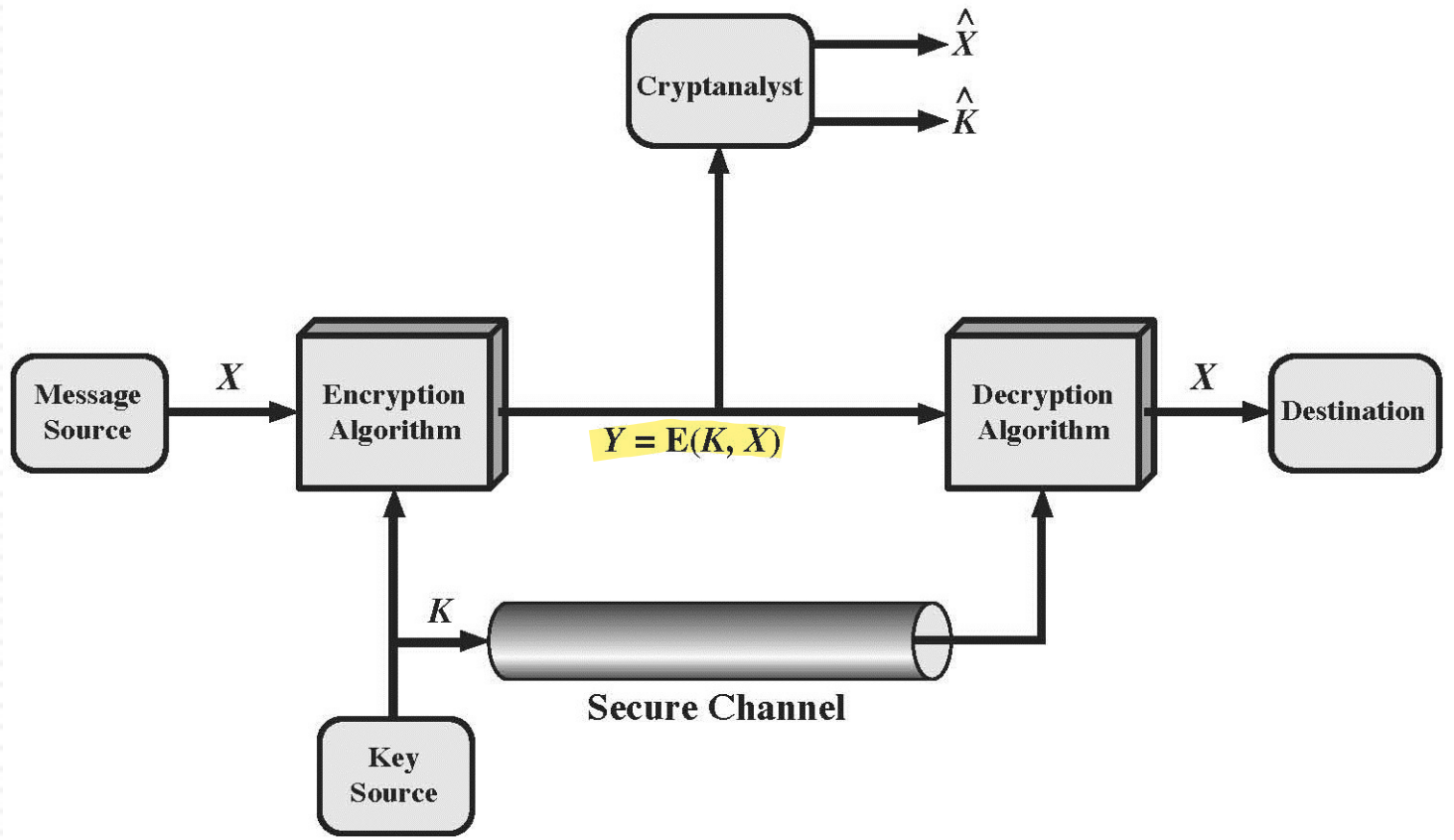
CLASSICAL ENCRYPTION TECHNIQUES
LECTURE 2

Cryptography

Basic Terminology

- *plaintext*
- *ciphertext*
- *cipher*
- *key*
- *encipher* (*encrypt*)
- *decipher* (*decrypt*)
- *cryptography*
- *cryptanalysis* (*codebreaking*)
- *cryptology*

Symmetric Cryptosystem



Cryptography

- Can characterize cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - product
  - number of keys used
    - single-key or secret
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Cryptanalysis

- Objective to recover key not just message
- General approaches:
  - cryptanalytic attack
  - brute-force attack

Cryptanalytic Attacks

- ciphertext only
  - only know algorithm & ciphertext
- known plaintext
  - know/suspect plaintext & ciphertext
- chosen plaintext
  - select plaintext and obtain ciphertext
- chosen ciphertext
  - select ciphertext and obtain plaintext
- chosen text
  - select plaintext or ciphertext to en/decrypt

More Definitions

- Unconditional security
  - No matter how much computer power or time is available, the cipher cannot be broken
- Computational security
  - Given limited computing resources (e.g. time), the cipher cannot be broken

Brute Force Search

- Always possible to simply try every key
- Most basic attack, proportional to key size

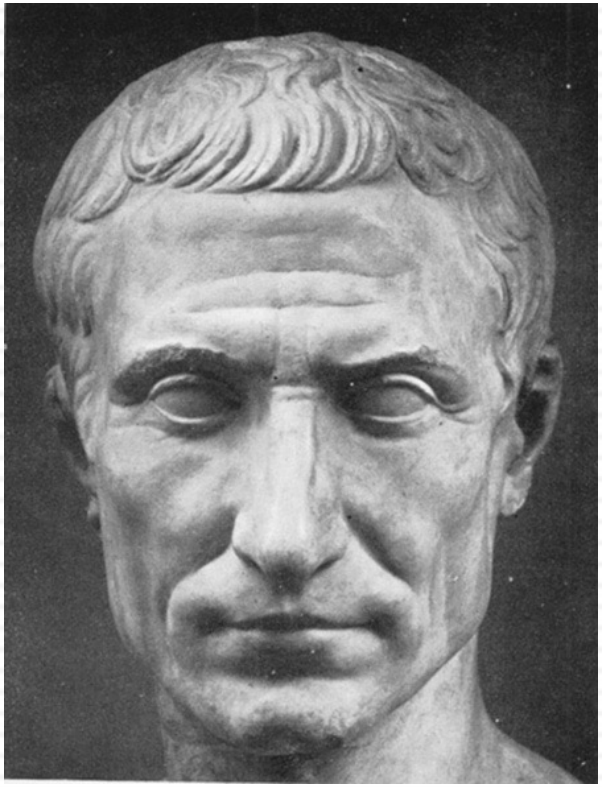
average

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

1.2 x 10^4 years? 3 x 10^4 years? 2 x 10^8 years? 4.6 x 10^9 years?

Caesar Cipher

PHHW PH DIWHU WKH WRJD SDUWB



Cryptanalysis of Caesar Cipher

GCUA VQ DTGCM

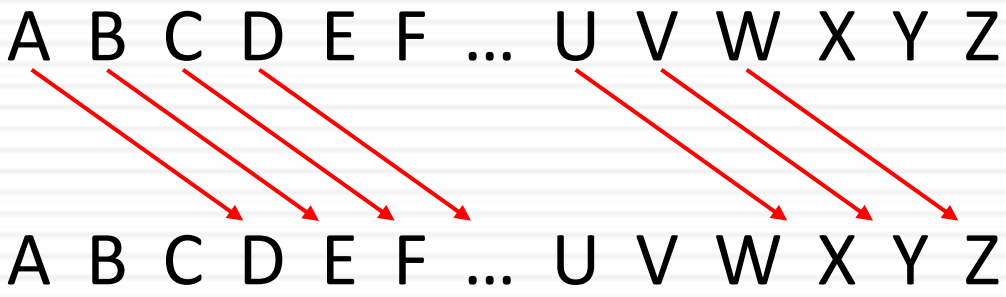
- Only have 26 possible ciphers
- Could simply try each in turn (brute force search)

Monoalphabetic Cipher

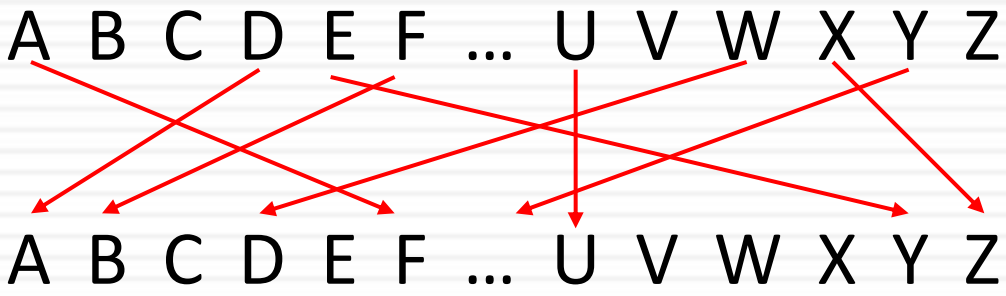
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDB
METSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZW
YMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJU
DTMOHMQ

- Each plaintext letter maps to a different random ciphertext letter

Caesar VS. Monoalphabetic



"regular"
26 total



"random"
26! total

Monoalphabetic Cipher

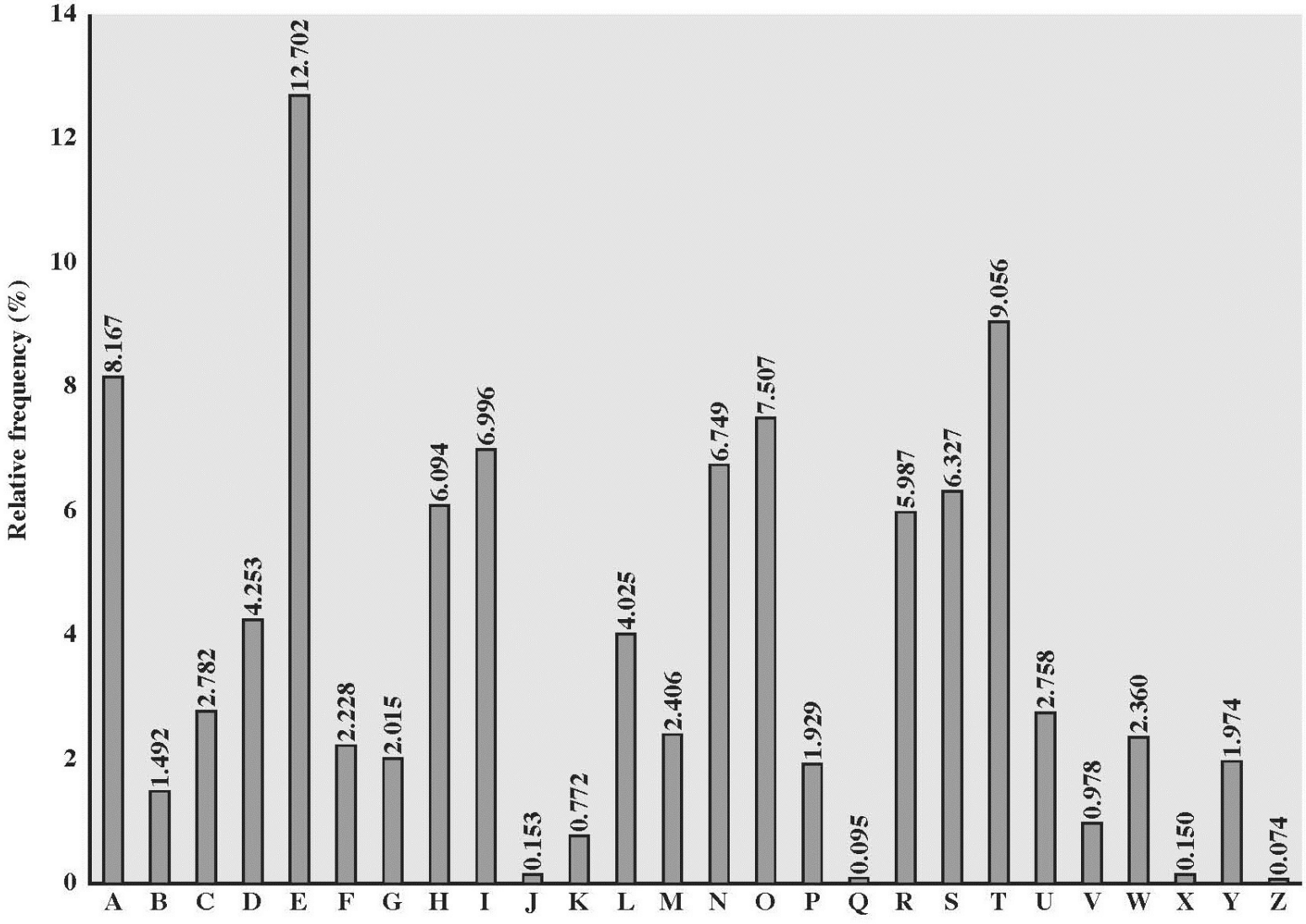
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDB
METSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZW
YMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJU
DTMOHMQ

- Each plaintext letter maps to a different random ciphertext letter
  - $26! = 4 \times 10^{26}$ different mappings
  - Is it safe?

Language Redundancy

- Human languages are *redundant*
- Letters are not equally commonly used
- In English E is by far the most common letter
  - followed by T, R, N, I, O, A, S
- Other letters like Z, J, K, Q, X are fairly rare
- Have tables of single, double & triple letter frequencies for various languages

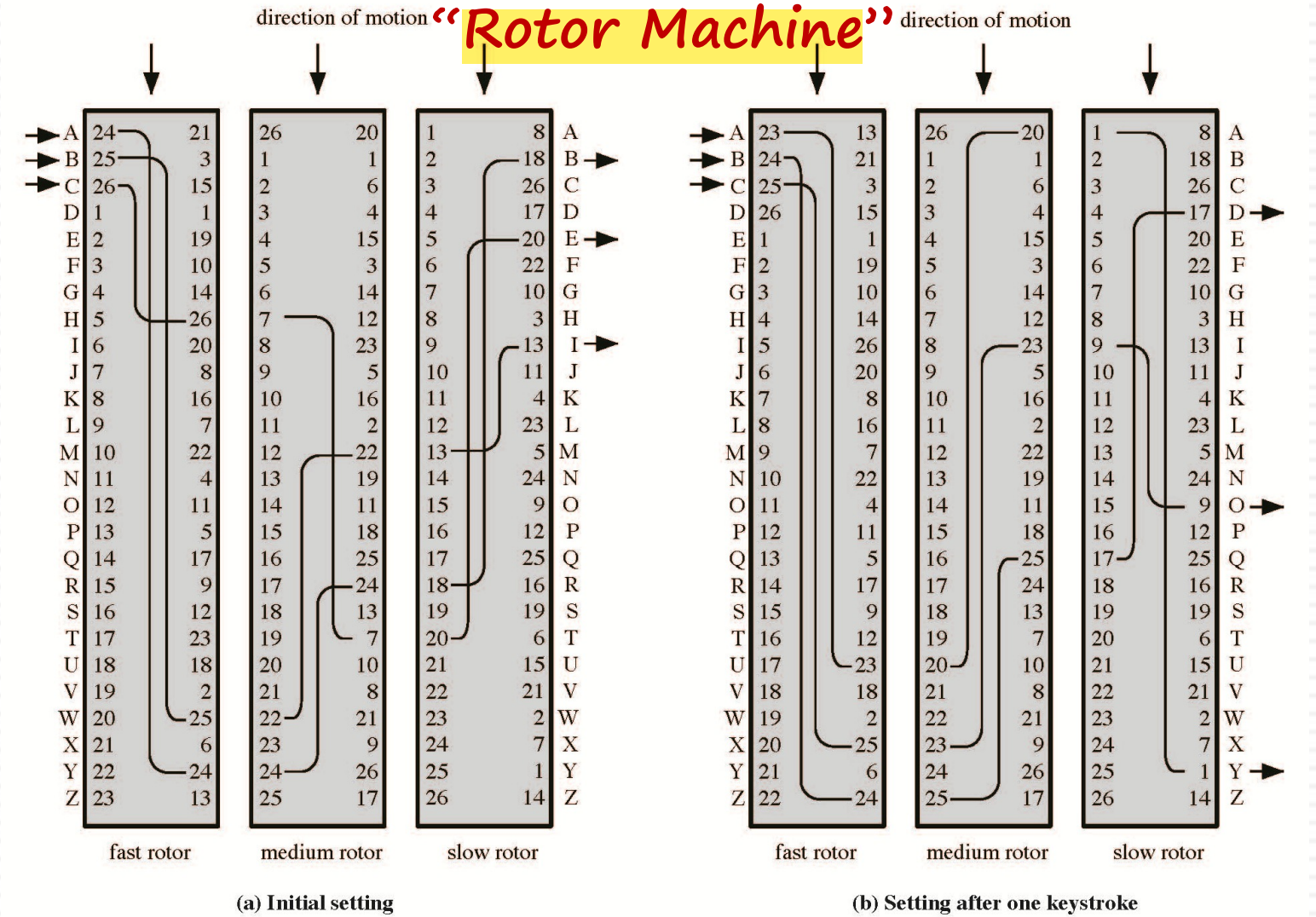
English Letter Frequencies



Use in Cryptanalysis

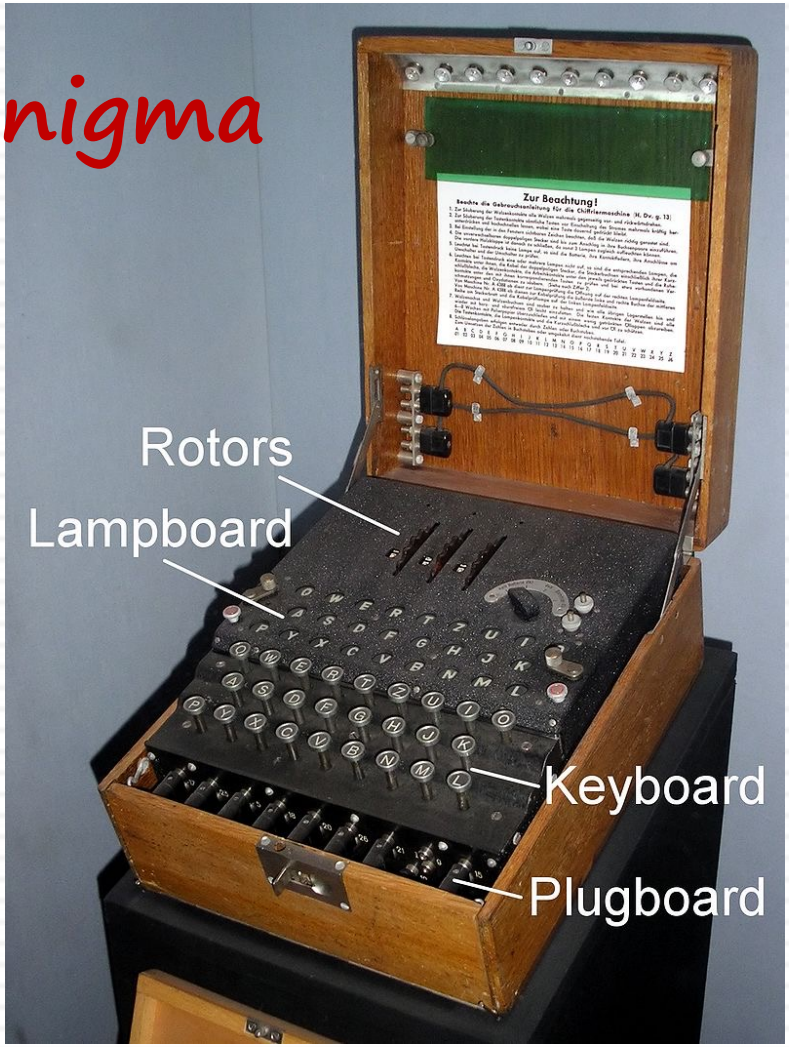
- Key concept
  - monoalphabetic substitution ciphers do not change relative letter frequencies
- Calculate letter frequencies for ciphertext
- Compare counts/plots against known values
- For monoalphabetic must identify each letter
  - tables of common double/triple letters help

Polyalphabetic Ciphers

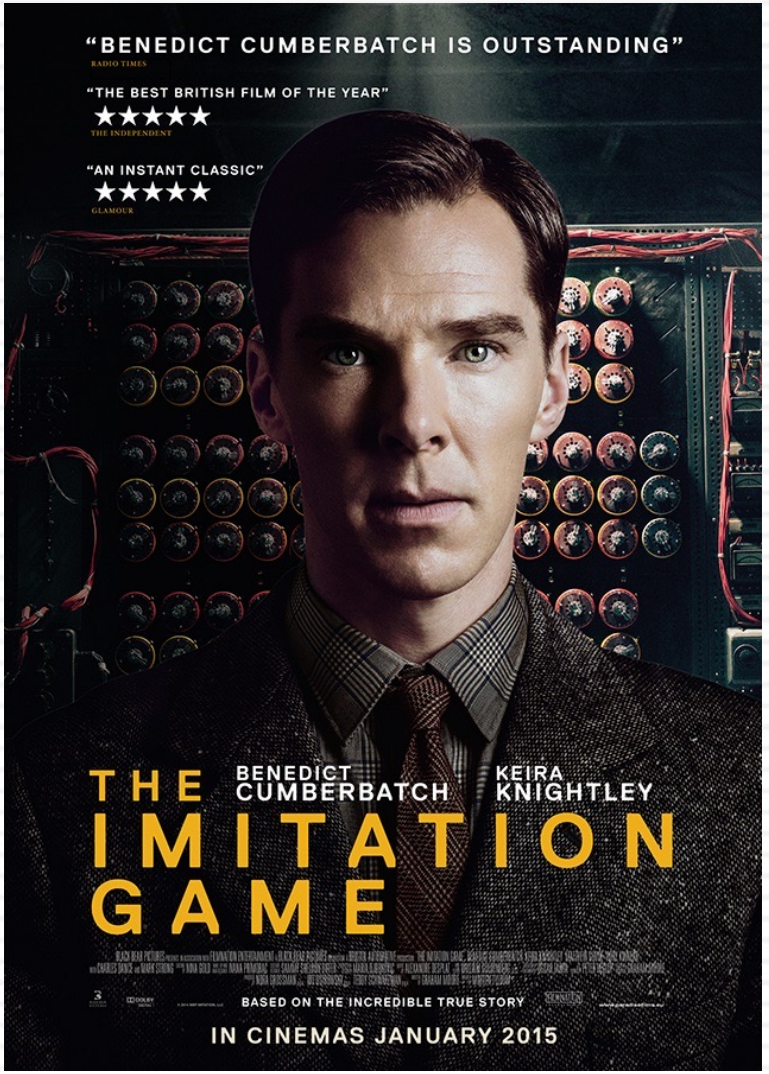


Rotor Machines

Hagelin



Enigma Machine



Polyalphabetic Ciphers

- Improve security using *multiple* cipher alphabets
- Make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- Use a key to select which alphabet is used for each letter of the message
- Use each alphabet in turn
- Repeat from start after end of key is reached

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
- Can only use the key *once* though
- Problems in generation & safe distribution of key

Transposition Ciphers

MEMATRHTGPRYETEFETEOAAT

M E M A T R H T G P R Y

E T E F E T E O A A T

"Rail Fence cipher"

- Hide the message by rearranging the letter order without altering the actual letters used
- Can recognize these since have the *same frequency distribution* as the original text

Row Transposition Ciphers

TTNAAPTMTSUOAODWCOIXKNLYPETZ

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

Product Ciphers

- Ciphers using substitutions or transpositions are *not* secure because of language characteristics
- Hence consider using *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 bridge from classical to modern ciphers

Steganography