

2/23/2005



# Simple Encryption Techniques

- Mono-Alphabetic Cipher
  - Caesar Cipher
  - Substitution Cipher

# Notation

- Plaintext -  $p$
- Cipher text -  $c$
- Key -  $k$
- Arbitrary Integer -  $n$

# What is Caesar Cipher

- Also known as Caesar Shift Cipher or Shift Cipher
- Named for Julius Caesar
- One of the earliest and simplest encryption algorithms
- Shift characters right by some set key value,  $k$

# Caesar Cipher

# Caesar Cipher

- Shift alphabet  $n$  places right

# Caesar Cipher

- Shift alphabet  $n$  places right
- Encryption:  $c = (p + n) \bmod 26$

# Caesar Cipher

- Shift alphabet  $n$  places right
- Encryption:  $c = ( p + n ) \bmod 26$
- Decryption:  $p = ( c - n ) \bmod 26$

# Caesar Cipher

- Shift alphabet  $n$  places right
- Encryption:  $c = ( p + n ) \bmod 26$
- Decryption:  $p = ( c - n ) \bmod 26$
  
- For Caesar Cipher,  $k = n$

# Caesar Cipher Example

# Caesar Cipher Example

- Key,  $k = 5$

# Caesar Cipher Example

- Key,  $k = 5$
- Alphabet translation:

# Caesar Cipher Example

- Key,  $k = 5$
- Alphabet translation:  
– abcdefghijklmnopqrstuvwxyz

# Caesar Cipher Example

- Key,  $k = 5$
- Alphabet translation:
  - abcdefghijklmnopqrstuvwxyz
  - FGHIJKLMNOPQRSTUVWXYZABCDE

- Key,  $k = 5$

- Alphabet translation:

  - abcdefghijklmnopqrstuvwxyz

  - FGHIJKLMNOPQRSTUVWXYZABCDE

- Key,  $k = 5$

- Alphabet translation:

–abcdefghijklmnopqrstuvwxyz

–FGHIJKLMNOPQRSTUVWXYZABCDE

Plaintext:

thiscaesarcipherisajoke

- Key,  $k = 5$

- Alphabet translation:

–abcdefghijklmnopqrstuvwxyz

–FGHIJKLMNOPQRSTUVWXYZABCDE

Plaintext:

thiscaesar cipher is a joke

Cipher text:

YMNXFJXFWHNUMJWNXFOTPJ

# What's Wrong with Caesar Cipher

# What's Wrong with Caesar Cipher

- It's easy to break!

# What's Wrong with Caesar Cipher

- It's easy to break!
- How many keys?

# What's Wrong with Caesar Cipher

- It's easy to break!
- How many keys?
- Only 25!!

How Can We Automate?

# How Can We Automate?

- Shift 1, show to user for approval, on failure shift by 1 again, repeat

# How Can We Automate?

- Shift 1, show to user for approval, on failure shift by 1 again, repeat
- If spaces are used, word boundaries are easy
  - Repeated letters (i.e. look, book, ...)
  - Small words (i.e. is, on, the, ...)

# How Can We Automate?

- Shift 1, show to user for approval, on failure shift by 1 again, repeat
- If spaces are used, word boundaries are easy
  - Repeated letters (i.e. look, book, ...)
  - Small words (i.e. is, on, the, ...)
- Use a dictionary to recognize words

# How Can We Automate?

- Shift 1, show to user for approval, on failure shift by 1 again, repeat
- If spaces are used, word boundaries are easy
  - Repeated letters (i.e. look, book, ...)
  - Small words (i.e. is, on, the, ...)
- Use a dictionary to recognize words
- ...

# Try It Yourself

KWW, A LGDV QGM AL OSK WSKQ.

FGO DWL 'K EGNW GF LG

KGEWLZAFY S DALLDW

EGJW VAXXAUMDL.

# Try It Yourself

KWW, A LGDV QGM AL OSK WSKQ.

FGO DWL 'K EGNW GF LG

KGEWLZAFY S DALLDW

EGJW VAXXAUMDL.

$$k = 18$$

# Try It Yourself

SEE, I TOLD YOU IT WAS EASY.

NOW LET'S MOVE ON TO

SOMETHING A LITTLE

MORE DIFFICULT.

$$k = 18$$

# How Can We Improve Caesar Cipher?

# How Can We Improve Caesar Cipher?

- Don't shift, substitute....

What is a Substitution Cipher?

# What is a Substitution Cipher?

- Create a table of the alphabet and a scrambled alphabet, replace accordingly

# What is a Substitution Cipher?

- Create a table of the alphabet and a scrambled alphabet, replace accordingly
- Number of keys?

# What is a Substitution Cipher?

- Create a table of the alphabet and a scrambled alphabet, replace accordingly
- Number of keys?
- $(26! - 1)$  keys
  - $4.032914611266057e+26$

# What is a Substitution Cipher?

- Create a table of the alphabet and a scrambled alphabet, replace accordingly
- Number of keys?
- $(26! - 1)$  keys
  - $4.032914611266057e+26$
- For substitution,  $k = \text{Scrambled Alphabet}$

# Substitution Example

# Substitution Example

- Alphabet translation:
  - abcdefghijklmnopqrstuvwxyz
  - JLD SGZYBUHEMWOQT CARXKFNIVP

# Substitution Example

- Alphabet translation:
  - abcdefghijklmnopqrstuvwxyz
  - JLDSGZYBUHEMWOQTCARXKFNIVP
- Key,  $k = \text{JLDSGZYBUHEMWOQTCARXKFNIVP}$

- Alphabet translation:

- abcdefghijklmnopqrstuvwxyz

- JLDSGZYBUHEMWOQTCARXKFNI VP

- Alphabet translation:

–abcdefghijklmnopqrstuvwxyz

–JLDSGZYBUHEMWOQTCARXKFNIVP

Plaintext:

substitutionisbetterbutnotgreat

- Alphabet translation:

–abcdefghijklmnopqrstuvwxyz

–JLDSGZYBUHEMWOQTCARXKFNIVP

Plaintext:

substitutionisbetterbutnotgreat

Cipher text:

RKLRXUXKUQOURLGXXGALKXOQXYAGJX

# What's Wrong with Substitution Cipher

- It is easy to break by a computer
- Is still susceptible to:
  - Detecting Repeated Words
  - Detecting Small Words
  - Dictionary Attacks
  - ...

# Try It Yourself

WSCF CF RGFW NXP G FLGEE

LRFFGUR ZHW DGY WIH

CLGUCYR G EIYU IYR?

# Try It Yourself

WSCF CF RGFW NXP G FLGEE

LRFFGUR ZHW DGY WIH

CLGUCYR G EIYU IYR?

Key,  $k =$  GZDQRNUSCOAELYIBXPFWHJVKWM

# Try It Yourself

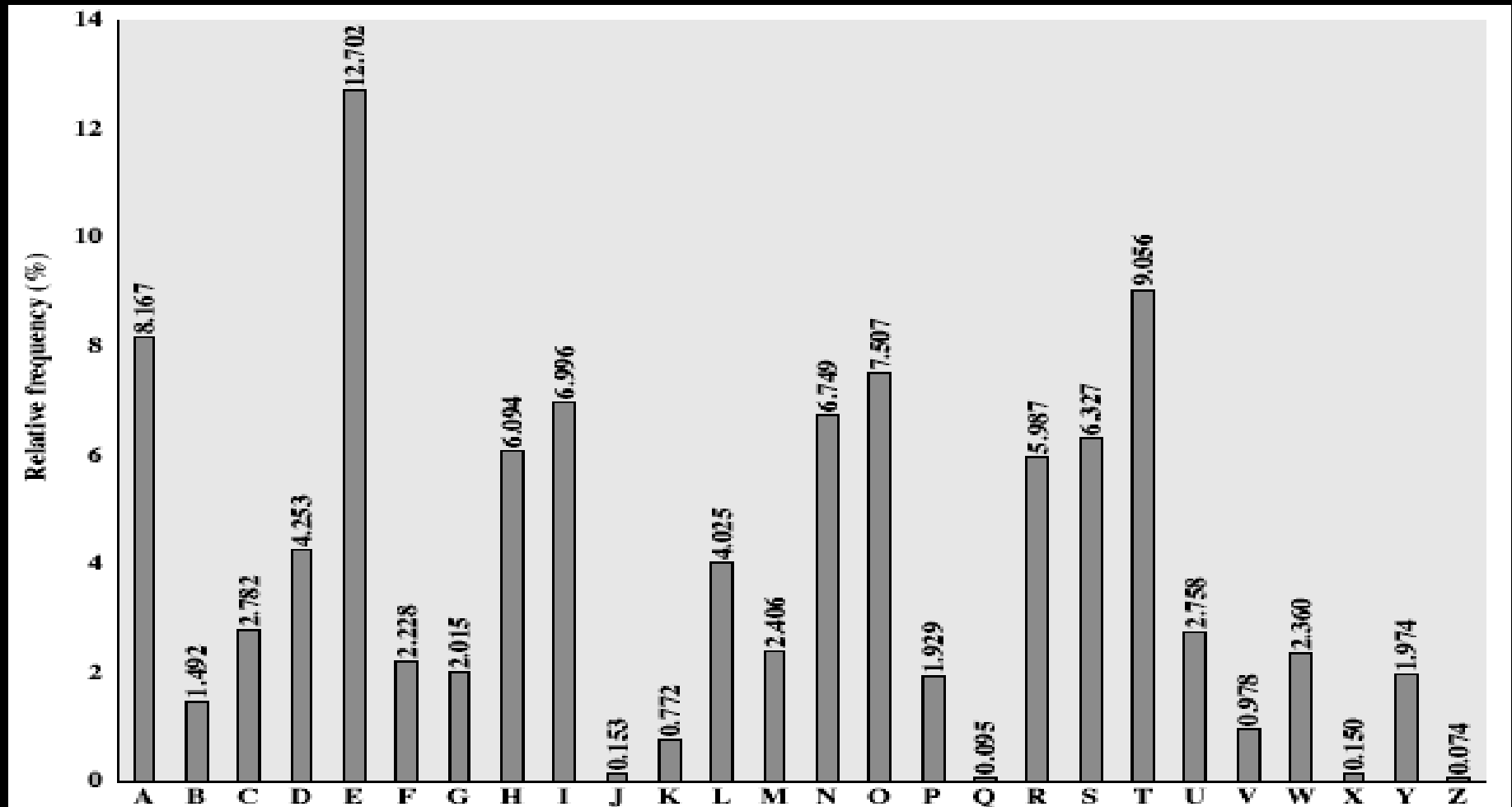
This is easy for a small  
message but can you  
imagine a long one?

Key,  $k$  = GZDQRNUSCOAELYIBXPFWHJVKWM

# Cracking via Frequency Distribution

- Fancy name, simple concept
  - Count how many times each encrypted letter appears, then compare to a graph of which letters appear how often
  - This can also be applied to sets of letters
    - i.e. -sh, -ch, -st, ...
  - Or small words
    - i.e. of, on, the, ...

# Frequency Distribution for English Alphabet



# Other Frequency Distributions

- Digraph frequencies:
  - th, he, in, er, an, re, on, en, at, es, ed, te, ti, or, st, ar, nd, to, nt, is, of, it, al, as, ha, ng, co, se, me, de
- Double letter frequencies:
  - ll, ee, ss, tt, oo, mm, ff, pp, rr, nn, cc, dd
- ...

# Try It Yourself

RCJEWLEPWDCYHSQPPMHEJPLYH

WEQUJQYTRALPWELXJWLICYKMPYCWCC

XMAELHBW? XJW, TMYRCJACLWMHMLY?

BCK MPW?

# Try It Yourself

RCJEWLEPWDCYHSQPPMHEJPLYH

WEQUJQYTRALPWELXJWLICYKMPYCWCC

XMAELHBW? XJW, TMYRCJACLWMHMLY?

BCK MPW?

Key,  $k$  = MXTAQWHBLZODSYCVUEPWJGKNRI

# Try It Yourself

Your first long message using frequency distribution was not too bad right? But, can you do it again? How fast?

Key,  $k =$  MXTAQWHBLZODSYCVUEPWJGKNRI

# Try It Yourself

CP DWB ZEOQ ND ZFT YOW ZPLMCHEOQ  
CEPQ C PJVUA ELVHH VW BF OO UP  
QRBEVDU. N LRTDU'E RDZNO VE OC  
BQDAQC W EDTDV EMDQR DZ? VEPD ZF  
T YOQO CFFRMCH E VM VE VHH WC QE  
OUD ZAL.

# Try It Yourself

CP DWB ZEOQ ND ZFT YOW ZPLMCHEOQ  
CEPQ C PJVUA ELVHH VW BF OO UP  
QRBEVDU. N LRTDU'E RDZNO VE OC  
BQDAQC W EDTDV EMDQR DZ? VEPD ZF  
T YOQO CFFRMCH E VM VE VHH WC QE  
OUD ZAL.

Key,  $k$  = CYPTOMALVSJFWUDBXQHEZKNGRI

# Try It Yourself

A computer would be much faster at cracking this simple encryption. Why don't you write a program to do it for you? It could be really fast if it is smart enough.

Key,  $k$  = CYPTOMALVSJFWUDBXQHEZKNGRI

# Real World Example

RE. RQCOSM VQDEOVJ

7208 IWBS IV.

EWMMQ, BW 13897

(350) 087 - 3333

HOIQ: 9209 9494 7856 1293

SUKOESI: 97/93

# Real World Example

RE. RQCOSM VQDEOVJ

7208 IWBS IV.

EWMMQ, BW 13897

(350) 087 - 3333

HOIQ: 9209 9494 7856 1293

SUKOESI: 97/93

Key,  $k$  = QZPRSTALONYMBCWKXEIVDHGUFJ 9720831564

# Real World Example

Dr. Daniel Tauritz

1234 Some St.

Rolla, MO 65401

(573) 341 - 5555

Visa: 0230 0909 1478 6215

Expires: 01/05

Key,  $k$  = QZPRSTALONYMBCWKXEIVDHGUFJ 9720831564

# Real World Encryption

- Obviously substitution ciphers... suck
- Better Algorithms
  - Public-Key Encryption
    - RSA, DSA
  - Symmetric-Key Encryption
    - DES, 3DES, AES
  - The Future of Encryption?
    - Elliptic Curve, Quantum

# More Information

- More Frequency Distribution Information
  - <http://www.cahlander.com/crypto/cryptopop.html>
- More Encryption Algorithms
  - “Applied Cryptography” by Bruce Schneier
    - Available at UMR Library
- NIST Encryption Standards
  - <http://csrc.nist.gov/CryptoToolkit/>