Math in Cybersecurity

John Marsh
SUNYIT Computer Science
Network and Computer Security

What is Cybersecurity?

Photo: Eugene Kaspersky, founder of computer-security company Kaspersky Labs, Moscow.
Credit: Vanity Fair, April 2011, article on StuxNet worm

A New World…

- Computers + Internet = A new world!
- The Internet: still in the "wild, wild west" phase
- We use computers and the Internet more and more every year…
  - At school
  - At work
  - At home

Computers and the Internet

- Today, the world runs on computers
  - Companies of all sizes rely on data centers
  - Local, state, and federal governments
  - Banking and financial industries
  - Individuals use email, social media, mobile devices

Computers and the Internet

- Mobile phones, mobile data plans
  - Only makes the problem more complicated!
  - Mobile applications include:
    - Voice
    - Email
    - Internet browsing
    - Social media
    - Location-based services
    - Audio/photo/video capture and upload
  - Mobile devices recently fueled actual revolutions!

Security and Privacy

- Data security
- Network security
- Computer security

} CYBER-SECURITY

→REQUIREMENT to safeguard personal information (privacy), business processes, and government operations

→NOBODY KNOWS how we are going to fulfill this requirement as threats and attacks grow more numerous and sophisticated

Cyber-Security in the Mohawk Valley

- Griffiss Technology Park
  - Air Force Research Labs (AFRL)
    - HEADQUARTERS of Information Directorate
  - Dozens of companies are located in Rome near AFRL
  - Thousands are employed in the computing and IT (Information Technology)
  - Cyber-security professionals are in high demand
- Local higher education programs
  - SUNYIT - BS Degree in NCS (Network and Computer Security)

sunyit

HERKIMER COUNTY COMMUNITY COLLEGE

UTICA COLLEGE

MVCC

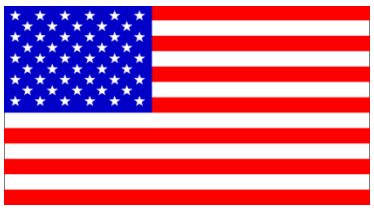
sunyit

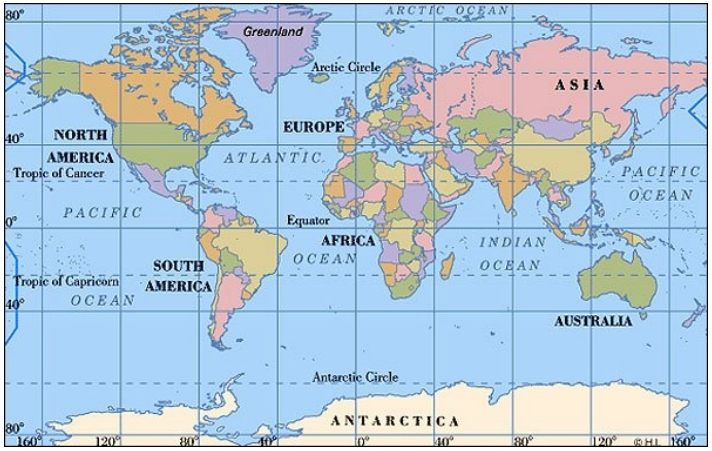
Cyber-Security in the Mohawk Valley

- Assured Information Security (AIS), Rome, NY
  - → Grown to 100 people
  - → New building going up right now

Math in Cyber-Security

- Math and science are the foundations of our modern technological world
  - 4 years of high school math
  - Strength in STEM (Science, Technology, Engineering, and Mathematics) is recognized as a critical ingredient in the competitiveness of the USA in the 21st century





Math in Cyber-Security

- An important example of math in cyber-security is in cryptography
- Cryptography is widely used on the internet to secure data against eavesdropping
  - Secure internet connections for online shopping
- **Plaintext**: unencrypted data
- **Cyphertext**: encrypted data
- **Key(s)**: Used to encrypt and decrypt data

Cryptography Example

- Caesar Cipher: Replace each letter by a letter further up the alphabet
  - Key: "**C**"
    → means "shift by 2" or "replace A by C"
  - Plaintext: "**THIS IS A TEST**"
  - Cyphertext: "**VJKU KU C VGUV**"

A	B	C	D	E	F	G	H	I	J	K	L	M
C	D	E	F	G	H	I	J	K	L	M	N	O

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Cryptography Example

- Vigenere Cipher
  - Key is not just one letter, but a whole word

    → each letter of the word means a different shift
  - Example:
    - Key: **MY KEY**
    - Plaintext: "**THIS IS A TEST**"
    - Cyphertext: "**FFSW GE Y DIQF**"

T	H	I	S	I	S	A	T	E	S	T
M	Y	K	E	Y	M	Y	K	E	Y	M
F	F	S	W	G	E	Y	D	I	Q	F

PLAINTEXT LETTER

KEY LETTER

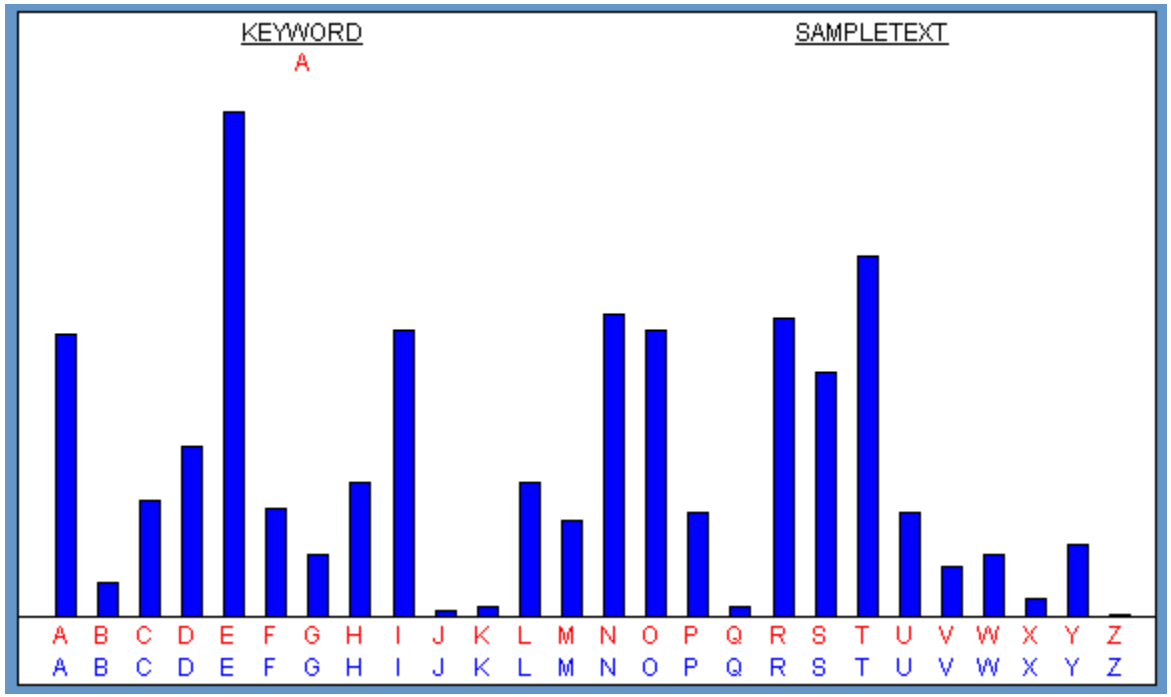
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

How To Break Caesar and Vigenere Cyphers

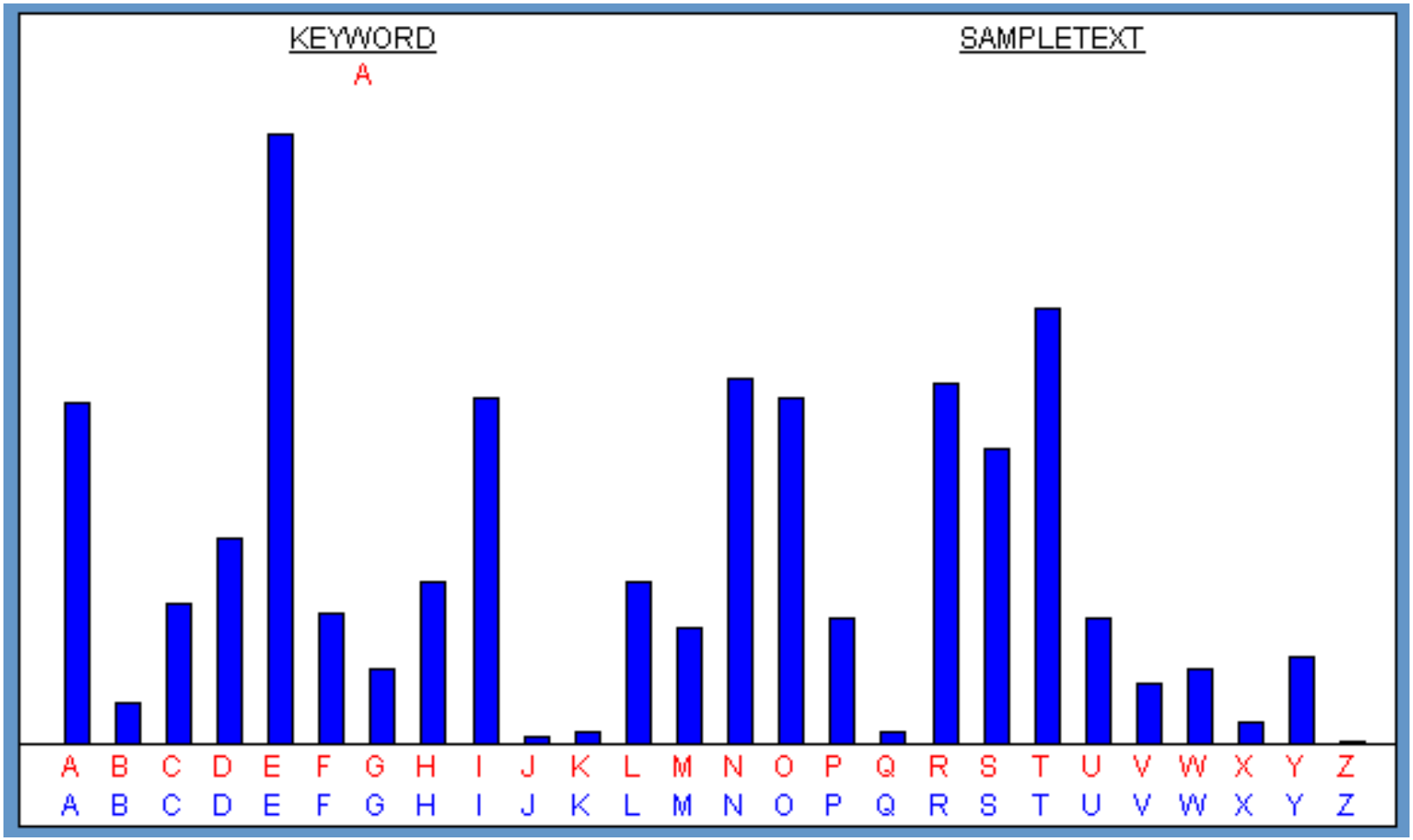
- Use the fact that some letters appear more often than others

  →A **histogram** tells this story!

- Figure out which letter is which by how often they appear!



English Language Text



Online Applets

- Histograms
  - http://math.ucsd.edu/~garsia/183/applets/CanonicalRoulette/index.html
- Caesar and Vigenere Ciphers
  - http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html