The University of Kansas

Computing

Aidan Schmelzle– BSCS and MSCS Student

ENGR Summer Camp 2025

TODAY'S AGENDA

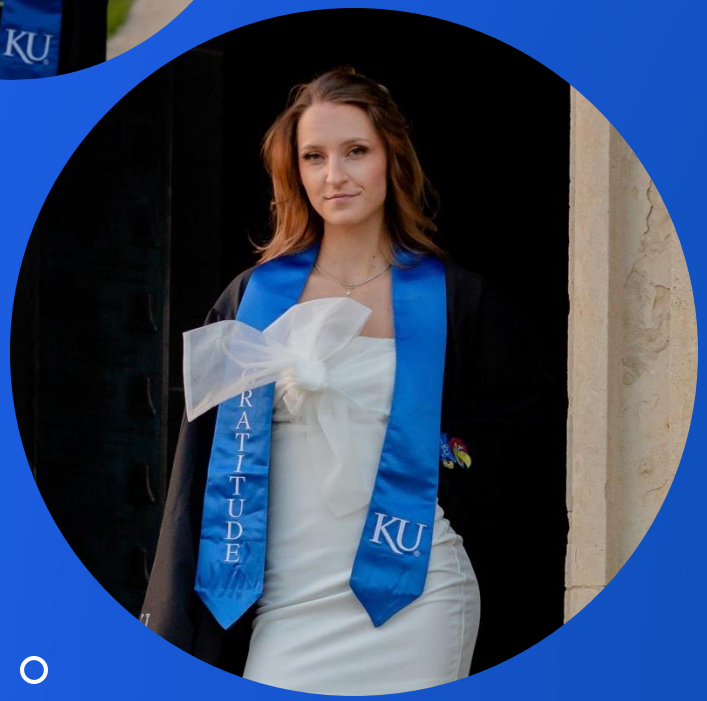
First 50 minutes:

- Computing Disciplines
- Intro to Cryptography

(10 minute break)

Second Hour:

- Ciphers
- Cryptography Worksheet



EECS 210 LAB

The UNIVERSITY *of* KANSAS

ABOUT ME

AIDAN SCHMELZLE (SHE/HER/HERS)

Graduated from KU with my B.S. in CompSci in May ’23

I also studied illustration and animation through the design department during my time in undergrad

I am currently pursuing my Master’s Degree (MSCS)

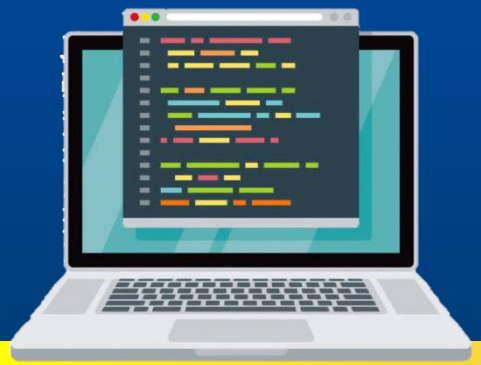
Research: Genetic Algorithms

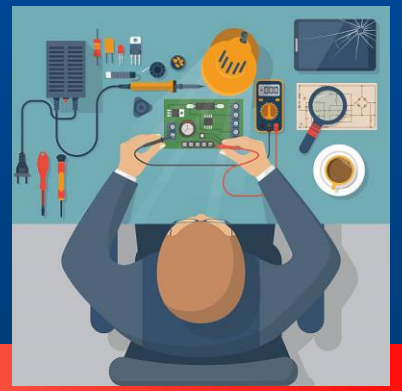
Advisor: Dr. Agah

TELL ME ABOUT YOU!

Your name, if you are a junior or senior,
and if you are considering computing.

Which Computing Discipline is Right for You?





Computer Science

- **Applied Computing**
- **Cybersecurity Engineering**

Computer Engineering

Electrical Engineering

The UNIVERSITY of KANSAS

What Can I Do As A:

Computer Scientist

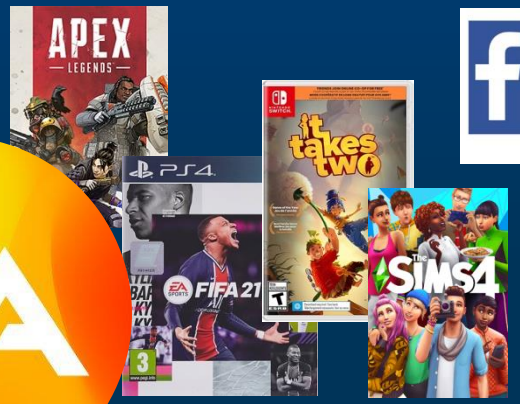
- Software Developer
- Web Developer
- Cybersecurity Professional
- Video Game Developer

Computer Engineer

- Software Developer
- Systems Engineer
- Computer Systems Analyst
- Hardware Designer

Electrical Engineer

- Electrical Design Engineer (CAD)
- Electronics Engineer
- Field Engineer



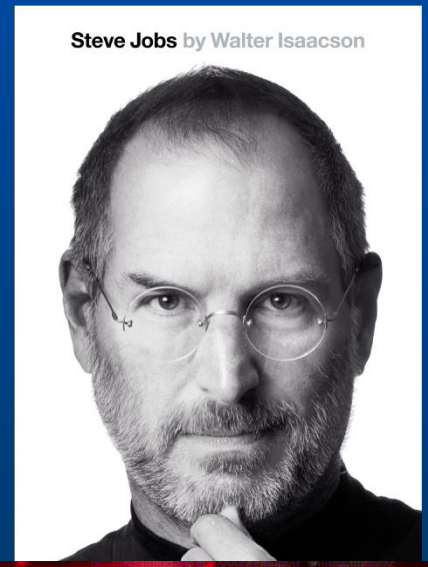
VERSITY of KANSAS

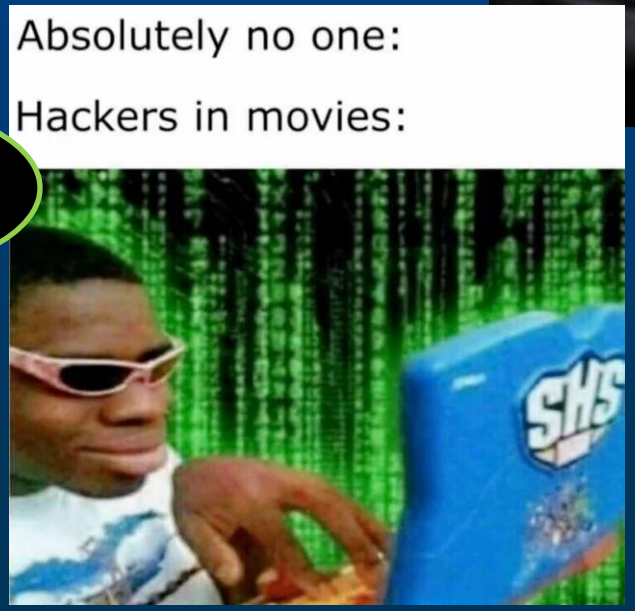
Degree Requirement Links

- Computer Science:
  - https://catalog.ku.edu/engineering/electrical-engineering-computer-science/bs-computer-science/#requirementstext
- Applied Computing:
  - https://catalog.ku.edu/engineering/electrical-engineering-computer-science/bs-applied-computing/#text
- Cybersecurity Engineering:
  - https://catalog.ku.edu/engineering/electrical-engineering-computer-science/bs-cybersecurity-engineering/
- Computer Engineering:
  - https://catalog.ku.edu/engineering/electrical-engineering-computer-science/bs-computer-engineering/
- Electrical Engineering:
  - https://catalog.ku.edu/engineering/electrical-engineering-computer-science/bs-electrical-engineering/

- Course Descriptions:
  - https://eecs.ku.edu/eecs-courses

What do you think of when you think of Computer Science?





What it Actually Is:

You

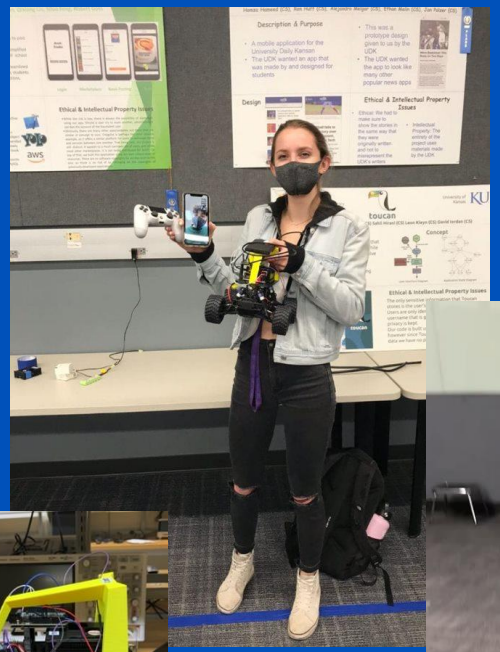
Eaton

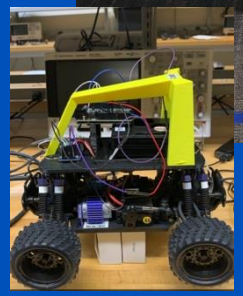
The UNIVERSITY of KANSAS

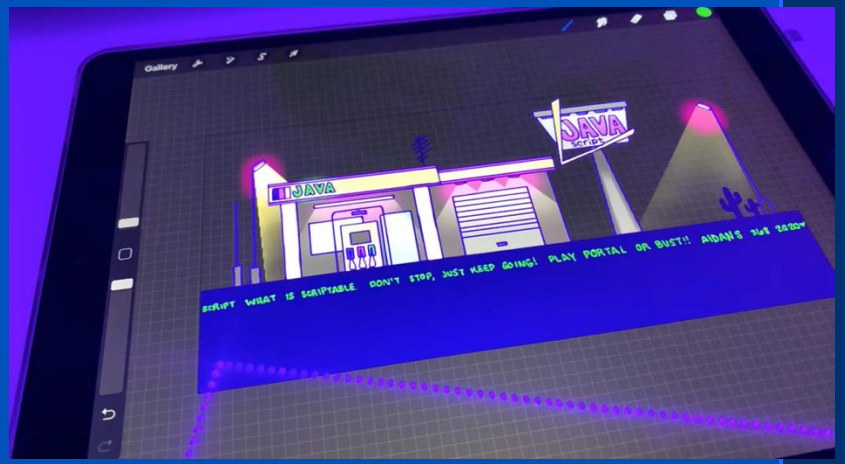
What You Will Actually Be Doing:

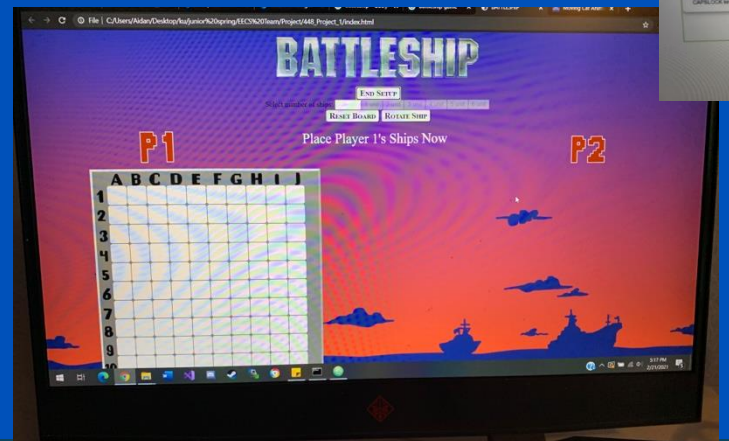
- Writing Code
  - Python, C, C++, SQL, etc, etc, etc.
- Data Structures
  - Learn best ways to store/ house data for specific use-cases
    - Do you need to be able to access data quickly?
    - Do you need to be able to store a huge amount of data long-term?
- Learning how computers interpret and execute the code we write
- Taking electives in focused areas:
  - Machine learning / artificial intelligence
  - Cybersecurity
  - Program verification

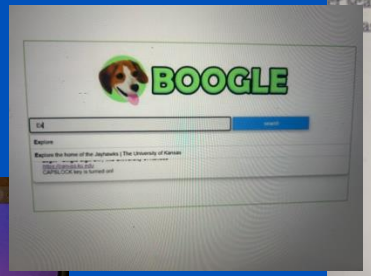
Cool Projects I Did in My Discipline!

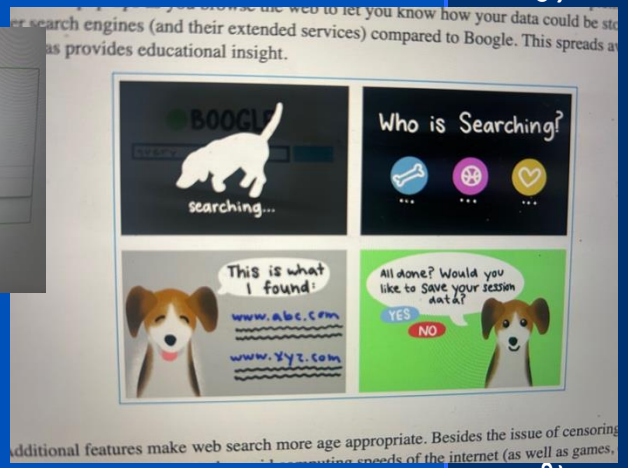












We do have:

NIANTIC

KU

Brian McClendon!

"that's our Lebron"

The University of Kansas

Ciphers & Encryption

Aidan Schmelzle– BSCS and MSCS Student
ENGR Summer Camp 2025

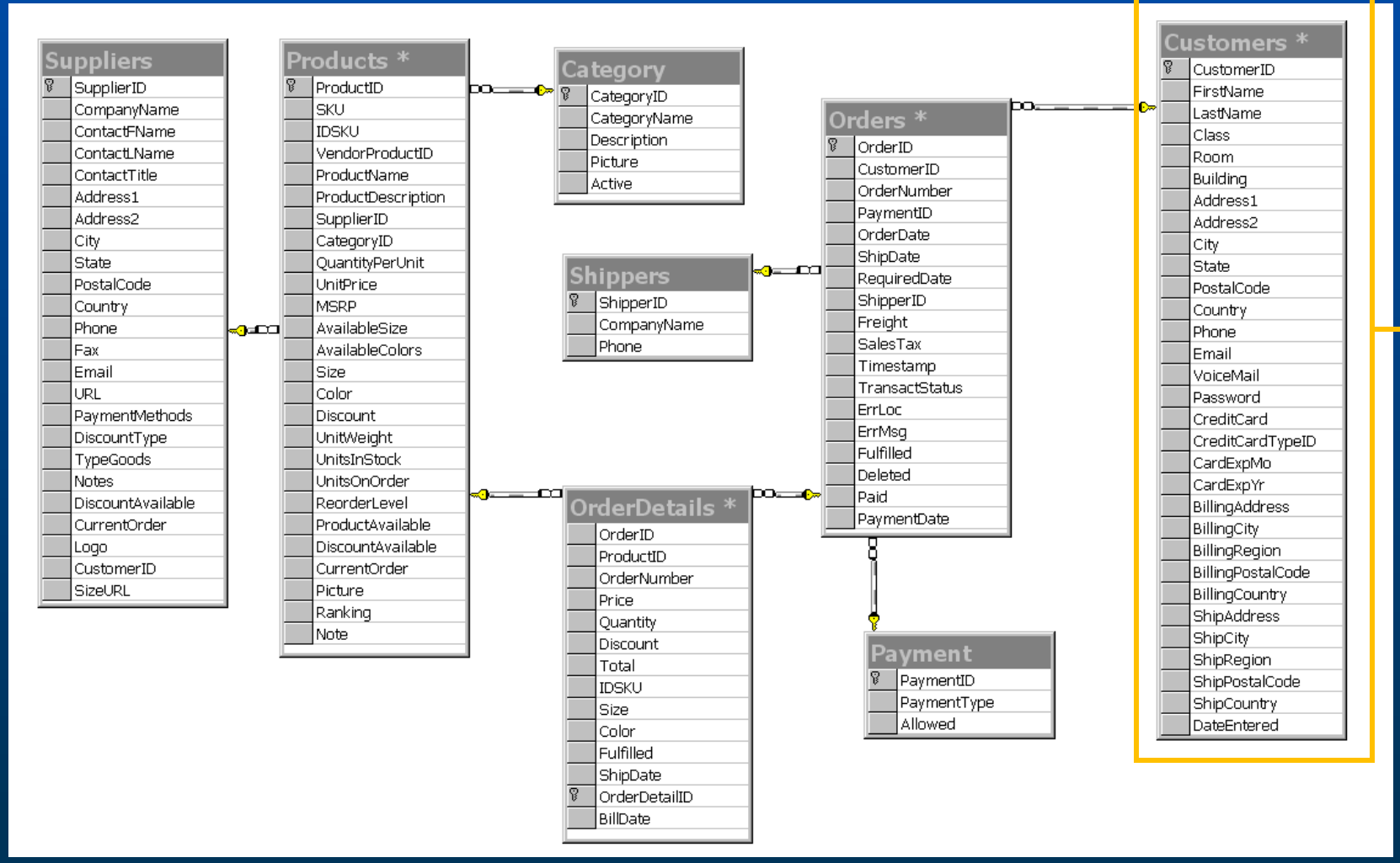
What is Encryption?

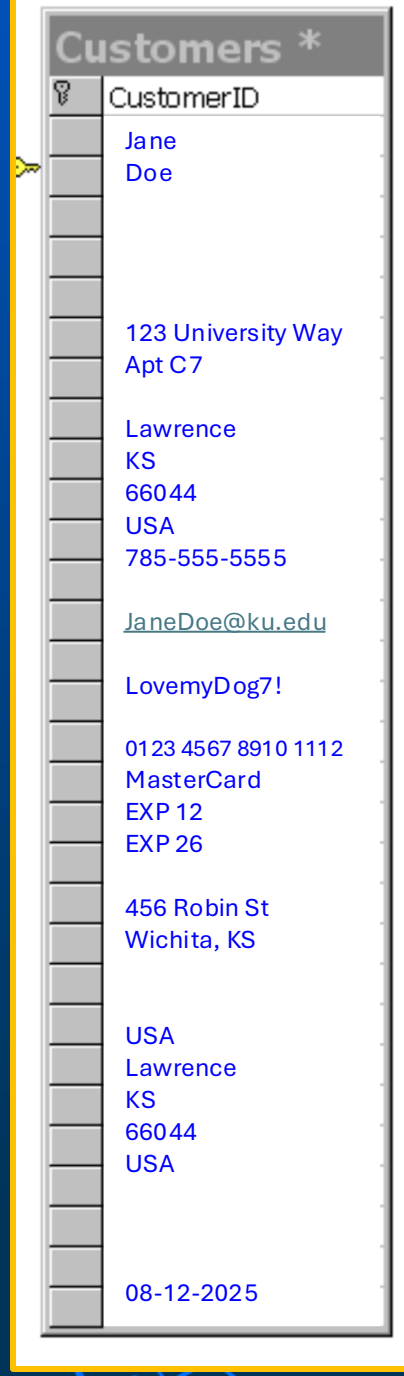
- Encryption is the process of converting information or data into a code, especially to prevent unauthorized access.

Why do we *Need* Encryption?

- We need to protect data in all forms
  - At rest
    - In this case, even if physical devices are stolen or accessed by unauthorized persons, the data is unreadable
  - In transit
    - The interception and potential alteration of data in transit is called a “Man in the Middle” attack
  - In use
    - Data needs to be protected while it is being accessed from your computer memory
      - Complex as this type of encryption requires methodologies that allows you to perform operations on your data without fully decrypting it

DB Schema:





The UNIVERSITY of KANSAS

Stored Data Should Instead Look Something Like This:

Results | Messages

	Customer_id	Customer_Name	Credit_card_number_encrypt
1	25665	mssqltips4	0x00433D8201CD98408F1283AEA54FDC21010000008F2462D...
2	74112	MSSQLTips2	0x00433D8201CD98408F1283AEA54FDC2101000000C3DBB29...
3	74113	MSSQLTips3	0x00433D8201CD98408F1283AEA54FDC2101000000FDC93D...
4	74114	MSSQLTips4	0x00433D8201CD98408F1283AEA54FDC2101000000E0C1891...
5	74115	MSSQLTips5	0x00433D8201CD98408F1283AEA54FDC2101000000DDCA5B...

TERMINOLOGY RELATED TO HACKING

White Hat Hacker

- Ethical security hacker
- Receives consent from system owner
- Follows rules and discloses flaws in order to expose and patch security vulnerabilities

Grey Hat Hacker

- Operates in “grey area”
- May not receive consent or adhere to legal guidelines before launching system attack
- May or may not disclose vulnerabilities
- May disclose vulnerabilities in exchange for compensation or other personal gain

Black Hat Hacker

- Malicious attacker
- Attempts to steal data or use data for illegal purposes

Ciphers

- Cryptography Basics
- Shift / Caesar Cipher
- Substitution Cipher
- Vigenère Cipher

- We will work through practice problems for each cipher together, and if there is time left, there are additional problems to solve.

CRYPTOGRAPHY BASICS

The UNIVERSITY of KANSAS

TERMINOLOGY

- Plaintext: readable text in its original, unencrypted form
- Ciphertext: encrypted text which is unreadable to anyone without the decryption key
- Keyspace: the set of all possible, distinct keys of a cryptosystem

** The word “cryptography” originates from the Greek words “kryptos” (κρυπτός) meaning “hidden” or “secret” and “Graphein” (γράφειν) meaning “writing.” Cryptography means “secret writing.”

ADVANCED TERMINOLOGY

- Symmetric-Key Encryption: a cryptographic method where the same key is used for both encrypting and decrypting the data

- Asymmetric-Key Encryption: a cryptographic method of where encryption and decryption use different keys which are mathematically related

Modulo

"the remainder when dividing"

%

We will use "mod" in our ciphers.

Practice with Modulo

Examples:

3 % 2 = 1
3 = (2 x 1) + 1

54 % 26 = 2
54 = (26 x 2) +2

1 % 5 = 1

Practice:

1. 36 % 5 = ____
2. 2 % 3 = ____
3. 110 % 10 = ____
4. 31 % 9 = ____

Please notice that modulo will only come into play when the dividend is larger than the divisor. Otherwise, the modulo is just the dividend.

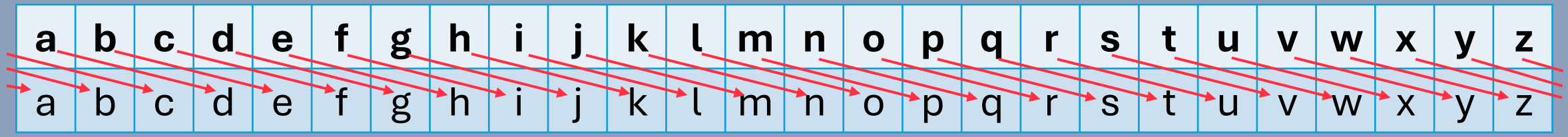
SHIFT CIPHER

SHIFT CIPHER

- In cryptography, the shift cipher is one of the simplest and most commonly-known encryption methods.
- Shift ciphers are performed by “shifting” all letters of plaintext “X” positions in the alphabet.

** Shift ciphers are also known as Caesar ciphers because General Julius Caesar utilized them when sending messages to his military to prevent military plans of action from being understood by adversaries in case of interception.

The Shift Cipher



plaintext: meet in engineering

key: shift: +3

ciphertext: phhw lq hqjlqhhulqj

The Math Behind The Shift Cipher

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$E_K(m) = (m + K) \% 26$

- K = amount of shift
- m = number of the plaintext letter
- c = number of the ciphertext letter

$D_K(c) = (c - K) \% 26$

Why is writing a formula for the cipher useful?

So we can automate the process!

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Let's practice!

Encrypt the word "FOX" with the shift cipher $E_K(m) = (m + K) \% 26$, where K = 4

F:	E_(_) = (_ + _) % 26	$E_4(5) = (5 + 4) \% 26$	$E_4(5) = 9 \% 26$	$E_4(5) = 9$	= J
O:	E_(_) = (_ + _) % 26	$E_4(14) = (14 + 4) \% 26$	$E_4(14) = 18 \% 26$	$E_4(14) = 18$	= S
X:	E_(_) = (_ + _) % 26	$E_4(23) = (23 + 4) \% 26$	$E_4(23) = 27 \% 26$	$E_4(23) = 1$	= B

DEMO

Colab Link

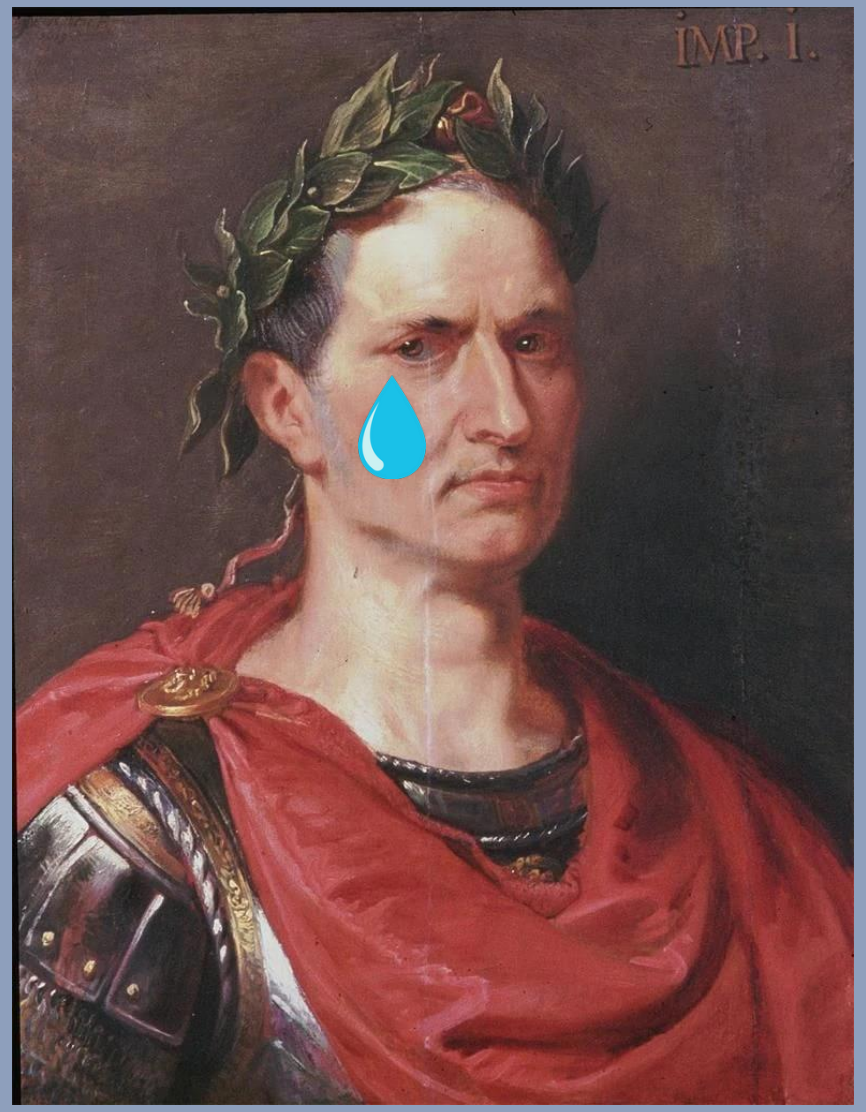
```
[8]  # Caesar Cipher

     def caesar_cipher(text, shift): # takes text and the amou
         result = "" # initialize a string to store the result
         for char in text: # for each character in the text st
             if char.isalpha(): # check to see if character is
                 start = ord('a') if char.islower() else ord('
                 shifted_char = chr((ord(char) - start + shift


                 result += shifted_char # add the new characte
             else:
                 result += char # if the character is not alpha
                 # examples: (space)! # % & ?
         return result
```

```
# Test the cipher

original_text = input("Enter the text to encrypt: ") # ge
shift_amount = int(input("Enter the shift amount: ")) # a
encrypted_text = caesar_cipher(original_text, shift_amoun
print("\noriginal text: ", original_text, "\n") # print o
print("encrypted text: ", encrypted_text, "\n") # print t
decrypted_text = caesar_cipher(encrypted_text, -shift_amo
print("decrypted text: ", decrypted_text) # print the dec
```

```
Enter the text to encrypt: Hello World!
Enter the shift amount: 3

original text:  Hello World!

encrypted text:  Khoor Zruog!

decrypted text:  Hello World!
```

Why isn't the Caesar Cipher Secure?

- The keyspace is very small (only 26)
  - additionally, one of the keys is 0 which means the message would still be in plaintext
- A computer can break a Caesar cipher in milliseconds without knowing the key!



* Cracking a code by trying all possible combinations is called brute force.

DEMO PT II

Colab Link

```
[8]  # Caesar Cipher

     def caesar_cipher(text, shift): # takes text and the amou
         result = "" # initialize a string to store the result
         for char in text: # for each character in the text st
             if char.isalpha(): # check to see if character is
                 start = ord('a') if char.islower() else ord('
                 shifted_char = chr((ord(char) - start + shift


                 result += shifted_char # add the new characte
             else:
                 result += char # if the character is not alpha
                 # examples: (space)! # % & ?
         return result
```

```
# Test the cipher

original_text = input("Enter the text to encrypt: ") # ge
shift_amount = int(input("Enter the shift amount: ")) # a
encrypted_text = caesar_cipher(original_text, shift_amoun
print("\noriginal text: ", original_text, "\n") # print o
print("encrypted text: ", encrypted_text, "\n") # print t
decrypted_text = caesar_cipher(encrypted_text, -shift_amo
print("decrypted text: ", decrypted_text) # print the dec
```

```
Enter the text to encrypt: Hello World!
Enter the shift amount: 3

original text:  Hello World!

encrypted text:  Khoor Zruog!

decrypted text:  Hello World!
```

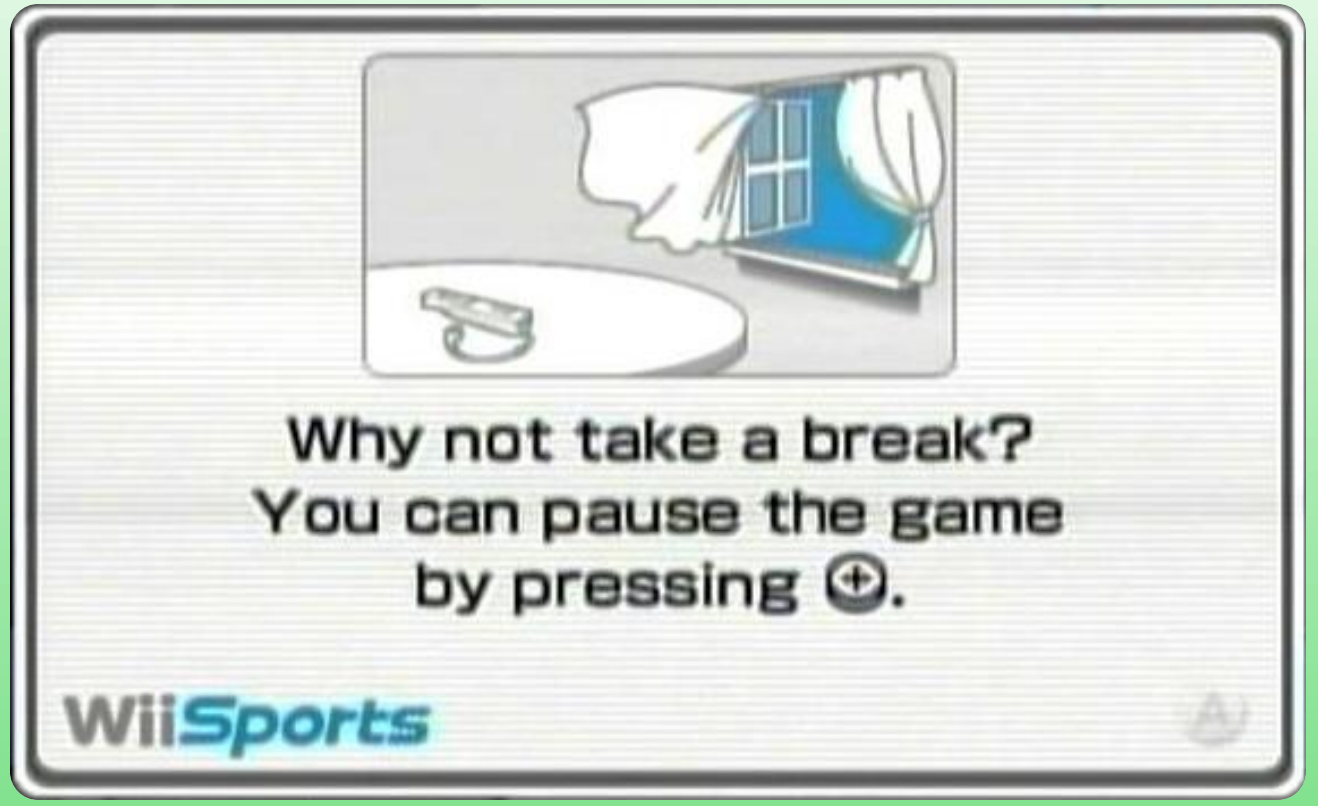
!!

You!

A messenger brings you a scroll with the text

“ZKDW LV IRU OXQFK?”

and whispers, “I bring an urgent message! The key is 3” before running away. What has General Caesar written to you?



BREAK TIME!

Take 10 minutes and we will continue with cryptography.

SUBSTITUTION CIPHER

Substitution Cipher

- Substitute one character for another
  - **Monoalphabetic cipher**: each letter of the plaintext is replaced with another letter of the alphabet.
    - It uses a **fixed key** which consist of the 26 letters of a “shuffled alphabet”

plaintext:	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
key:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

plaintext: FISH **ciphertext: XSIA**

Substitution Cipher

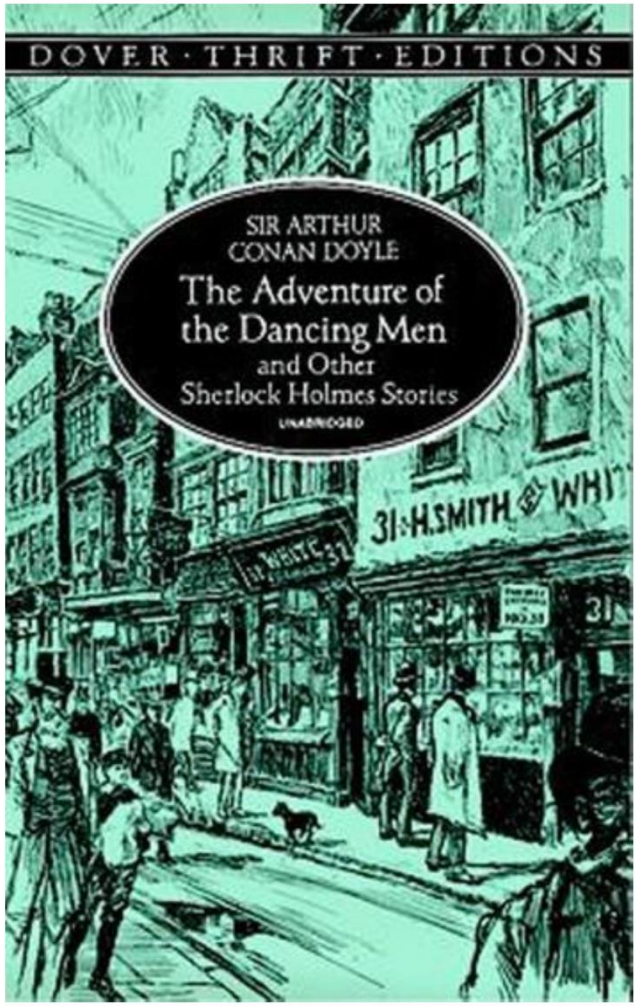
- Keyspace: 26! $\approx 4 * 10^6$ possible substitution alphabets
- Can we brute force the cipher?
  - 10^9 tests/second
  - $\approx 4 * 10^{13}$ second
  - $\approx 3 * 10^7$ YEARS to brute force the cipher

Did We Fix the Problem?

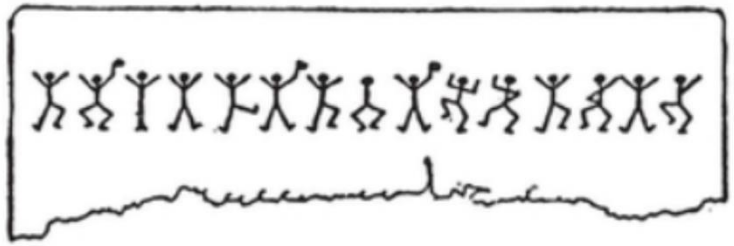
First, let's talk about …

- Frequency Analysis: method to correlate language-specific patterns/ distributions between plaintext and ciphertext.

Frequency Analysis

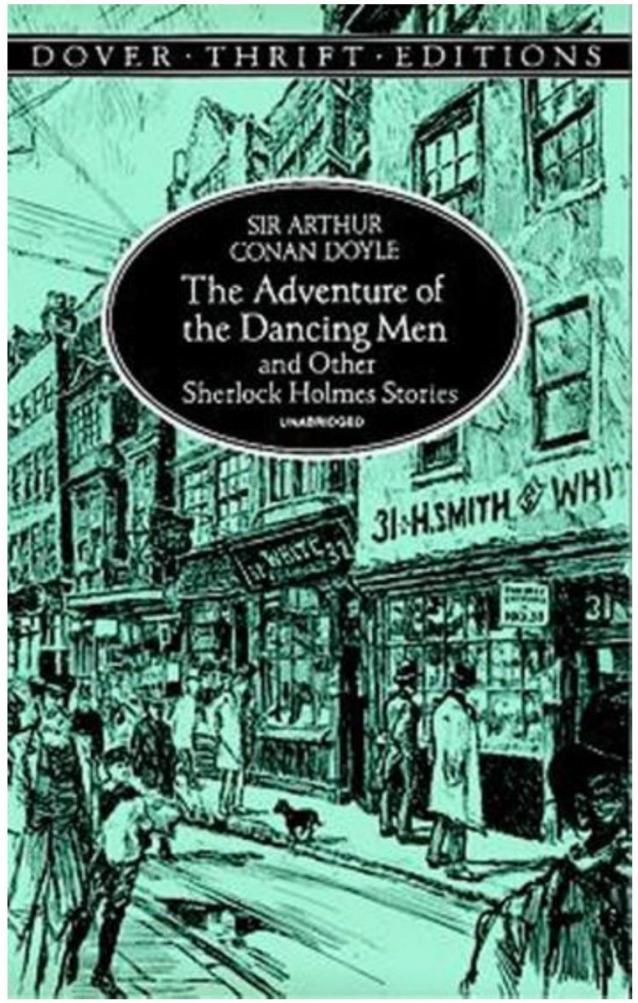


Holmes held up the paper so that the sunlight shone full upon it. It was a page torn from a notebook. The markings were done in pencil, and ran in this way:



Holmes examined it for some time, and then, folding it carefully up, he placed it in his pocketbook.

Frequency Analysis



"Having once recognized, however, that the symbols stood for letters, and having applied the rules which guide us in all forms of secret writings, the solution was easy enough. The first message submitted to me was so short that it was impossible for me to do more than to say, with some confidence, that the symbol  stood for E. As you are aware, E is the most common letter in the English alphabet, and it predominates to so marked an extent that even in a short sentence one would expect to find it most often. Out of fifteen symbols in the first message, four were the same, so it was reasonable to set this down as E. It is true that in some cases the figure was bearing a flag, and in some cases not, but it was probable, from the way in which the flags were distributed, that they were used to break the sentence up into words. I accepted this as a hypothesis, and noted that E was represented by 

Frequency Analysis

```
Vg gbbx n ybg bs oybbq,
fjrng naq grnef gb trg
gb jurer jr ner gbqnl,
ohg jr unir whfg ortha.
Gbqnl jr ortva va
rnearfg gur jbex bs
znxvat fher gung gur
jbeyq jr yrnir bhe
puvyqera vf whfg n
yvggyr ovg orggre guna
gur bar jr vaunovg
gbqnl.
```

ciphertext:

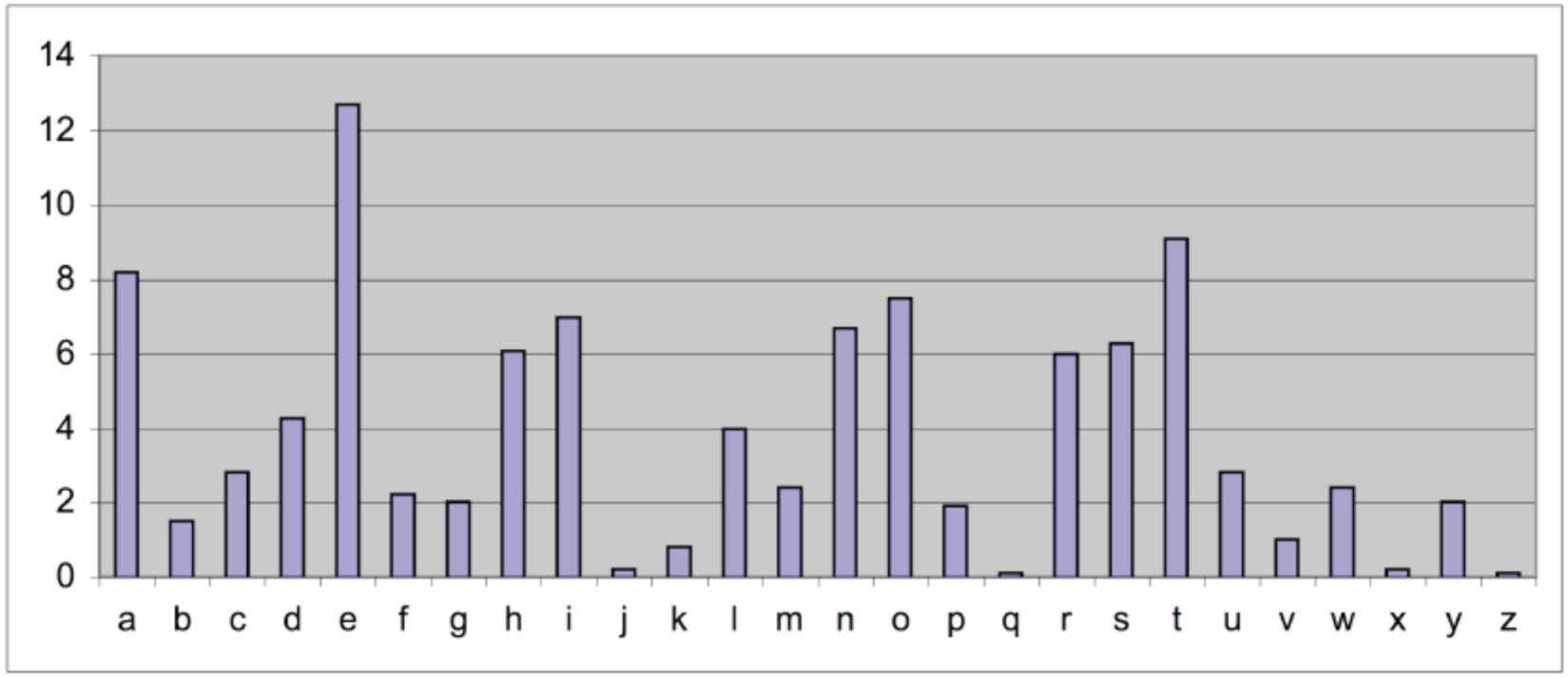
```
It took a lot of blood,
sweat and tears to get
to where we are today,
but we have just begun.
Today we begin in
earnest the work of
making sure that the
world we leave our
children is just a
little bit better than
the one we inhabit
today.
```

plaintext:

Frequency Analysis

* How can we even build further off of this knowledge?

In English:



Common English Bigrams and Trigrams:

Bigrams

th 1.52%	en 0.55%	ng 0.18%
he 1.28%	ed 0.53%	of 0.16%
in 0.94%	to 0.52%	al 0.09%
er 0.94%	it 0.50%	de 0.09%
an 0.82%	ou 0.50%	se 0.08%
re 0.68%	ea 0.47%	le 0.08%
nd 0.63%	hi 0.46%	sa 0.06%
at 0.59%	is 0.46%	si 0.05%
on 0.57%	or 0.43%	ar 0.04%
nt 0.56%	ti 0.34%	ve 0.04%
ha 0.56%	as 0.33%	ra 0.04%
es 0.56%	te 0.27%	ld 0.02%
st 0.55%	et 0.19%	ur 0.02%

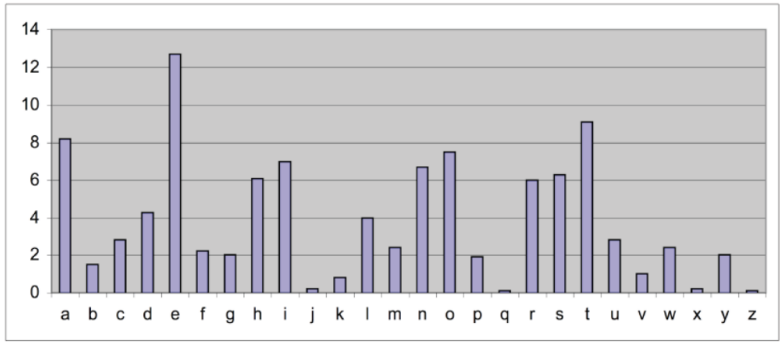
Trigrams

1. the	6. ion	11. nce
2. and	7. tio	12. edt
3. tha	8. for	13. tis
4. ent	9. nde	14. oft
5. ing	10.has	15. sth

- Example:

GS SGU WL LS KZAVU YJAY JU WL GSY XWLYNZKUX KR LSPUYJWGO NGUQHUMYUX

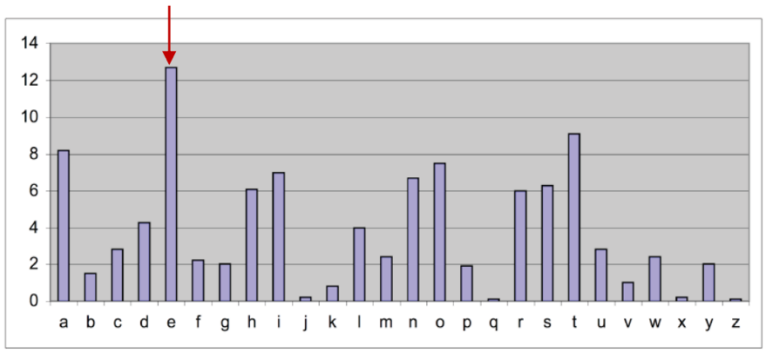
- Count the frequency
  - U: 8; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2



- Example:

GS SGE WL LS KZAVE YJAY JE WL GSY XWLYNZKEX KR LSPEYJWGO NGEQHEMYEX

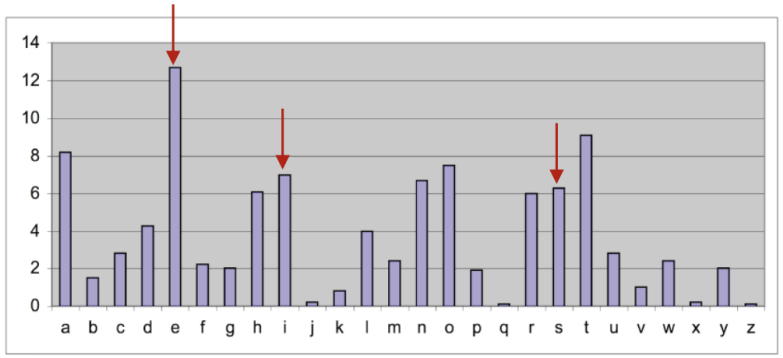
- Frequency analysis
  - U: 8 → E; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2



- Example:

GS SGE WL LS KZAVE YJAY JE WL GSY XWLYNZKEX KR LSPEYJWGO NGEQHEMYEX

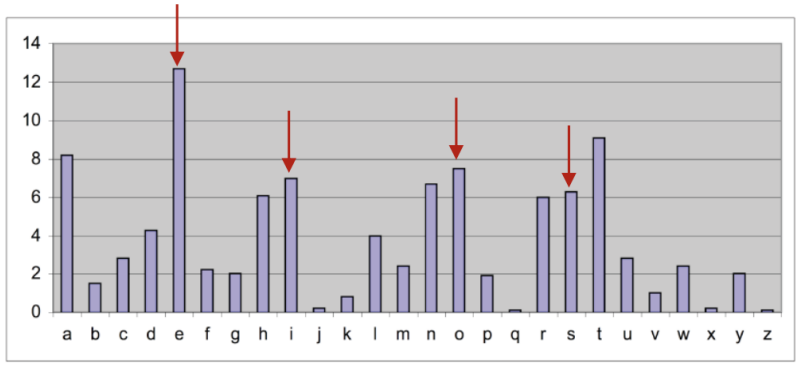
- Frequency analysis
  - U: 8 → E; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2
  - frequent two-letter words?
    - WL → IS



- Example:

GS SGE IS SS KZAVE YJAY JE IS GSY XISYNZKEX KR SSPEYJIGO NGEQHEMYEX

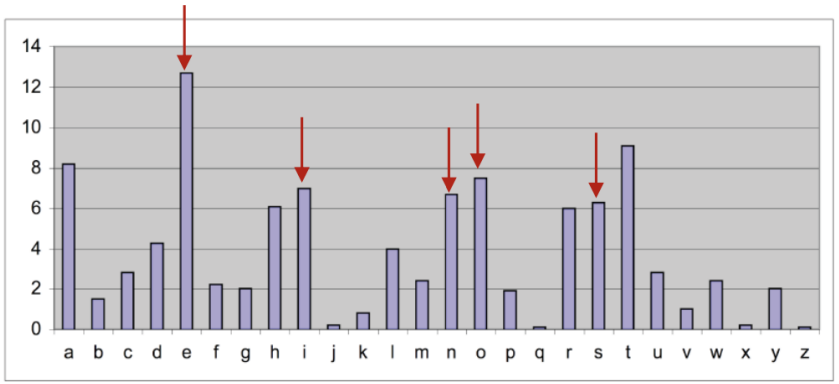
- Frequency analysis
  - U: 8 → E; Y: 6; G: 5; S: 5; L: 5 → S; W: 4 → I; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2
  - frequent two-letter word?
    - WL → IS
    - SS → SO



- Example:

GO OGE IS SO KZAVE YJAY JE IS GOY XISYNZKEX KR SOPEYJIGO NGEQHEMYEX

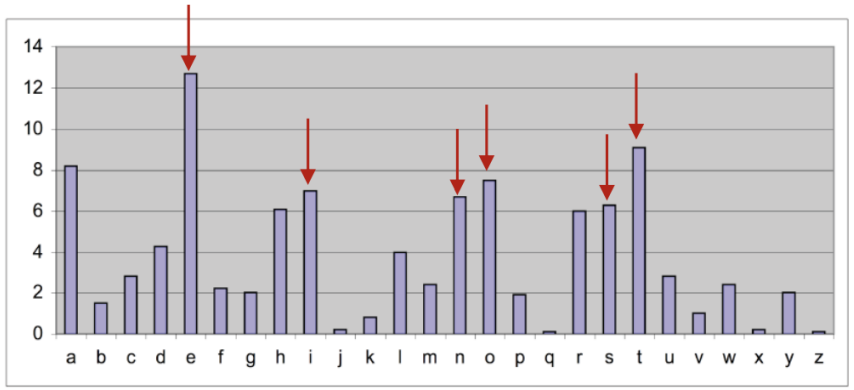
- Frequency analysis
  - U: 8 → E; Y: 6; G: 5; S: 5→O; L: 5 → S; W: 4 → I; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2
  - what is G?
    - GO→NO
    - OGE→ONE



- Example:

NO ONE IS SO KZAVE YJAY JE IS NOY XISYNZKEX KR SOPEYJINO NNEQHEMYEX

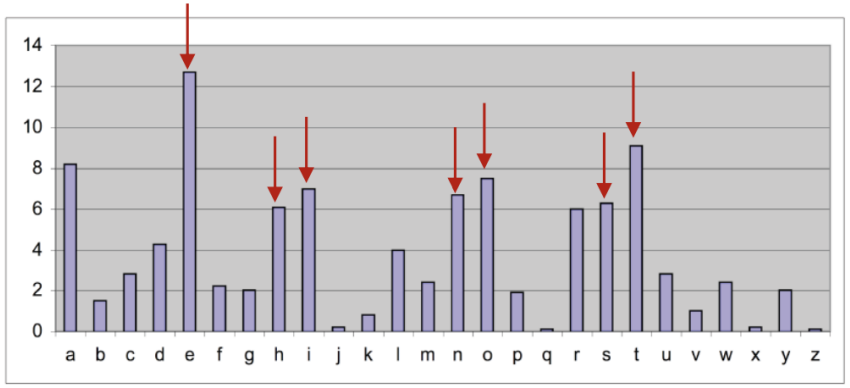
- Frequency analysis
  - U: 8 → E; Y: 6; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2
  - what is Y?
    - NOY→NOT



- Example:

NO ONE IS SO KZAVE TJAT JE IS NOT XISTNZKEX KR SOPETJINO NNEQHEMTEX

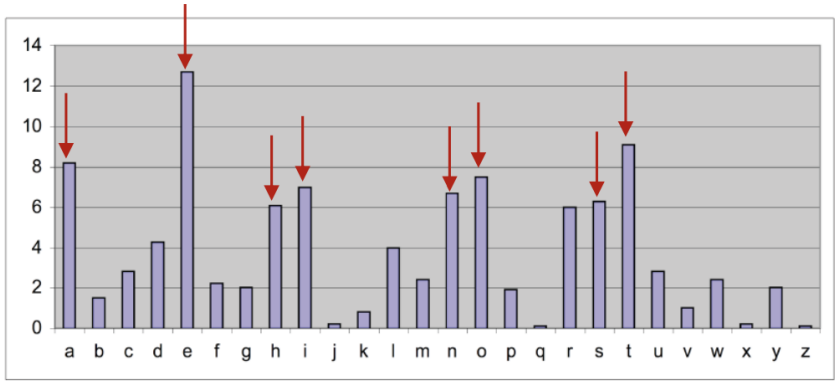
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3; K: 3; X: 3; A: 2; N: 2; Z:2
  - what is J?
    - JE→HE



- Example:

NO ONE IS SO KZAVE THAT HE IS NOT XISTNZKEX KR SOPETHINO NNEQHEMTEX

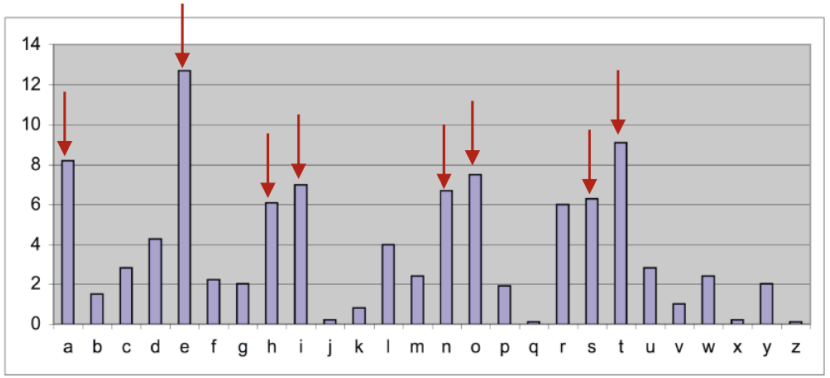
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3; X: 3; A: 2; N: 2; Z:2
  - what is A?
    - THAT→THAT



- Example:

NO ONE IS SO KZAVE THAT HE IS NOT XISTNZKEX KR SOPETHINO NNEQHEMTEX

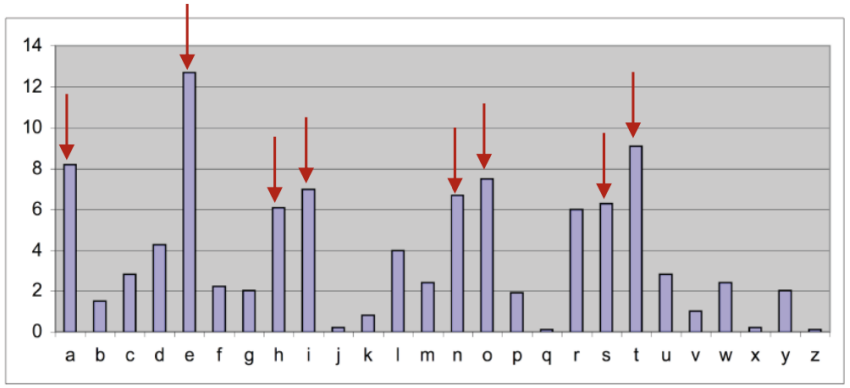
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3; X: 3; A: 2→ A; N: 2; Z:2
  - what is P and O?
    - SOPETHINO → SOMETHING



- Example:

NO ONE IS SO KZAVE THAT HE IS NOT XISTNZKEX KR SOMETHING NNEQHEMTEX

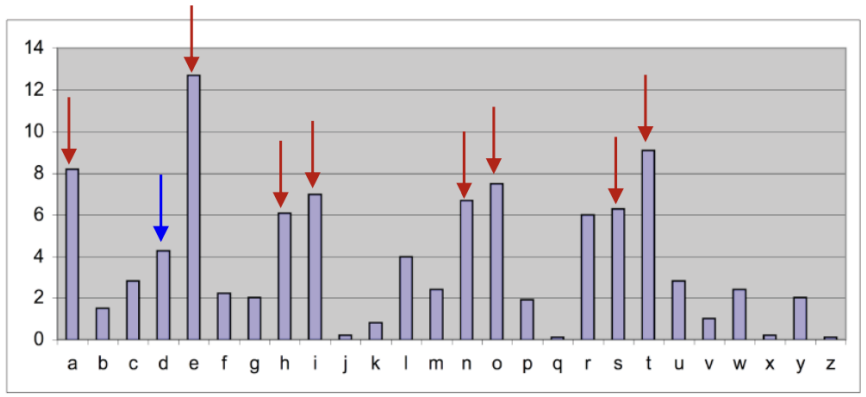
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3; X: 3; A: 2→ A; N: 2; Z:2
  - EX ?
    - ER or ED or ES



- Example:

NO ONE IS SO KZAVE THAT HE IS NOT DISTNZKED KR SOMETHING NNEQHEMTED

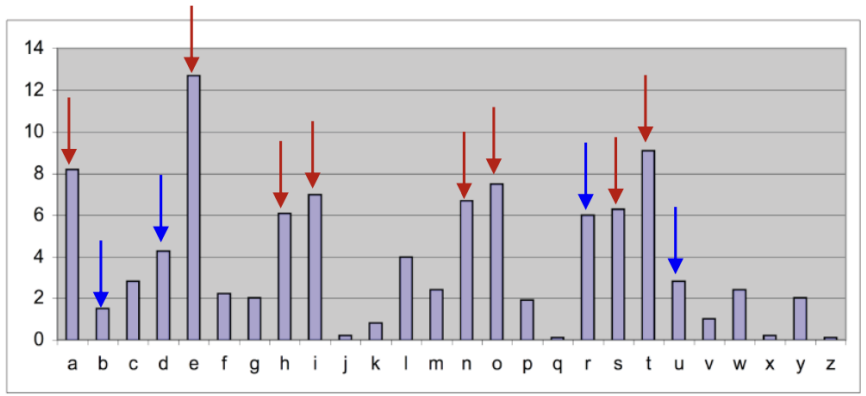
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3; X: 3; A: 2→ A; N: 2; Z:2
  - guess X → D



- Example:

NO ONE IS SO KZAVE THAT HE IS NOT DISTNZKED KR SOMETHING NNEQHEMTED

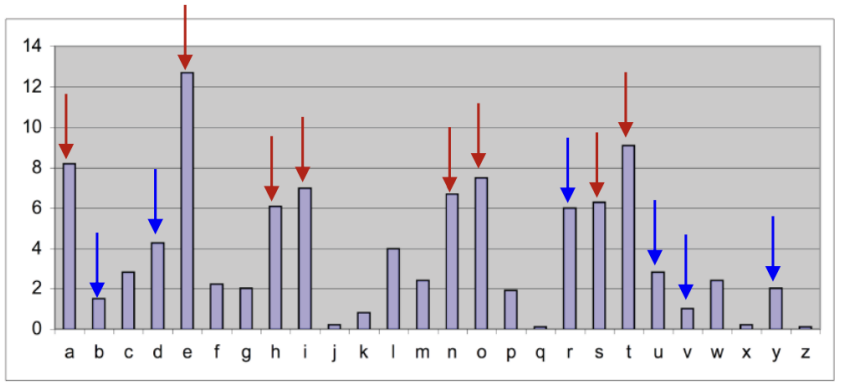
- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3; X: 3→ D; A: 2→ A; N: 2; Z:2
  - DISTNZKED → DISTURBED



- Example:

NO ONE IS SO BRAVE THAT HE IS NOT DISTURBED BR SOMETHING UNEQHEMTED

- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3→B; X: 3→ D; A: 2→ A; N: 2→U; Z:2→R
  - BRAVE → BRAVE
  - BR → BY
  - UNEQHEMTED → UNEXPECTED



- Example:

NO ONE IS SO BRAVE THAT HE IS NOT DISTURBED BY SOMETHING UNEXPECTED

- Frequency analysis
  - U: 8 → E; Y: 6→ T; G: 5→N; S: 5→O; L: 5 → S; W: 4 → I; J: 3 → H; K: 3→B; X: 3→ D; A: 2→ A; N: 2→U; Z:2→R

  - **What is your take-away from this cryptanalysis example?**

So! Did We Fix the Problem?

- No, we can still crack the substitution cipher using cryptanalysis.
  - the study of methods for obtaining the meaning of encrypted information without accessing the secret information
  - utilize the weakness of the design or implementation of a cryptographic algorithm
    - Our example here was frequency analysis

VIGENÈRE CIPHER

VIGENÈRE CIPHER

- The Vigenère Cipher is a shift cipher where each character of plaintext is encoded with a different Caesar cipher

- The cipher is named after Blaise de Vigenère (pictured above), though it was first described by Giovan Battista Bellaso in 1553 (pictured below).

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

plaintext

key

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B						

plaintext

key

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E					

plaintext →

key ↓

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E	A				

plaintext

key

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E	A	Y			

plaintext

key

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E	A	Y	E		

plaintext

key

	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

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E	A	Y	E	P	

plaintext

key

	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

The UNIVERSITY of KANSAS

plaintext:

J	A	Y	H	A	W	K

key:

S	E	C	R	E	T	S

ciphertext:

B	E	A	Y	E	P	C

plaintext

key

	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

Vigenère Cipher Security

- Strengths:
  - mitigates frequency analysis weakness
  - Keyspace: there are too many keys to crack the cipher with brute force manually
    - For a key length of k, there are 26^k possible keys
- We CAN break the Vigenère cipher
  - First find the key length
  - Test every possible key for each key length

Cybersecurity Classes of Interest:

- EECS 569: Digital Forensics
- EECS 666: Network Security
- EECS 683: Hardware Security
- EECS 700: Data Privacy & Security
- EECS 765: Intro to Cryptography & Computer Security
- EECS 785: IoT Security
- EECS 787: Mobile Security

EECS PRIVACY & SECURITY FACULTY

Dr. Fengjun Li

- IoT Security
- Social Network Privacy
- Network Security
- Secure Data Sharing & Publishing
- Adversarial ML

Dr. Bo Luo

- Information Security & Privacy
- Database Security
- Smart Grid System Privacy & Security

Dr. Drew Davidson

- Cybersecurity & Privacy
- Secure Design
- Mobile Security

Dr. Han Wang

- Data Privacy & Security

Dr. Tamzidul Hoque

- Hardware Security

What *IS* Research?

- Professors research current technologies to mitigate vulnerabilities, verify processes, and to make advances in the field.
  - Make new discoveries
  - Prove/ validate existing theories and methodologies
  - Explore the unknown within a field

Proceedings of the Second International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2018)
IEEE Xplore DVD Part Number:CFP18OZV-DVD; ISBN:978-1-5386-1441-9

A RECENT REVIEW ON IOT BASED TECHNIQUES AND APPLICATIONS

[1*] M.Nagakannan, [2]C.Johnson Inbaraj, [2]K.Mukesh Kannan,
[1*,2]Pg Scholar, School of Computing, Kalasalingam Academy of Research and Education, Tamilnadu, India
[1*]nagakannan16.nk@gmail.com

[1]S.Ramkumar,
[1]Assistant Professor, School of Computing, Kalasalingam Academy of Research and Education, Tamilnadu, India,
[1]ramkumar.drl2013@gmail.com

***Abstract*- We deals with a review on applications used in IOT in this paper since in today's era IOT is one of the fast growing field the concept IOT is mainly used for connecting various devices with internet by using IOT. For connecting and using IOT into devices we make applications. In this paper we are going to see what the applications that are used by IOT are. Since it is inessential to say that current advertising around the IOT is enormous. In this era everyday a company announces a new IOT based product under different field. The main mission in the paper is providing an outlook about IOT techniques and its Applications.**

Keywords: WHIZ, Smart, Agile, IOT.

I. INTRODUCTION

Kevin Ashton who first coined the concept IOT in the year 1999. He mainly made his research in objects by making a bridge of communication between objects in present world with internet.. However this concept was first used in twentieth century, computers were brain without sense. Later after introducing IOT into them the computers can sense things for themselves. One of good example for this is GPS system in cell phones. Yet the GPS was not tested till 2004 later it came into existence with help of satellite it was used. The main aim of IOT is to unify everything within the world below a standard infrastructure, however solely providing management over issues however additionally inform North American country the state of a thing. IOT brings us a large amount of technological changes in our life, were our life become simpler and more comfort by using this concept. As well we all know how our life has changed by the arrival of internet, like the same the IOT take us to a new era of living by acting as communicator for smart objects with us and by saying this "if communication on human to human is possible, then communication on object with object is also possible". Internet of things could be a new net application that results in associate degree era of sensible technology wherever there exists thing-thing communication instead of human-human communication.

Through IOT, every and each object during this world will be known, connected and take choices severally. It's taken its birth from mobile computing and omnipresent computing. Technologies adore RFID, wireless device networks associate degrade embedded systems play an important role in forming an IOT application. Internet of Things (IOT) is creating a new look, by making industrial systems powerful and applications by jump on the spouting in the sectors like wireless, mobile, RFID and devices. IOT is utilized as appliance for homes, agile handy devices, whiz city, agile grids, allied car, allied health, agile retail, whiz supply chain, agile farming. These are some top appliances used by IOT.

Though IOT is employed in several domains, its path to success isn't swish. There's incalculable utility of IOT appliance into all the terrain together with pharmaceutical, producing, factory-made, hauling, erudition, governance, hollowing, environment and so on. Although IOT has teeming edges, there square measures. IOT is built on the footing of the Internet, security problems of the Internet are overseen in IOT. And as IOT encompass three layers: viewpoint layer, transportation layer and utilization layer. In world to come Internet of Things can provide a generous vision and also license everyone to ingress and afford rich information about things and security problems involved in IOT.

Strategies used by IOT are explained in the fig.1 is always "Any" these are following ones

- Anything Any devices
- Anyone Anybody
- Any Service Any Business
- Any Path Any Network
- Any Place Any where
- Anytime Any Context

These are the things are possible by IOT, here any is the keyword. The word any is said to be powerful mantra of IOT.

Computing in Health

- Imaging
  - ex. Dr. Shomaji – Carotid Artery Research with Computer Vision
- Data Privacy & Security
  - Health record storage and maintenance
  - Protect PII (Personally-Identifying Information)
- Advance telemedicine software
- Data Science
  - Analyze health statistics to extract insights

OPPORTUNITIES KU HAS FOR YOU

KU Career Services
HireJayhawks

Rock Chalk Job Hawk

>hack_ KU

KU

KU WOMEN IN COMPUTING

GRACE HOPPER CELEBRATION
ANITA B.ORG

My Big Sister Advice to You:

- Before arriving:
  - Take a programming class (many available online)
  - Get an Arduino starter kit
  - Take MATH! Take Calculus.
- Upon degree start:
  - GET A WINDOWS / LINUX COMPUTER – sorry my Mac friends ☹
  - GO TO CLASS EVEN IF YOUR FRIENDS DO NOT
  - Live in the dorms if you can afford to
  - Live with people who are pursuing a degree of equal difficulty or people who you KNOW have a strong work ethic
  - DO. YOUR. HOMEWORK. YOURSELF.
  - Do as much hands-on work as you can
    - Make your own passion projects
  - Attend department events
    - HackKU, Career Fair, Clubs
  - Do an internship!! Utilize your summers to get ahead.
  - Attend Office Hours! Get to know your instructors.

The UNIVERSITY of KANSAS

Acknowledgements

Dr. Fengjun Li
Dr. Bo Luo

THANK YOU!

Please let me know if you have any questions about computer science, my experience at KU, or otherwise!