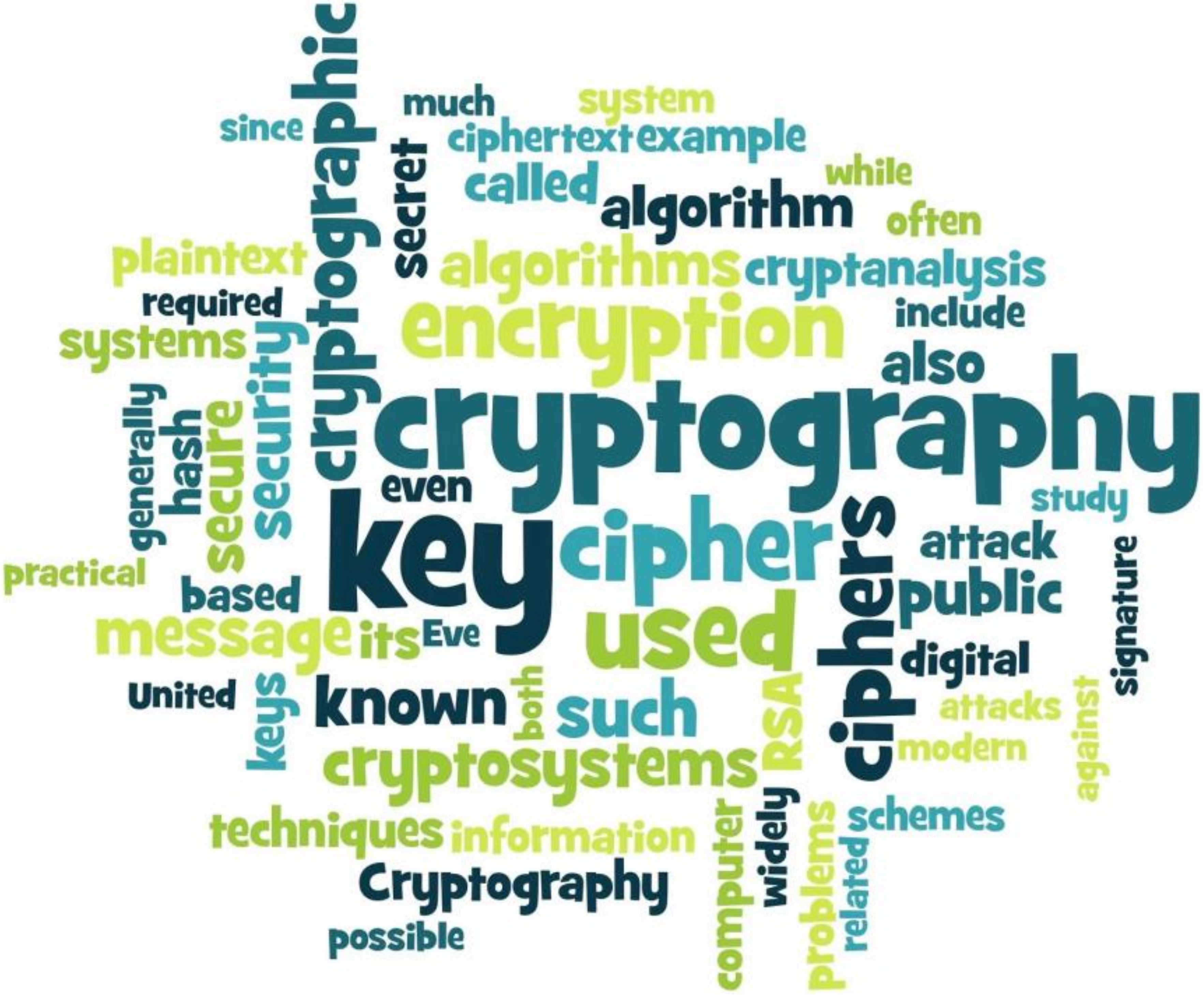
# BGSU CyberGuardian Intro to Basic Cryptography

BGSU® | Department of Computer Science

BOWLING GREEN STATE UNIVERSITY


cryptographic
much
system
since
ciphertext
example
secret
called
while
algorithm
often
plaintext
algorithms
cryptanalysis
required
include
encryption
systems
security
also
generally
hash
secure
cryptography
even
study
key
cipher
ciphers
attack
signature
practical
based
public
message
its
Eve
used
digital
United
keys
known
both
such
RSA
attacks
against
modern
cryptosystems
techniques
information
computer
widely
problems
related
schemes
Cryptography
possible

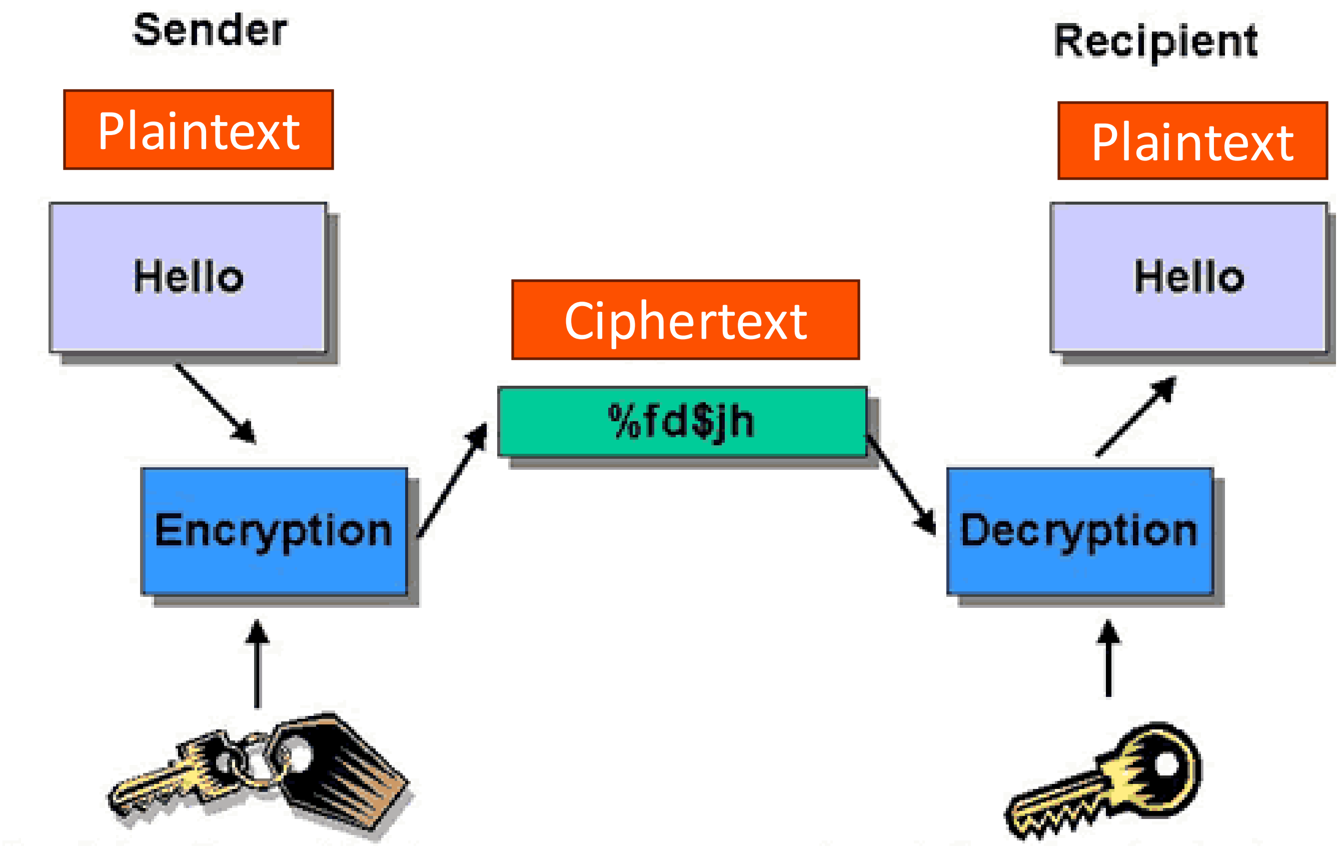
# Exercise with A Mini Cryptex (15 min)

- Two students in one group and explore the mini Cryptex in front of you
- Your task is open the Cryptex, take the items out, and then close it with any password that you like: **You must remember your password!**
- The default password is ‘iloveu’
- A simple instruction is included in the Cryptex box: https://www.youtube.com/watch?v=0SpJ0UsCIEo
- (note: the screws on the mini cryptex don't have to be fully unscrewed to remove the code wheels from the main body)

# Security in the Physical and Digital Worlds

- Physical World
  - Store personal secrets or transfer sensitive information securely via a cryptex-like tool
  - Access is secured through a mechanical password. Only those who know the password can open the Cryptex and access the contents.
- On the Internet?

# Encryption and Decryption



- Encryption Terminology
  - *Encryption*: Transform representation so it is no longer understandable
  - *Decryption*: Reversing encryption process
  - *Plaintext/Cleartext*: Information before encryption
  - *Ciphertext*: Information after encryption
  - Cipher: an algorithm for performing encryption or decryption

# Symmetric Encryption Analogy

- Assume Alice buys a physical password lock, as shown in the picture. The password to lock and unlock is the same: 2390. Alice usually uses this tool to lock a small black box that contains her little secret notes.

  - Q1: What is the physical password lock called in the digital world?
    - Cipher (encryption/decryption algorithm)
  - Q2: What are the encryption and decryption keys?
    - Both are 2390
  - Q3: What are the operations of opening/closing the lock called?
    - Encryption and decryption

*Encryption*

*Decryption*

*Plaintext*

*Ciphertext*

Cipher

# Asymmetric Encryption Analogy

*Encryption*

*Decryption*

*Plaintext*

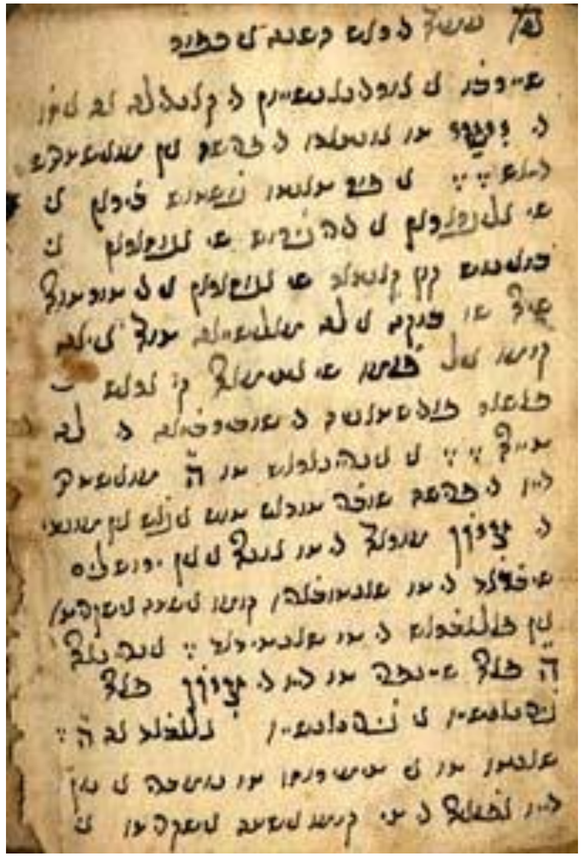
*Ciphertext*

Cipher

- Assume Alice buys a physical password lock, as shown in the picture. The passwords to lock and unlock are different: 2390 is used to close the lock, while 7690 is used to open the lock.
- Alice usually gives this small tool and a small black box to some of her friends to secretly pass some interesting stuff to her. All of Alice’s friends know that 2390 can be used to lock the box, but no one knows 7690.
  - Q1: What are public key and private keys in this scenario?
    - Public key: 2390, private key: 7690.
  - Q2: Who owns the private key?
    - Only Alice.
  - Q3: If Bob gets the black box from Alice, put some snacks inside, lock the box with the password 2390, and put it in Alice’s mailbox, then could anybody else picks up Alice’s box and get the snacks from the box?
    - No, only Alice is able to.

# Early Cryptography

**500 – 600 BC: Atbash cipher – used by Hebrew scribes, Substitution cipher**

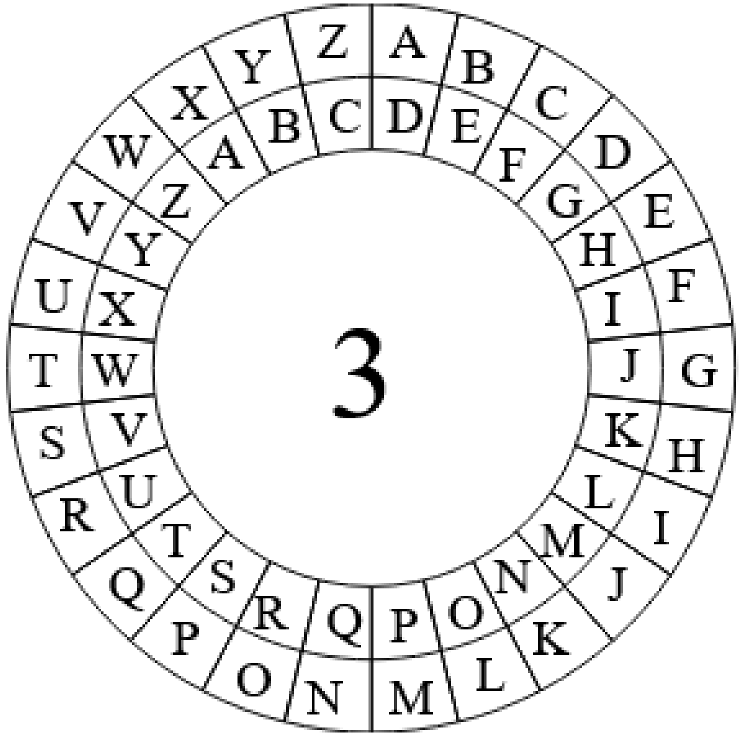


**486 BC: Scytale used by Ancient Greeks**

**Transposition cipher**

# Substitution Cipher: Monoalphabetic Substitution

- A monoalphabetic cipher uses **fixed substitution** over the entire message. **Caesar Cipher** is one example of such a cipher.
- Ex. A key of 3 means rotate 3 letters right, A's are now D's, B's are now E's, etc
  - A key of –3 would mean rotate 3 letters left


3
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
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

Imagine the outer alphabet rotating 3 letters to the right

The inner alphabet becomes your "new" alphabet to encrypt your message

# Example of Caesar Cipher

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Key: 3 (right shift 3 times for each character to get ciphertext from plaintext)

# Exercise on Caesar Cipher (15 minutes)

- Watch a demo for using CrypTool2 to encrypt/decrypt with Caesar Cipher
- Set up a Caesar Cipher environment for yourself

# Exercise on Caesar Cipher (20 minutes)

- Each group sets up a password on your mini Cryptex and keeps it secret.
- Encrypt your password using the Caesar Cipher on Cryptool with any key you choose, generating a ciphertext.
- Exchange your ciphertext and mini Cryptex with another group.
- Bruteforce the ciphertext to discover the password, then use it to unlock the exchanged mini Cryptex.

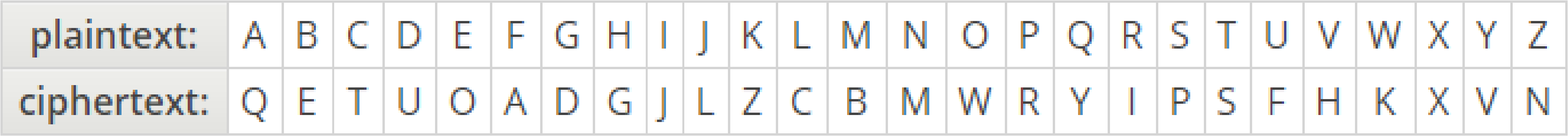
# Weakness of Caesar Cipher

- If you perform a brute force attack on a Caesar cipher, what is the maximum number of tries needed to crack the cipher?
- If I encrypt the letter 'A' using a Caesar cipher by right shifting it 26,001 times, what ciphertext will I obtain?

# Improvement on Caesar Cipher

- See example below:
- The following ciphertext was found and a substitution cipher was used based on the mapping of the table shared by the sender and receiver.

**Ciphertext: QSSQTZ QS UQKM**



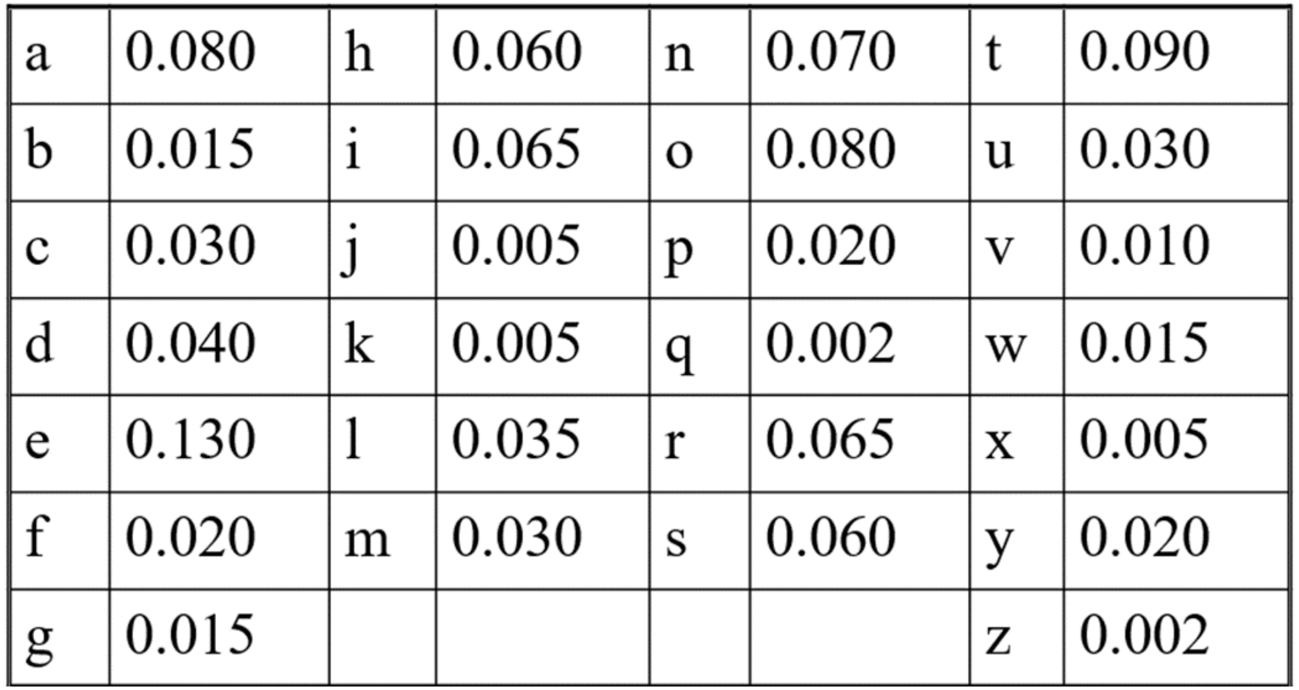
| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| ciphertext: |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

- **Question: What is the original plaintext?**

Answer: Attack at dawn

# Frequency Analysis

- Frequency Matching: The attacker matches the frequencies of the letters in the ciphertext with the known frequencies of letters in the plaintext language.
- Example: If 'X' is the most frequent letter in the ciphertext and 'E' is the most frequent letter in English, the attacker might initially guess that 'X' maps to 'E'.
- Frequency Analysis tool example: [https://www.dcode.fr/frequency-analysis](https://www.dcode.fr/frequency-analysis)



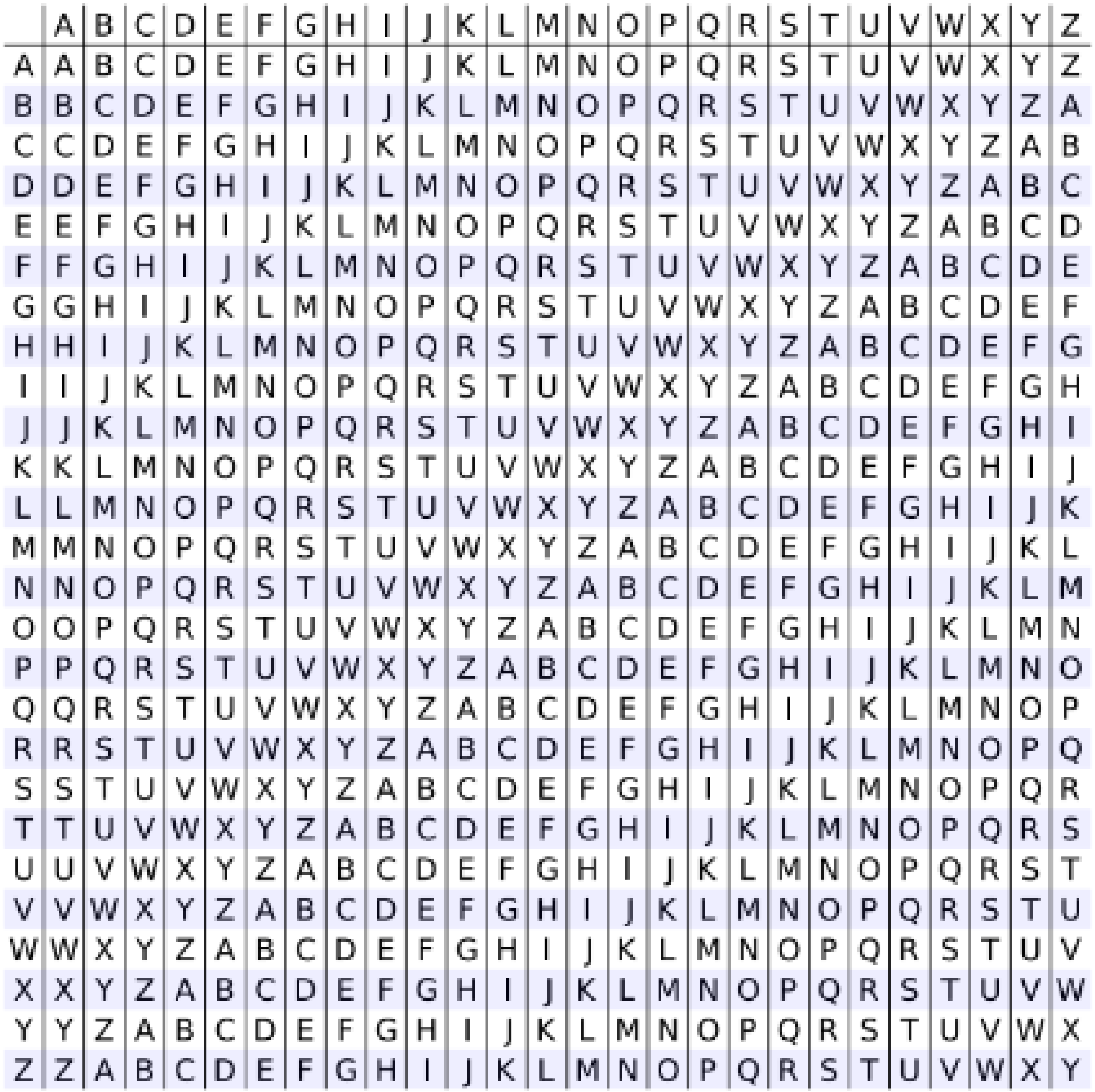
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| a | 0.080 | h | 0.060 | n | 0.070 | t | 0.090 |
| b | 0.015 | i | 0.065 | o | 0.080 | u | 0.030 |
| c | 0.030 | j | 0.005 | p | 0.020 | v | 0.010 |
| d | 0.040 | k | 0.005 | q | 0.002 | w | 0.015 |
| e | 0.130 | l | 0.035 | r | 0.065 | x | 0.005 |
| f | 0.020 | m | 0.030 | s | 0.060 | y | 0.020 |
| g | 0.015 | | | | | z | 0.002 |

# Polyalphabetic Ciphers

- We just saw how monoalphabetic ciphers are vulnerable to frequency analysis

- For polyalphabetic ciphers, each occurrence of a character can have a different substitute (can’t use frequency analysis)
  - Ex. one A could map to a D, and the next A could map to an M
  - The German Enigma used this approach

# Vigenère Cipher



| | 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 |

- Uses a public 26x26 table
- Each row and column corresponds to a Caesar cipher with a shift 0-26
- Choose a key, and repeat it until it matches the length of your message

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Plaintext: | m | e | e | t | a | t | s | i | x |
| Key: | b | g | s | u | b | g | s | u | b |

- To encrypt m by b, go to m-th row and the b-th column, and we get “n” as the ciphertext

# Weakness of Vigenere Cipher

- Invented by Blaise de Vigenère in 1586
- Considered to be secure until 1863
- The Vigenère Cipher can be cracked by converting it into multiple monoalphabetic ciphers and then cracking each one with frequency analysis.
  - For example, since the key is repeatedly used in encryption (e.g., BGSUBGSUBGSU...), if the attacker knows that the key size is 4, they know that the 1st, 5th, 9th, 13th, etc., characters are encrypted using the same character "B". The attacker can group these characters together and crack them using frequency analysis.

| Index | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | B | G | S | U | B | G | S | U | B | G | S | U | B | G | S | U | B | G | S | U | B |
| Ciphertext | W | Z | J | R | F | I | O | J | Z | P | X | W | Z | J | R | F | I | J | S | X | W |

# Modern Ciphers

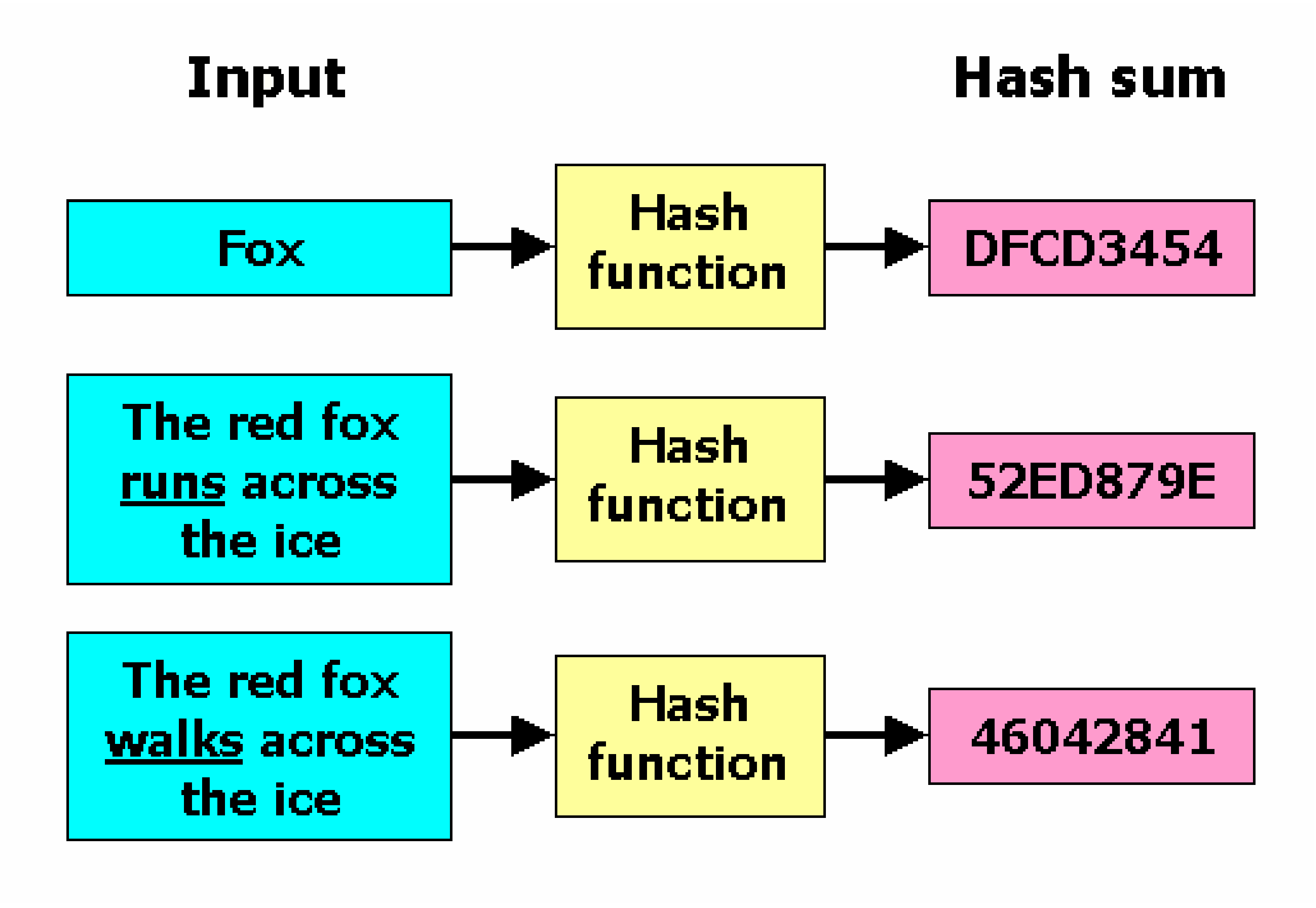
- Modern Ciphers are considered Computationally Secure and there does not exist an efficient way to crack those ciphers.
- Symmetric Cipher
    - Achieve security through complicated substitution and permutation
    - Mostly widely used Symmetric Cipher is Advanced Encryption Standard (AES)
- Asymmetric Cipher
    - Achieve security through mathematical difficulty of certain calculation
    - Mostly widely used Asymmetric Cipher is Rivest-Shamir-Adleman (RSA)

# Exercise on AES Cipher (20 minutes)

- Do this exercise individually and feel free to help each other
- Your task is to recover an encrypted file provided by the instructor

# Another important Crypto Method: Hash Functions

- A mathematical algorithm that transforms an arbitrary amount of input data (message) into a fixed-size string of bytes.
- Important features
  - One-way: Not computationally feasible to find message with given hash
  - Collision resistant: nearly impossible for two messages to hash to the same result
    - Used to check integrity of data



# Exercise on Hash Function (15 minutes)

- Do this exercise individually and feel free to help each other
- Your task is to find out whether the plaintext that you recovered from the last exercise is an original webpage from the BGSU CS website.

# Wrap Up

- Cryptography basics
- Use Cryptool2 to do fun activities
- Brute-force the Caesar Cipher
- Encryption and Decryption with AES
- Using Hash Functions to Check the Integrity of Files