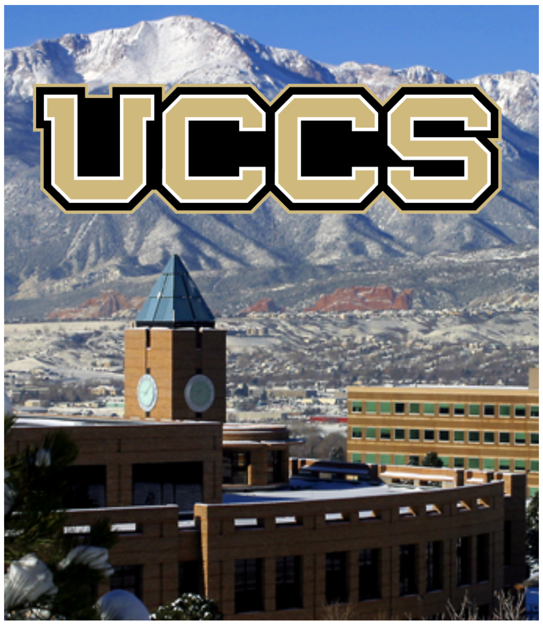


Symmetric Cryptography

Classical Cipher: Substitution

Sang-Yoon Chang, Ph.D.

Module Objectives:
Classical Cipher: Substitution

Substitution Cipher

Modulo Operations

Caesar Cipher, Monoalphabetic Cipher, Polyalphabetic Cipher, Vigenere Cipher

Module Objectives:
Classical Cipher: Substitution

Substitution Cipher

Modulo Operations

Caesar Cipher, Monoalphabetic Cipher,
Polyalphabetic Cipher, Vigenere Cipher

History of Cryptography

Long history of at least 4000 years

Alphabet (Merriam-Webster Dictionary)

1. “A set of letters or other characters with which one or more languages are written especially if arranged in a customary order”

2. “A system of signs or signals that serve as equivalents for letters”

Alphabet (in Cryptography)

Minimal unit for information coding

Can be letters, numbers, signs, etc.

Alphabet set depends on the information coding scheme/system

Alphabet (in Cryptography)

English: {a, b, c, …, z}

Morse Code: {., -}

Computer Bits: {1,0}

Decimal: {0,1,2, …, 9}

Hexadecimal: {0,1,2, … F}

Alphabet (in Cryptography)

Alphabet Size

English: {a, b, c, …, z} 26

Morse Code: {., -} 2

Computer Bits: {1,0} 2

Decimal: {0,1,2, …, 9} 10

Hexadecimal: {0,1,2, … F} 16

Substitution Cipher

Each alphabet in the plaintext is replaced by another alphabet to generate ciphertext

Caesar Cipher

Earliest known substitution cipher

Replaces each alphabet with the alphabet after shifting “*x*” times to the right

The amount of shift (*x*) is the key

Caesar Cipher Example

$x = 2$ ← Key

A → C

B → D

C → E

…

Caesar Cipher Example

x = 2 ← Key

A → C

B → D

C → E

…

Plaintext:

MEET ME LATER

Ciphertext:

OGGV OG NCVGT

Caesar Cipher Example

x = 4 ← Key

A → E

B → F

C → G

…

Plaintext:

MEET ME LATER

Ciphertext:

QIIX QI PEXIV

Caesar Cipher Example

x = 26 ← Key

A → A

B → B

C → C

…

Plaintext:

MEET ME LATER

Ciphertext:

MEET ME LATER

Caesar Cipher Example

$x = 26 \cdot i + 4 = 4$, for any integer i

A → E

B → F

C → G

…

Plaintext:

MEET ME LATER

Ciphertext:

QIIX QI PEXIV

Caesar Cipher on English Plaintext

Possible keys are {0,1,…,25}

Key size is equal to the size of
the plaintext alphabet (26)

$x = 26 \cdot i + a = a$, where i is an integer
E.g., $x = 25 = -1 = 51 = 77 = \ldots$

Caesar Cipher on English Plaintext

Possible keys are {0,1,…,25}

Key size is equal to the size of the plaintext alphabet (26)

$x = 26 \cdot i + a = a$, where i is an integer
E.g., $x = 25 = -1 = 51 = 77 = \ldots$

Modulo Operation Definitions

"*a* mod *n*" is the remainder when *a* is divided by *n* (where *n* is positive and called **modulus**)

If $a = q \cdot n + r$, for any integer q,
$r = a \bmod n$

If (a mod n) = (b mod n),
a* and *b* are congruent modulo *n
and $a \equiv b \pmod{n}$

Modulo Operation Definitions

12 mod 7 = 5

$12 = 7 \cdot 1 + 5$ "$a = q \cdot n + r$"

7 is modulus (positive)

Modulo Operation Definitions

$-11 \bmod 7 = 3$

$-11 = 7 \cdot (-2) + 3$ “$a = q \cdot n + r$”

7 is modulus (positive)

Modulo Operation Definitions

$\ldots \equiv -9 \equiv -2 \equiv 5 \equiv 12 \equiv 19 \equiv \ldots \pmod 7$

(mod *n*) operator maps all integers into the set of integers between 0 and n-1

$Z_n = \{0, 1, \ldots, (n-1)\}$ is **residue classes**

Modulo Operation Definitions

Each integer in Z_n represents residue class:
$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$
E.g., the residue classes (mod 7) are:
$[0] = \{..., -21, -14, -7, 0, 7, 14, 21, 28, ...\}$
$[1] = \{..., -20, -13, -6, 1, 8, 15, 22, 29, ...\}$
...
$[6] = \{..., -15, -8, -1, 6, 13, 20, 27, 34, ...\}$

Finding the smallest nonnegative *r* to which $a \equiv r \pmod{n}$ is called **reducing *a* modulo *n***

Caesar Cipher Example

x = 4 ← Key

A → E

B → F

C → G

…

Plaintext:

MEET ME LATER

Ciphertext:

QIIX QI PEXIV

Coding Letters to Numbers

A → 0

B → 1

C → 2

…

Z → 25

Caesar Cipher Using English Letters

Encryption:

c = E(x, p) = (p + x) mod 26

Decryption:

p = D(x, c) = (c – x) mod 26

The keys are equivalent if they are
in the same residue class mod 26

Caesar Cipher Limitation 

Key size is equal to the size of
the plaintext alphabet
(e.g., 26 for English letters)

Small key size

Vulnerable to brute force attack

Monoalphabetic Cipher

Each plaintext alphabet is assigned to
a different unique ciphertext alphabet

Key assigns the mapping for each alphabet

Key is a permutation of alphabet set
(n! permutations for n-element set)

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

A → D

B → K

C → V

…

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATER

Ciphertext: ?

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATER

Ciphertext: CFFUCFSDUFY

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATER

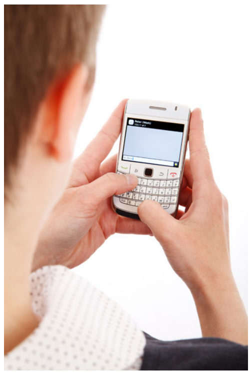
Ciphertext: CFFUCFSDUFY

Monoalphabetic Cipher

The possible number of keys is $n!$
where n is the plaintext alphabet size

E.g., $n=26$
Possible number of keys is $26! > 4 \cdot 10^{26}$

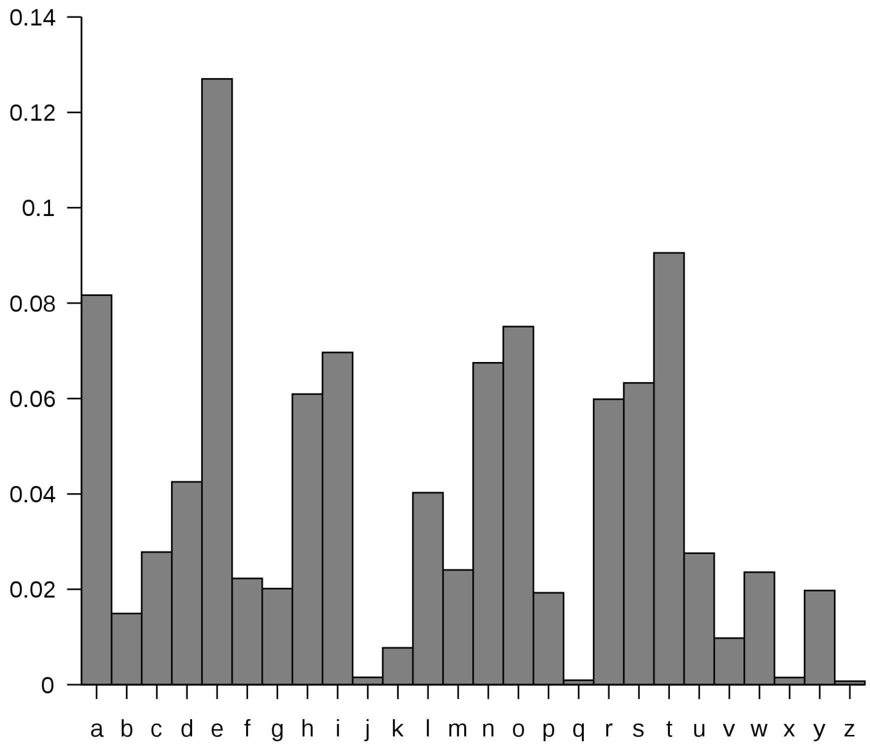
Plaintext's Natural Redundancy



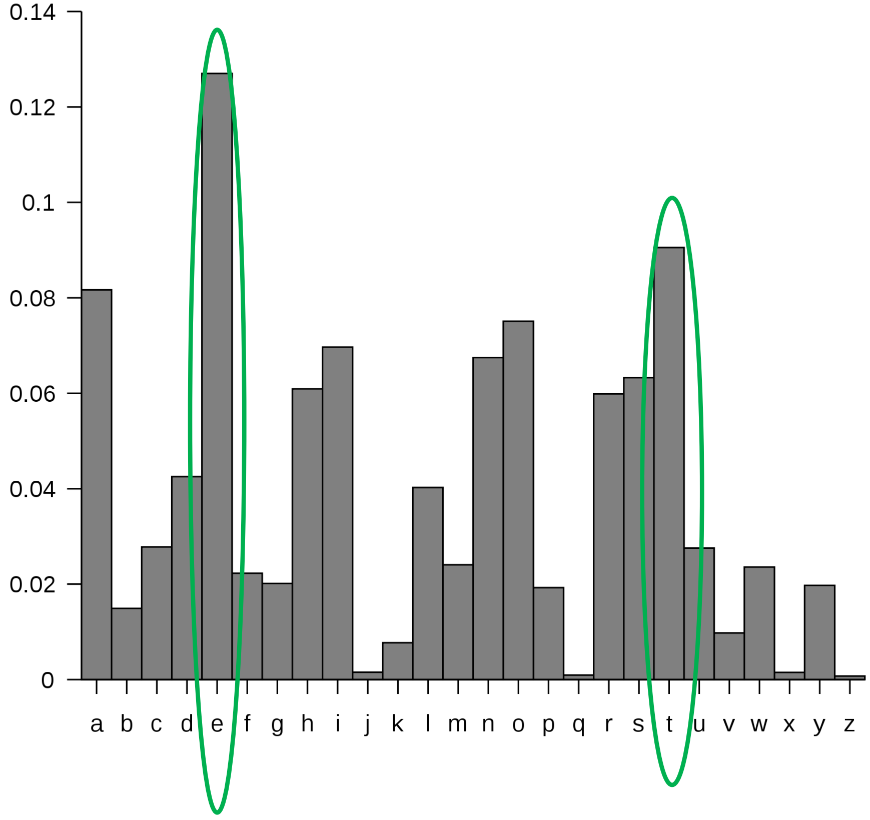
Natural redundancy and biases exist in plaintext

Such plaintext biases can be used for cryptanalysis, e.g., against monoalphabetic cipher

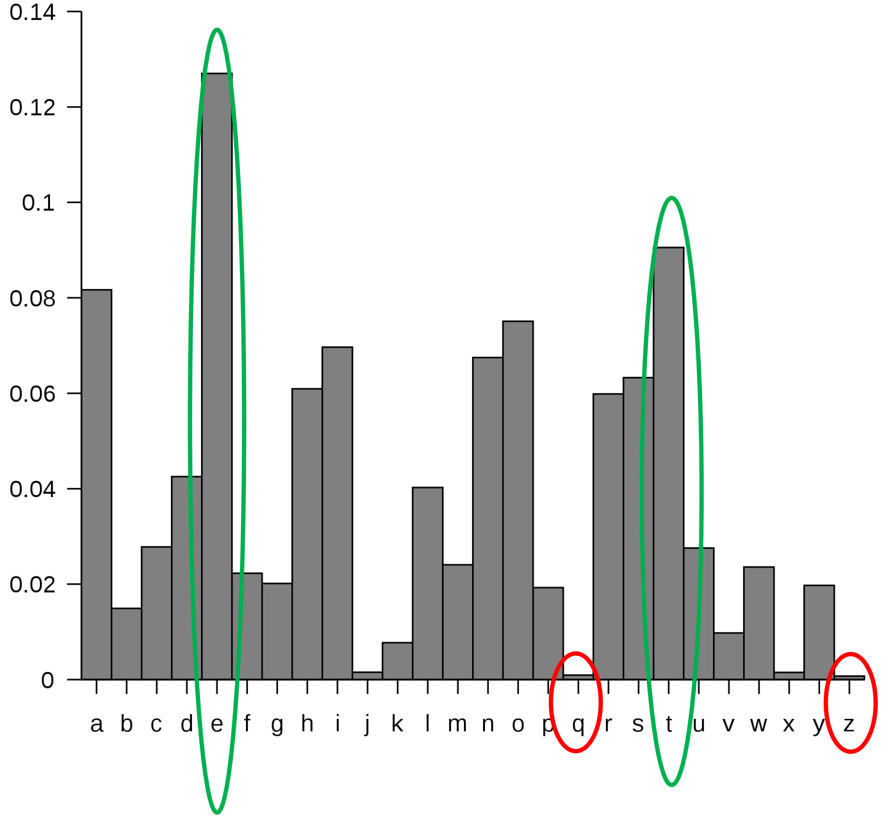
English Letter Frequency



English Letter Frequency



English Letter Frequency



Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATER

Ciphertext: CFFUCFSDUFY

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATER

Ciphertext: CFFUCFSDUFY

Monoalphabetic Cipher Example

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: MEETMELATERAT…

Ciphertext: CFFUCFSDUFYDU…

Plaintext’s Natural Redundancy

The frequency bias can also occurs
in sequence of multiple alphabets

E.g., “TH” and “QU” in English

Uniform Distribution for Alphabets

No frequency biases, or uniform distribution for alphabets, maximizes the information entropy in alphabets

In uniform distribution, all alphabets are equally likely and have equal frequency

Polyalphabetic Cipher

Use multiple monoalphabetic cipher substitutions

Use a key to define encryption mappings per alphabet

Vigenere Cipher: Simple Polyalphabetic Cipher

Multiple Caesar Ciphers in parallel

Key: LEMON

Plaintext:	MEET ME LATER
(Shift by:)	LEMO NL EMONL
Ciphertext:	XIQH ZP PMHRC

Vigenere Cipher: Simple Polyalphabetic Cipher

Encryption: $C_i = (p_i + k_{i \bmod m}) \bmod 26$

Key: LEMON m=5

Plaintext: MEET ME LATER
(Shift by:) LEMO NL EMONL
Ciphertext: XIQH ZP PMHRC

Vigenere Cipher: Simple Polyalphabetic Cipher

Decryption: $p_i = (C_i - k_{i \bmod m}) \bmod 26$

Key: LEMON m=5

Ciphertext: XIQH ZP PMHRC
(Left-Shift by:) LEMO NL EMONL
Plaintext: MEET ME LATER

Vigenere Cipher: Simple Polyalphabetic Cipher

Encryption: $C_i = (p_i + k_{i \bmod m}) \bmod 26$

Key: LEMON m=5 # Keys = n^m

Plaintext: MEET ME LATER

(Shift by:) LEMO NL EMONL

Ciphertext: XIQH ZP PMHRC

Vigenere Cipher: Simple Polyalphabetic Cipher

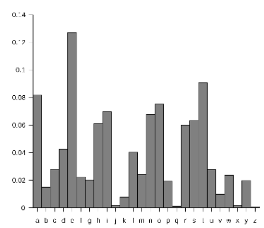
Encryption: $C_i = (p_i + k_{i \bmod m}) \bmod 26$

Key: LEMON m=5

Plaintext: MEET ME LATER

(Shift by:) LEMO NL EMONL

Ciphertext: XIQH ZP PMHRC



Vigenere Cipher: One-Time Pad

One-time pad if $m \geq$ (plaintext size)

Key: LEMONISSOUR

m=11

Plaintext: MEET ME LATER

(Shift by:) LEMO NI SSOUR

Ciphertext: XIQH ZM DSHYI

Vigenere Cipher: One-Time Pad

One-time pad if m ≥ (plaintext size)

Key: LEMONISSOUR …
m needs to be as long as plaintext

Plaintext:	MEET ME LATER …
(Shift by:)	LEMO NI SSOUR …
Ciphertext:	XIQH ZM DSHYI …