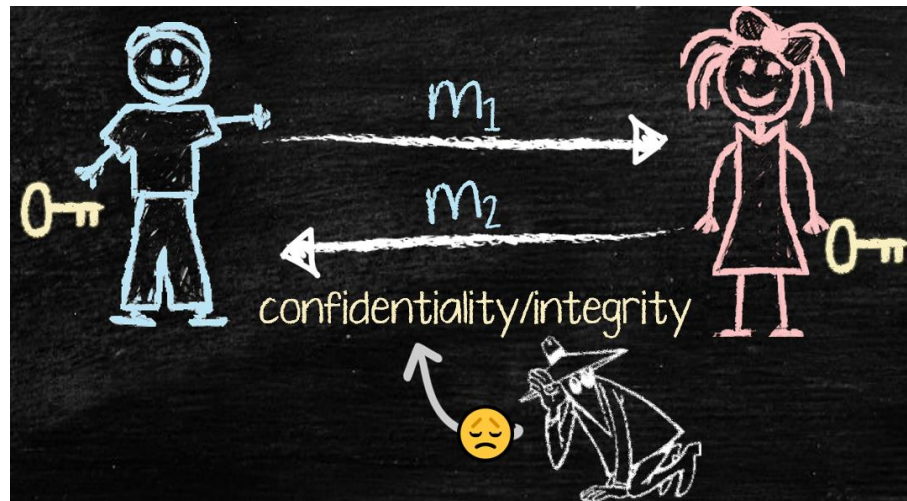


# Introduction to Cryptography

---

# Introduction

- The word Cryptography is Greek
  - Crypto: Secret + Graphy: Writing
- Basic goal is **Secure communication**
  - Send messages that no one but the expected recipient can read
  - Has so many other applications, though!



# Terminology

- Cryptography
  - Method to send secret messages using a key
- Cryptanalysis
  - Trying to break the key and read those messages

# Terminology

- Plaintext: A message in its original form
- Ciphertext: A message in encrypted form
- Encryption: Transforming PT to CT
- Decryption: Transforming CT to PT
- Encryption Algorithm / Cipher: The method used for encryption

# Is It Secure?

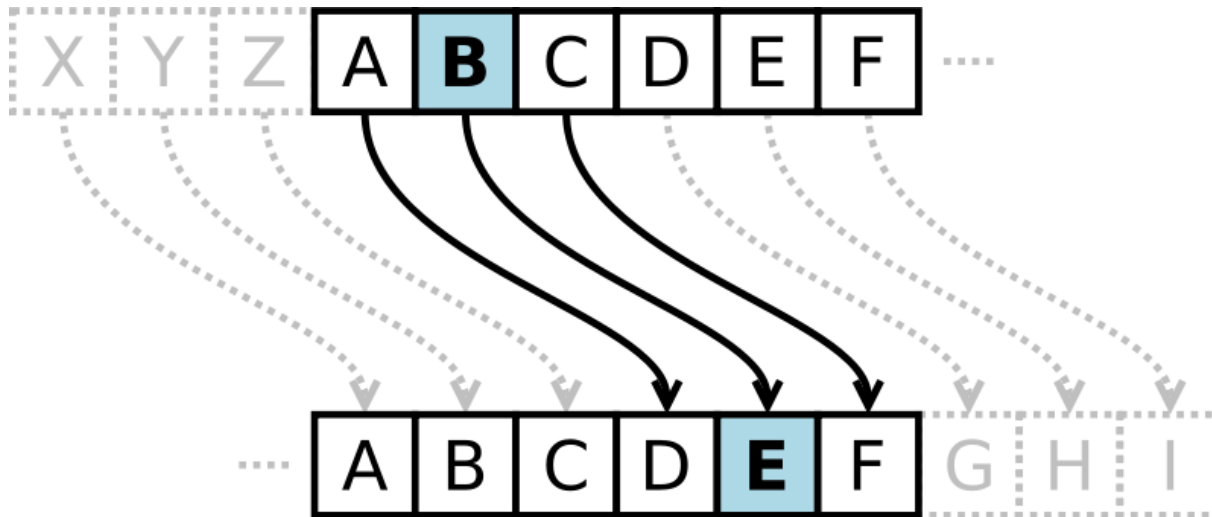
- How do we know if a cryptographic technique is “secure”?
  - We let lots of really smart people try to break it (cryptanalysis)
  - If they can't, we assume it is secure
- Problem: We might be wrong

# Simple Ciphers

- Originally, cryptography was performed by hand
- Goal was to protect messages sent by couriers
  - From people who might intercept the courier
  - From the courier himself
- War was a popular time to use them

# Caesar Cipher

- Earliest documented cipher was used by Caesar in 50BC !
- Each letter in a message is substituted by another that is 3 letters away.
  - A becomes D, P becomes S, etc.



# Caesar Cipher: Example

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

ATTACK AT DAWN

--- - - - -



# Shift Cipher

- Generic version of Caesar cipher
- Each letter is shifted by  $N$ .
  - In Caesar,  $N=3$

# Shift Cipher: Example

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

- Let's do one for  $N=10$ ...

ATTACK AT DAWN

# Shift Cipher: Cryptanalysis

- How do we break this?
- Brute-force: Try all possible values for N
  - There are only 26
- Feasibility?
  - Easy by hand
  - Trivial by computer

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

- Generate a random set of substitutions for each letter
  - Always a 1:1 correspondence

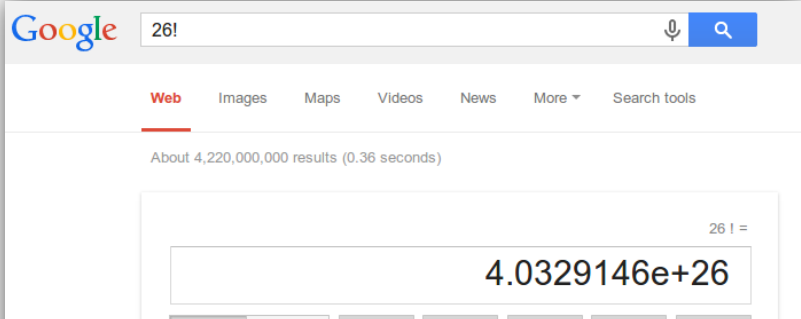
# Substitution Cipher: Example

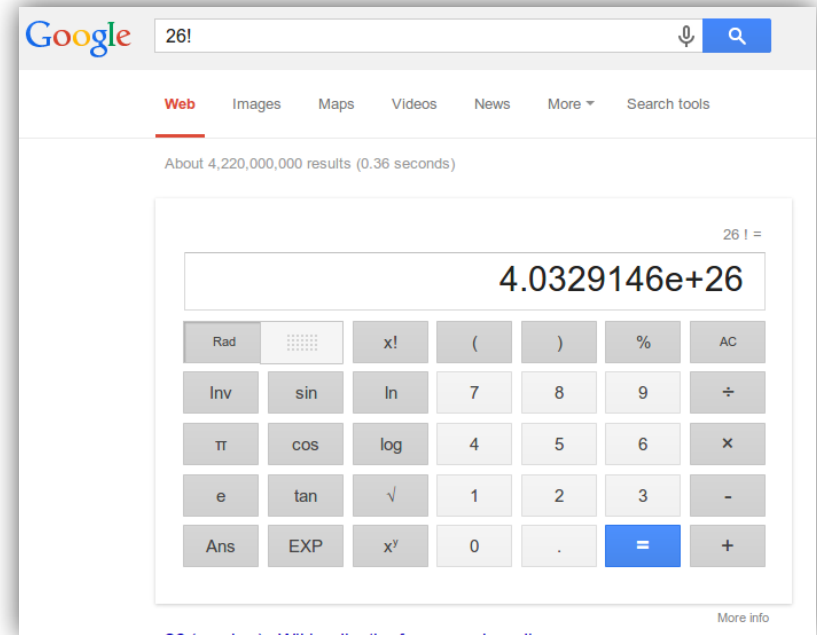
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |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

ATTACK AT DAWN

-----

# Substitution Cipher: Cryptanalysis

- Brute-force: Try all possible letter combinations
    - There are  $(26!)$
  - Not going to do that by hand...
- 
- A screenshot of a Google search interface. The search bar contains the text "26!". Below the search bar, the "Web" tab is selected. The search results show "About 4,220,000,000 results (0.36 seconds)". A large box displays the result "4.0329146e+26" for the query "26 ! =".



# Substitution Cipher: Cryptanalysis

QYYQAV QY WQID

- Key observation: In a substitution cipher, **basic language features** are preserved
  - You can tell how often a letter occurs in the message
  - You can see when letters repeat
  - Etc.
- Use a technique called frequency analysis

# Frequency Analysis

- A cryptanalysis technique discovered by Al-Kindi in Iraq
- Not all letters in a language occur with the same frequency
- In English
  - E is most common  
<http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html>
  - Vowels are about 40%
  - Vowels tend to be separated by consonants
  - Q tends to be followed by U
  - Etc.



# Vigenère Cipher

- Poly-alphabetic cipher
  - One plaintext letter can become *different* ciphertext letters
- Uses a text based key and modulo arithmetic to perform the encryption
- Frequency analysis is possible, but much more difficult

# Vigenère Cipher: Example

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 |

- Let's choose a key of "MONKEY"

ATTACK AT DAWN

MONKEY MO NKEY

- - - - -

# One-Time Pad

- Vigenère cipher with a randomly chosen key as long as the message
- Key needs to be shared between parties beforehand
- Key can **never** be re-used
- Provable unbreakable without the key
- This is the only perfect cryptography

# One-Time Pad: Example

|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 |

- Our random key is “FOWIFOZMQOAF”

ATTACK AT DAWN

FOWIFO ZM QOAF

# Quick Note: Crypto Components

- All of the previous techniques have two basic components:
  - Algorithm (What you do to the message)
  - Key (The secret that you need in order to encrypt/decrypt properly)
- When using these algorithms, the key is secret
- The algorithm is not

# Summing Up

- We trust a cryptographic algorithm if lots of smart people can't break it
- We looked at three types of simple ciphers:
  - Shift Cipher
  - Substitution Cipher
  - Vigenère Cipher
- They each have an algorithm and a key