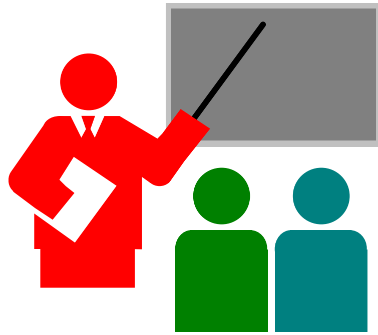
Steganography

- Hide characters in a text, hide bits in a photograph
- Least significant bit (lsb) of a digital photograph may be a message.
- Drawback: high overhead to hide relatively few info bits
- Advantage: Can obscure encryption use



Ref: http://www.cse.wustl.edu/~jain/cse571-09/ftp/stegano/index.html

Summary



1. The key methods for cryptography are: Substitution and transposition
2. Letter frequency can be used to break substitution
3. Substitution can be extended to multiple letters and multiple ciphers. Mono-alphabetic=1 cipher, Poly-alphabetic=multiple ciphers
4. Examples: Caesar cipher (1 letter substitution), Playfair (2-letter), Hill (multiple letters), Vigenere (poly-alphabetic).
5. Multiple stages of substitution and transposition can be used to form strong ciphers.

Homework 2

- Submit solution to problem 2.18

2.18 This problem explores the use of a one-time pad version of the Vigenere cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5…, then the first letter of the plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

A. Encrypt the plain text sendmoremoney with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9

B. Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plain text cashnotneeded.